IJNS
International Journal of Network Security

ISSN 1816-353X (Print)
ISSN 1816-3548 (Online)

Vol. 18, No. 4 (July 2016)

INTERNATIONAL JOURNAL OF NETWORK SECURITY

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Network Security is published both in traditional paper form (ISSN 1816-353X) and in Internet (ISSN 1816-3548) at http://ijns.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

International Journal of Network Security

Vol. 18, No. 4 (July 1, 2016)

Strong Zero-knowledge Authentication Based on Virtual Passwords

Younes Asimi[1], Abdallah Amghar[2], Ahmed Asimi[1] and Yassine Sadqi[1]

(Corresponding author: Ahmed Asimi)

Departments of Mathematics and Computer Sciences, Ibn Zohr University[1]

Department of Physic, Ibn Zohr University[2]

Information Systems and Vision Laboratory (LabSiV), B. P. 8106, City Dakhla, Agadir, Morocco

(Email: *asimiahmed*2008@*gmail.com*)

(Received May 23, 2014; revised and accepted Sept. 23 & Nov. 8, 2014)

Abstract

Currently, the security of the users' privacy in public spaces has more concerns especially in web applications. Also, the unconsciousness of users by the importance of the quality cryptographic of these authentication parameters makes their commoditized accounts. Hence, investment in the computer discipline becomes more demanding to prevent potential attacks. In this paper, we introduce a new strong zero knowledge authentication system based on virtual passwords (SAVP). Its objective of this paper is to ensure the identification of users on the network by ensuring intractability, portability, unpredictability, integrity and reusability of their authentication settings. In the second section, we study the difficulties and users habits followed in the selection, storage or memorizing passwords, as well, the evolution and the limits of all categories of texture password authentication. Also, we locate the importance of integration of salts in authentication mechanisms and their impacts on the robustness of passwords regenerated. As for the third section, we start with a detail description of all mechanisms and component contributing to the robustness of our mutual authentication system. Our goal is to provide a strong zero knowledge authentication system based on salts generated by a cryptographically secure random regenerator, algorithm for dynamic rotation of binary strings, symmetric cryptography primitive, one-way hash function and random nonce to provide mutual authentication. The security analysis of our proposal, which is the goal of the fourth section, shows their ability to resist against multiple types of attacks.

Keywords : *Dynamic rotation of binary strings, mutual authentication, one-way hash function, strong zero knowledge authentication, virtual password*

1 Introduction and Notations

Authentication systems have highly evolved in recent years, particularly in public environments especially in web applications. Also, activities and government enterprises rely increasingly on these technologies. This protocol requires identification by username/password and monitoring states of sessions and cookies. In addition, their facilities implementation and deployment have made omnipresent and unavoidable. Their seductive and opportunities in the evolution of companies encourage more attackers to re-evolve their ways of attacks.

Attacks against this protocol affect, in general, the confidentiality of data exchanged between the client and the server. In particular, authentication settings and states monitoring. For this, it requires the use of Secure Socket Layer (SSL/TLS) when registering or logging on to the internet via HTTPS. That seeks to have a valid digital certificate and a browser be able to manage the public key infrastructure (PKI). In case of sensitive data, instead of sending passwords in clear, they introduced one way hash functions to make the password hash. But with the variety of types of attacks that fit with any situation, this system is unable to ensure the privacy of the users. In particular, if we note that static passwords gen-

eration is totally breakable. At present, they are three strong alternative password authentication systems: One-time Passwords [2, 13], Object Passwords [16] and Virtual Passwords [14, 29].

The security of web applications is one of the areas that generate more concerns within research laboratories and companies [3, 7, 8, 9, 13, 19, 20, 21, 22, 26, 28, 31]. In particular, the transmission and storage of highly sensitive data like passwords. Certainly the experts have sacrificed more time to certify the objectives of computer security [31]. The emergence of new vulnerabilities related to cryptographic hash functions, the JavaScript programming language and existing authentication systems, we addressed in this paper to design a new of strong authentication system for remedy these problems. We focused on strong zero-knowledge authentication based on the virtual passwords be able of withstanding data theft attacks on the client or server side, such as Phishing, Shoulder surfing, SQL injection, collision, the man in the middle, brute force, dictionary and spyware. Thus, we rely our proposal on one-way hash function, symmetric cryptographic primitive, salts per user generated by a cryptographic random regenerator sure [1] and random nonce to ensure mutual authentication.

Our work is divided into four sections. In the second section, we study the difficulties and habits followed by users in passwords selection and storage, also, the evolution and the limits of all texture password authentication categories. And, we locate the importance of integration of salts in user authentication mechanisms and their impact on the robustness of the generated passwords. In the third section, we start by describing in detail the objectives of our proposal such as: zero-knowledge, untraceability, portability, integrity and authentication settings. Then, we study the regenerator user-specific random salts and their impact on the quality of cryptographic passwords regenerated. For dealing with problems of static salts, we propose an algorithm for dynamic rotation of binary strings and study its impact on the unpredictability and non-traceability of original passwords totally breakable for minimal disruption. The results obtained show the random nature of passwords generated for the minimum conditions of security. The security analysis of our system, which is the objective of the fourth section, shows the ability of our system to resist against multiple types of attacks.

In the rest of this paper for each user U_i, we denote by:

ID_i	: The user identifier U_i.
PW_i	: A valid original password.
PWV_i	: The virtual password.
HPW_i	: The final password.
RS_i	: Random salt.
$CSRS_i$	: Cryptographically secure random salt.
CRC	: Cyclic redundancy check.
CVL	: CRC code of variables lengths.
DR	: Dynamic rotation.
E	: Symmetric cryptographic primitive.
H	: One-way hash function.
Tb_i, Ts_i	: Random nonce.
$<<<$	: Rotation left without loss of information.
$>>>$	: Rotation right without loss of information.
$\oplus$	: XOR operation.
$==$	: Comparison.
$\|\|$	: Concatenation.
$P(x)$	: Probability of event x.
$NIST$	: National Institute of Standards and Technology.
CC_i	: Challenge of server calculated by the client.
RCS_i	: Challenge and response of client calculated by the server.
RC_i	: Client's response to server's challenge.
RCC_i^{new}	: Response and challenge server's calculated by the client.
X_i^{new}	: Renewal of the parameter X.

2 Related Work

The improvements proposed to evaluate their level of security remain unable to overcome all these weaknesses [26, 31]. In particular, if we note that the design architectures provide static passwords engendering more security concern. Similarly, habits followed by users to select and maintain passwords of many online accounts are courageous for attackers. It should also be noted that all studies in this field confirm that the great challenge among the users is the difficulty to remember a password for each online account [3, 7], which generate the following habits:

- Users choose passwords that are easy, memorizable and guessable.
- They reuse the same password on multiple accounts despite their consciences by the risks.

- They resort to share these passwords with other individuals.
- They often forget their passwords.
- They store them in plain text in the browser.
- They use personal information to build these passwords.

In general, all studies in this field have shown that the problem of memorization and storage is among the major causes of the inability of users to respond to recommendations of the computer security related to passwords [8, 9, 19, 22, 28, 31]. But at the university level, a survey realized by Shay et al. [27] showed that the majority of the users are aware by the impact of the requirements of the computer security on their accounts. Moreover, they found users who can memorize complex passwords. In parallel, other alternatives were proposed to replace the architectures of authentication by texture passwords. Conlan et al. [5] confirmed that the only alternative which entered in significant competition with this technique is the one which based itself on graphic indicators to calculate the passwords of every user. But, the technique of passwords textures stays the most usable, profitable and attractive [32].

2.1 Evolution of Texture Password Authentication

The robustness of a password is the measure of its capacity to resist against various types of attacks. It estimates the average degree of necessary attempts (for every type) to an attacker to discover any original password. The robustness is a function of the length, the range of lengths, the period, the unpredictability, the untraceability, the reusability and the complexity of distribution of the random characters of the password.

2.1.1 Static Passwords

At the time of the computing, this technique was the simplest method of authentication to implement, efficient and secure to protect the accesses to sensitive data. The evolution and the opening of the computer systems on the network have made the static passwords ineffective to assure the privacy of users. Also, the evolutions of the techniques of attacks have trivialized them especially in public environments. In this case, a password remains identical for several connections commonly met under Windows and Unix. The current recommendation is to limit their uses for the local authentication.

2.1.2 One-Time Passwords

To push aside the risk theft of static passwords in insecure channels, Lamport [13] described a scheme of a one-time password (OTP) which based on the repetitive hashing. It generates a different password for every connection more strong than the static password. The inconveniences of this technique come from the dependence of the generated passwords, the listening of doors, the stealing of the passwords and the time required executing N times the hash function. Several variants studies were developed to evolve the level of security of this protocol. Bellovin and Merrit [2], proposed a protocol for exchange of encrypted keys (EKE) and then its extension, which allows preventing the dictionary attacks and the compromise of password files. This extension is based on a one-way hash function to hash passwords, nonce for mutual authentication and Diffie-Hellman to compute a session key. Morris and Thompson [18] introduced another alternative of OTP to ensure password security on UNIX. They are based on storing passwords salted and hashed to reduce the risk of password file compromise [3]. This technique has been improved by Feldmeier and Karn [32].

2.1.3 Objects Passwords

The systems of alphanumeric passwords are easily attacked by shoulder-surfing and Spyware, in which the adversary can record users' movements by a hidden camera when the user tapes the password or with a Trojan Horse. In order to meet the recommendations of the security related to the choice of passwords that have high entropy. Also, to help users who are unable to store random passwords generated by the machine. ObPwd [16] is another alternative system to generate the strong's enough passwords based on digital objects. The user does not need to remember a very complex password. But, just for him to remember a password object locally or in the web. When the user points at an object, this system takes care to recover its signature (SHA-1) as being a password of strong entropy. The choice of objects digital as passwords is an interesting alternative to be explored. Because, in addition to the cryptographic quality of passwords created and maintained by the users, it is very sophisticated against Spyware and shoulder-surfing attacks. Especially, the software that are based on the recording of keystrokes

on local machines.

2.1.4 Virtual Passwords

Another alternative for traditional password was proposed by Lei et al. [14] in 2008. It is based on a virtual password system. Its objective was for them to have a mechanism of authentication capable of withstanding the theft attacks, phishing and the keylogger and shoulder-surfing attacks. They used a linear random function, a salt generated by the random server, a fixed password and a random number selected by the user. This virtual system has been modified by [30] in order to minimize processing time by the server. This system is theoretically breakable because all keys $\{0, ..., Z-1\}$ are finished. In 2011, Sandeep Kumar Sood et al. [31] proposed a Inverse Cookie-based Virtual Password Authentication Protocol. This authentication protocol is based on the storage of cookies on the client computer and the Secure Socket Layer protocol (SSL) to protect the advantages of authentication by password and to evolve its complexity against multiple attacks including dictionary attacks online. But, according to an analytical study made on SSL protocol by American researchers, monitoring of web traffics leaves sufficient information even if the data that transit are encrypted [17]. It also presents a very important evolution for passwords authentication systems, because it allows to regenerate different virtual passwords for every user. But, it does not manage to push aside SSL vulnerabilities. In addition, it does not ensure the quality of the encrypted passwords.

2.1.5 Evolution of Salts

The salt was introduced by Morris and Thompson [18] as another alternative of OTP to ensure the password security on UNIX. We note that several extensions have been proposed to develop the security of the password against multiple attacks specifically against Phishing and Spyware attacks. The technical of SpoofGuard [4] is a browser extension that examines Web pages and notifies the user when data requests may be part of a spoof attack (Phishing). Halderman et al. [11] proposed a mechanism operates entirely on the client. This extension allows the reassurance of the passwords against the attacks of dictionary by means of a hash function. We are stretching the hash function it can complicate the calculation of the original password. More critically, it generates the static passwords unable to resist against multiple attacks (Phishing or Replay attack). In 2005, PwdHash [23] was developed for Internet Browsers Explored and Mozilla Firefox. It allows improving the security of passwords in Web applications. It generates a different password for each site seamlessly. This extension applies a cryptographic function on a password in clear and its private salt stored in the client computer. In general, this extension allows you to generate a global salt (equivalent to the domain name of remote site) specific to each site. This technique helps to prevent Phishing attack but remains unable to resist against network attacks (Man in the middle, Replay attack) and attacks against servers (brute force attack, dictionary attack, theft of the database). Numerous studies on JavaScript attacks showed that the implementation in complete safety of the hashing in the browser is rather difficult on the modern Web applications.

3 Our Proposal

The studied systems of authentication are divided on three categories: virtual passwords, object-based passwords and one-time passwords. The robustness of passwords of all these proposals on one hand is expressed according to the length, to the plage, to the random nature and to the unpredictability and on the other hand is related to the behavior of users which has a very important impact on the cryptographic quality of their passwords, and that it is impossible to control, but can be evolved through the sensitization. The aim of our proposal is to strengthen the users' authentication by virtual passwords. We therefore propose a system be able of withstand multiples types of attacks including Phishing, dictionary attack, brute force, Spyware, man in the middle and also the problem of collision [31]. It minimizes the number of passwords memorized by users. It's based on a salt per user generated by a cryptographically secure random regenerator [1], one-way hash functions, a symmetric cryptographic primitive, nonce to ensure the mutual authentication and the updating of authentication settings during the phase renewal.

Random passwords are difficult to remember. Thus, the interest to introduce this new proposal of a zero-knowledge authentication system based on virtual passwords (SAVP). The users don't need to remember a password for each account and can use it for more than one account. Because, the cryptographic quality of our system is related to the random nature of regenerating of salt used to ensure untraceability of passwords on the network [1].

Our proposal is characterized by:

- A random salt appropriate to each user [1] to avoid the problem of change of domains.
- The integrity of this salt is assured by CRC code of variables lengths [1].
- The space of keys is unlimited and the primitive signals constituting the generated keys meet of the following conditions [1]:
  - Their length and period are variable and unpredictable.
  - Their distributions will also be unpredictable.
  - The untraceability of the keys.
- The users are free to choose the way of seizing words pass by keyboard or to use the passwords objects that have a great ability to counter spyware attacks.
- The users do not need to make calculations. The regeneration of the virtual passwords is made transparently.
- The use of a strong cryptographic hash function (SHA-224).
- The update of the authentication settings collaborates to protect servers against the potentials types of attacks.
- It is almost impossible to find the same virtual password for two users who have the same original passwords.

3.1 Zero-Knowledge Proof

The concept of a proof of zero-knowledge was introduced in the firstly by Goldwasser, Micali and Racko [10]. It is used in cryptography to ensure the identity of users. It appears in the mutual authentication protocols without disclosure of secret data in the form of challenges and responses. The entities must authenticate without needing to reveal the accuracy of their secrets.

3.2 Reuse of Passwords

Users are unable to memorize a complex password for every account. Thus, the majority of them reuse a single password in several accounts, share with others and also store it clear in the browsers [3, 7]. To cope with these difficulties, in our system, we melt the security level passwords regenerated on the cryptographic quality of our regenerator of the salts used [1]. The goal is to have passwords able to resist the network and server's attacks. Therefore, the users will not need to change them to make sure on their cryptographic qualities. But, they have to cope with Spyware attacks.

3.3 Untraceability of Passwords

In internet, the traceability of connection data (logs) is a solution to monitor users and conducting surveys. It also serves to follow their activities to create profiles in the semantic case of Web: the movements, the consulted sites, the exchanges and the sharing. And it can become a cause of mistrust and disclosure of confidential data. Since most attacks are based on spying sensitive data on the web especially the passwords, thus our objective is to propose and study a strong authentication system based on the regeneration of virtual passwords to guarantee their untraceability.

3.4 Portability of Our Authentication System

In addition to security in web applications, it adds another very important characteristic: the portability of an authentication system. Indeed, most authentication systems offer very complex architectures to gain the trust of users. Generally, they base on the capacity of modern Web browsers to memorized the parameters of authentication to simplify the users experience. But, they forget the risks bound to the problem of not standardization of browsers and the security of the files of storage of these parameters client side. More critical, they impede the movement of internet users to a specific browser. For that purpose, in our proposal, all authentication parameters will be stored on the server side to assure the portability of our system. Besides, the passwords will be strengthened by safe cryptographic salts to have more security, simplicity, safety and trust of the users.

3.5 Controls of Integrity

The majority of authentication architectures leave out the control of the integrity of data exchanged between the server and the client during authentication. They can be the cause of failure of authentication because attacks do not always have an intention to have the access to

your account; but they can try just to damage the validity of your parameters of authentication. Consequently, the corruption can be involuntary. For this interest, we propose a dynamic system that ensures the integrity and authenticity of the parameters of authentication of data exchanged between the communicating entities. Thus, we introduce a technique for error detection (CRC) of variables lengths which adapts with any polynomial generator (Noted CVL) [1] to ensure the integrity of messages exchanged between the client and the server salt and an one-way hash function to generate very strong passwords which will be used as encryption keys and decryption.

3.6 Random Generator of a Safe Cryptographic Salt

We refer to [1], the salts regenerated by our regenerator $RGSCS$ have unpredictable primitive signals, pseudo-random and in certain cases seems chaotic. That is to say, their divinations by the successive iterations are almost impossible. The interest to introduce this system is to meet the requirements of computer security and also to solve the problems of storage and memorization of complex passwords of the users in Web applications. It is built on salts appropriate to every user generated by a secure cryptographic random regenerator [1]. The purpose, is to contribute to the level improvement of security of the passwords against multiple types of attacks.

The regenerator $RGSCS$ consists of three processes. For details see [1]:

- The regeneration of random salts.
- The calculation of a CRC of variable length on any primitive signal to assure the integrity of regenerated salts.
- The check of the integrity of salts and the update of the authentication settings.

According to $NIST$ [25], the length and the range of lengths are among the key factors of the robustness of generated passwords. To test the impact of this regenerator on their cryptographic quality, we have to calculate minimal and maximal complexity ($\mathbf{S_{m,N}}$). Then the probability to have such a primitive signal for minimal passwords. According to [1], we have:

1) The cardinal of $\mathbf{S_{m,N}}$ is $\#\mathbf{S_{m,N}} = \mathbf{2^m(2^{N+1} - 1)}$.
2) If the elements of $\mathbf{S_{m,N}}$ are equiprobable then for all $\mathbf{S} \in \mathbf{S_{m,N}}$ we get $\mathbf{P(x) = 1/\#S_{m,N}}$.

The recommendation of the information security is to have a password that consists of at least eight characters. In the table below, we studied the complexity and the probability of the virtual passwords according to a password and salt regenerated by our algorithm [1].

Table 1: The complexity and the probability of the virtual passwords regenerated

The length of the salt (bit)	Complexity	Probability
without	$\mathbf{1.845\ 10^{19}}$	$\mathbf{5.422\ 10^{-20}}$
140	$\mathbf{2.572\ 10^{61}}$	$\mathbf{3.890\ 10^{-62}}$
150	$\mathbf{2.663\ 10^{64}}$	$\mathbf{3.799\ 10^{-65}}$
160	$\mathbf{2.696\ 10^{67}}$	$\mathbf{3.710\ 10^{-68}}$
...	...	...
180	$\mathbf{2.827\ 10^{68}}$	$\mathbf{3.538\ 10^{-74}}$
185	$\mathbf{9.047\ 10^{74}}$	$\mathbf{1.106\ 10^{-75}}$

According to these results (Table 1), we notice that the complexity and the probability to have such a primitive signal are strongly evolved and compared with the original passwords (without salt). Thus, the key space has increased by $\mathbf{1.394\ 10^{42}}$ for a salt of a minimum length and by $\mathbf{4.904\ 10^{55}}$ for a salt of a maximum length by report an original password. Also, the probability of such a primitive signal has decreased by $\mathbf{7.175\ 10^{-43}}$ for a salt of a minimum length and $\mathbf{2.040\ 10^{-56}}$ for a salt of a maximum length by report an original password. Of course, the keys space is very important for evolving their level of security against multiple attacks, but, this is not sufficient to speak about the random complexity of the passwords which meet the requirements of the computer security. For that purpose, we have to estimate the impact of this regenerator on the unpredictability of the regenerated primitive signals.

3.7 Dynamic Rotation of Binary Strings

Knowing that, if an attacker manages to find the static salt associated with a password, their mission to find the original password in clear rest to build a dictionary contains all possible combinations. Indeed, the concatenation has no influence on the level of security, it can extend only its length. And if of more the integration of this technique in the systems of authentication remains in a static way [4, 11, 18, 23], then to strengthen the level of security of a system of authentication based on

passwords, we thought of proposing a virtual system of authentication based not only on blocks of data, but on their binary parts. Hence, we propose a new mechanism of regeneration virtual passwords by basing itself on salts by user [1] and on algorithm of dynamic rotation of the binary strings before the hashing. The goal is to have passwords which have the recommended characteristics in current authentication systems namely: untraceability, randomness, virtual and also reusable.

In our approach, the objective is not to complicate the existing proposals. For that purpose, we build our proposal on simple and practicable operations in most of the programming languages namely:

- The concatenation of a password PW_i and an unpredictable salt RS_i appropriate to every user U_i.
- The regeneration of a binary sequence $S = x_{nb} \dots x_1$ from $PW_i \| RS_i$, with $x_i \in \{0, 1\}$.
- The ordinary sum of the bits positioned in one in S to determine the dynamic position of the rotation P_i: $P_i = \sum_{i=1}^{nb} x_i$.
- The dynamic rotation depends on the parity of P_i, as follows:
  - If P_i is even, we shall have a circular rotation to the right with P_i position.
  - If P_i is odd, we shall have a circular rotation to the left with $nb - P_i$ position.
- Hence, the regeneration of the virtual passwords $PWV_i = DR(PW_i \| RS_i)$.

To estimate the complexity of the virtual passwords generated in our system, a behavioral study is dedicated to the analysis of these generated primitive signals. For this, we will study the divergence of Hamming distances between the primitive signals [1] after minimal internal disturbances (a single bit) on a totally breakable password for the same salt and its impact on the robustness of these passwords regenerated.

3.7.1 Impact of Minimal Perturbations of an Original Password on Virtual Passwords

To estimate the impact of this algorithm of dynamic rotation over the complexity of the regenerated virtual passwords, we will study the distribution of distances of the primitive signals regenerated by minimal disturbances (only bit by iteration) on the initial condition ($PW_i \| RS_i$). For this, we take the original totally breakable password "*aaaaaaaa*" concatenated with a given salt. The perturbations will be only made on the original password.

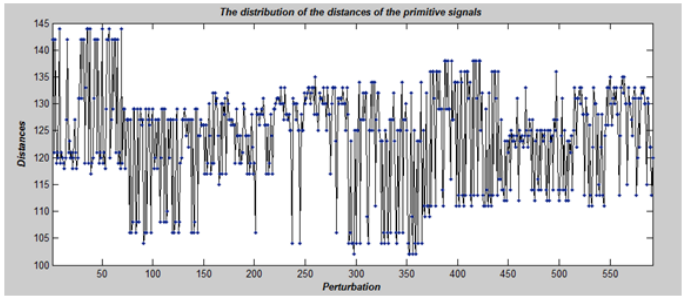


Figure 1: The distribution of distances of primitive signals according to the minimal perturbations on the initial condition

According to this histogram (Figure 1) we notice that, for any iteration, the range of lengths of the distances is more important and more subtle (between 100 and 145 bits), and their distribution seems chaotic. Therefore, our system assures the untraceability in spite the reuse of a same password. This algorithm will thus have a very remarkable contribution on the complexity of the virtual passwords regenerated. However, if an attacker manages to find the final plaintext passwords, it will be painful for him the exact localization of the password entered by the user.

3.7.2 Impact of Salts on the Robustness of Passwords

In order to argue the impact of this dynamic rotation algorithm on the robustness of passwords, we study the correlation of primitive signals regenerated for original password concatenated with two hundred salts. More critically, we chose a password that meets the minimum recommendation of computer security.

Original password: $a * 7F\_eW5$.

According to this histogram (Figure 2), we can split the zones of interest into three portions:

- Between 0.3 and 0.42: the distribution of the normalized distances [1] seems to a chaotic phenomenon.
- Between 0.42 and 0.52: we have an accumulation of the normalized distances. But, with a distribution seems a bit like Gaussian curve followed by small peaks.

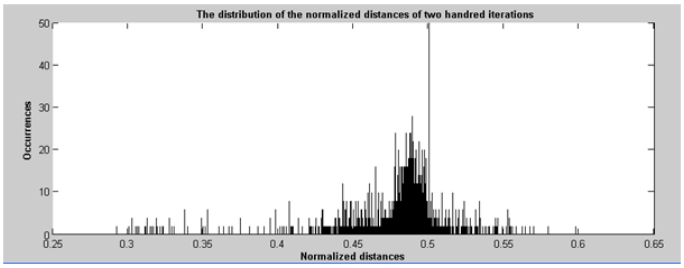


Figure 2: The distribution of normalized distances

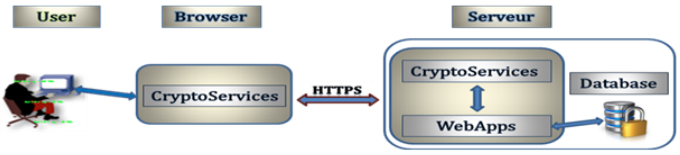


Figure 3: Model of SAVP

- Between 0.52 and 0.6: almost the same as the first portion.

We refer to (Figures 1, 2), $NIST$ [25] and [1], our system has filled the characteristics recommended by computer security. It enables us to make sure well over the cryptographic nature of the virtual passwords. Finally, we can summarize these internal characteristics as follows:

- The distribution of lengths and periods is random.
- The passwords are unpredictable.
- The untraceability of the original passwords.

Consequently, we assure the uncorrelated, the untraceability and unpredictable of the regenerated primitive signals can withstand the multiple types of attacks such as: dictionary attack, brute force attack, phishing attack, man in the middle attack (MIM) and also in the collision problem. Therefore, the robustness and the complexity of the virtual passwords regenerated are assured.

3.8 Strong Authentication by Virtual Passwords

3.8.1 General SAVP Scheme

Figure 3 is a model of strong authentication by virtual passwords (SAVP). The scheme of our proposal is composed of the following items:

The browsers. They would support the protocol $HTTPS$ to guarantee more confidentiality of data exchanged between the customer and the server.

Extension CryptoServices. It must provide, in both sides, the following features:

- The hash functions.
- The symmetric cryptographic primitives.
- The dynamic rotation of binary strings.
- The CRC code of a variable length.
- Regeneration random salts RS_i specific to each user U_i.

WebApps. It is web application usually placed on a web server and handles by pressing of widgets using a web browser via a computer network. It can be a system of content management, search engine, an e-commerce software, a social network, etc.

Database. Each user U_i is characterized by four authentication settings, which will be created during the recording phase. These settings are used to identify users during the authentication phase (See Table 2). They can be changed easily during the renewal phase:

- **Identifier (ID_i):** Only identifier (ID_i) for each user (U_i).

Table 2: Users authentication settings

ID_i	HPW_i	$CSRS_i$	N_i

- **Password (HPW_i):** In our proposal, the password will be used as an encryption key and decryption to ensure:
  1) The identification of users during authentication and renewal phases.
  2) The confidentiality of nonce exchanged between the client and the server to assure the mutual authentication.
  3) The confidentiality of the new passwords chosen by the users during the renewal phase.
- **Salt ($CSRS_i$)**: In the registration phase, a random regenerator handles to regenerate $CSRS_i$ for each user who has a chaotic behavior [1]. It will be associated with the original password to ensure its robustness and its complexity.
- **A positive integer (N_i):** It corresponds to the sum of the bits positioned in one in a primitive

signal RS_i. It will be used to generate a polynomial generator to make sure on the integrity of the salts ($CSRS_i$) [1].

3.8.2 Conception of SAVP

Our mutual authentication system SAVP consists of three phases: the registration phase, the identification and authentication phase and the renewal phase.

3.8.2.1 Registration Phase

This phase, allows any new user to register with the Web application. Each user should have a unique representation within server. The data exchanged very sensitive require a level of confidentiality and integrity quite high (See Figure 4). Hence, the necessity to recommend the use of $HTTPS$ protocol to ensure the confidentiality and integrity of the authentication settings.

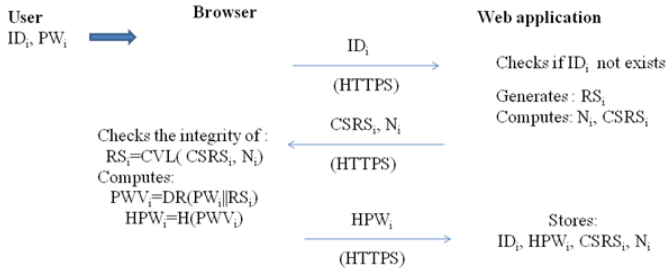


Figure 4: Registration phase

This registration process can generate for each user U_i itself authentication settings. It is based on random salts regenerated by a cryptographically safe regenerator and original password chosen by the user U_i as follows:

- The user U_i must have a valid password PW_i and an unique identifier ID_i that does not exist in the server database. If it exists, the server sends back a message of exception informing the user to choose other identifier.
- The browser sends the identifier ID_i entered by the user U_i to the server.
- The server checks the existence of the user U_i, otherwise:
  - Generates a random salt RS_i.
  - Calculates a number N_i and $CSRS_i$.
  - Sends a salt $CSRS_i$ and a number N_i to the browser.
- The browser:
  - Calculates $RS_i = CVL(CSRS_i, N_i)$.
  - Calculates virtual password, by using the Dynamic Rotation (DR) on the concatenation of an original password and a random salt: $PWV_i = DR(PW_i \| RS_i)$.
  - Calculates the final password by hashing of the virtual password with a one-way hash function H: $HPW_i = H(PWV_i)$.
  - Sends the final password HPW_i to server.
- The server:
  - Saves the authentication parameters associated to the user U_i: ID_i, HPW_i, $CSRS_i$, N_i.

3.8.2.2 Identification and Authentication Phase

In this phase each user U_i must provide a proof of its identity (username/password) to the server. Obviously, authentication systems based on a simple password do not meet the demanding requirements of computer security. For this, we integrated several parameters of authentication to assure strong authentication of the users. The goal is to establish a secured session with the Web server by using the $HTTPS$ protocol and the authentication service. In this phase, we have to make sure on (See Figure 5):

- Identity of the users.
- Integrity and confidentiality of exchanged random salts.
- Validity of recalculated passwords.
- Mutual authentication.

The identification and authentication process allows verifying well the identity and authenticity of the users and the server. The aim is to provide mutual authentication between communicating entities without disclosure the originals parameters of authentication. Also, for more confidence and seductive, we ensure over the untraceability and portability in our system.

- The browser:
  - Sends the identifier ID_i of a user U_i to the server.
  - Generates a nonce Tb_i.
- The server checks the existence of the user:

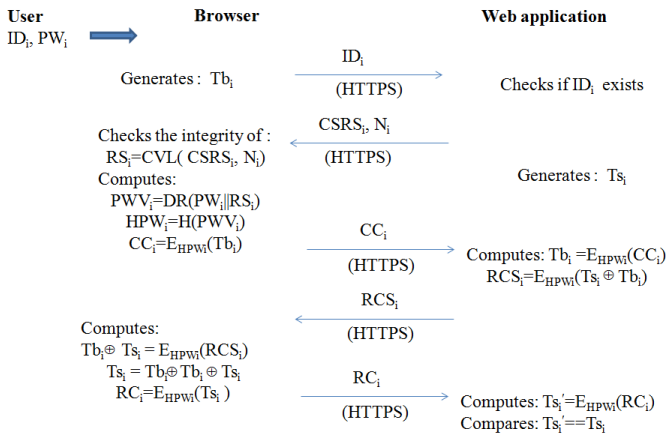


Figure 5: Identification and authentication phase

- If yes, then the server:
  - ∗ sends a cryptographically secure random salt $CSRS_i$ and N_i number.
  - ∗ Generates a nonce Ts_i.
- Otherwise, it returns an error message.

- The browser:
  - Checks the integrity of $CSRS_i$ by calculating $RS_i = CVL(CSRS_i, N_i)$.
  - Calculates the virtual password of a user U_i by Dynamic Rotation applied to the concatenation of its original valid password PW_i and its random salt RS_i : $PWV_i = DR(PW_i \| RS_i)$.
  - Calculates the final password of the user U_i by hashing the virtual password PWV_i with a one-way hash function H: $HPW_i = H(PWV_i)$.
  - Encrypts the nonce Tb_i by the final password HPW_i as a symmetric encryption key: $CC_i = E_{HPW_i}(Tb_i)$.
  - Sends CC_i as an authentication challenge to the server.

- The server:
  - Decrypts the received message: $Tb_i = E_{HPW_i}(CC_i)$.
  - Calculates a challenge for the browser: $RCS_i = E_{HPW_i}(Tb_i \oplus Ts_i)$.
  - Sends as an authentication challenge to the browser : RCS_i.

- The browser:
  - Decrypts the received message: $Tb_i \oplus Ts_i = E_{HPW_i}(RCS_i)$.
  - Calculates: $Ts_i = Tb_i \oplus Tb_i \oplus Ts_i$.
  - Calculates: $RC_i = E_{HPW_i}(Ts_i)$.
  - Sends as a response to the authentication challenge to the server: RC_i.

- The server:
  - Decrypts the received message : $Ts_i^{'} = E_{HPW_i}(RC_i)$.
  - Compares the received nonce of mutual authentication $Ts_i^{'}$ with one who sent Ts_i: $Ts_i^{'} == Ts_i$.
  - If comparison is successful, then:
    - ⋆ Mutual authentication is assured between the browser and the server.
    - ⋆ Successful Connection.

3.8.2.3 Renewal Phase

This phase is very interested and recommended especially for newly registered users. Because, it allows renewing all authentication settings in a more secure environment than registration phase. Also, it offers a higher level of protection of sensitive authentication settings (See Figure 6). In this phase, we must ensure:

- The identity of users.
- The integrity and confidentiality of regenerated salts and passwords.
- The validity of recalculated passwords.
- The mutual authentication.
- Updating of the authentication settings.

This process allows to renew the authentication settings safely. It gives another chance to users for strengthen these authentication settings.

- The browser sends the identifier ID_i of a user U_i to the server.
- The server checks the existence of the user:
  - If it exists, then:
    - ∗ Generates a new random salt RS_i^{new} and calculates a new number N_i^{new}.

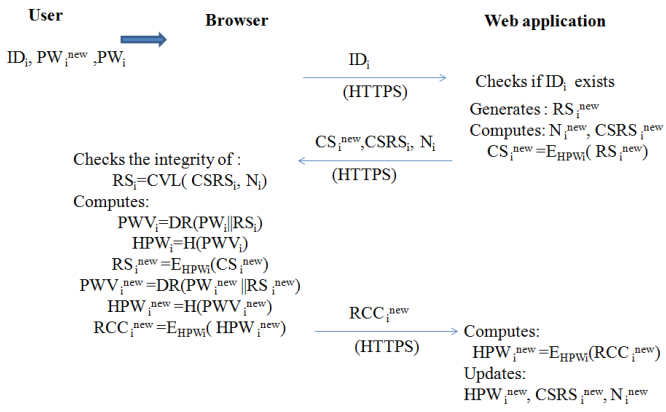


Figure 6: Renewal phase

  - ∗ Encrypts the random salt RS_i^{new} generated by the final password HPW_i of user U_i: $CS_i^{new} = E_{HPW_i}(RS_i^{new})$.
  - ∗ Sends CS_i^{new}, $CSRS_i$ and N_i to the browser.
- Otherwise, returns an error message.

- The browser:
  - Checks the integrity of $CSRS_i$ by the calculation of $RS_i = CVL(CSRS_i, N_i)$.
  - Calculates:
    - ∗ The virtual password of a user U_i by the Dynamic Rotation exercised on the concatenation of its valid original password PW_i and its random salt RS_i: $PWV_i = DR(PW_i \| RS_i)$.
    - ∗ The final password of the user U_i by hashing the virtual password PWV_i with a one-way hash function H: $HPW_i = H(PWV_i)$.
    - ∗ Decrypts the received message CS_i^{new} by the final password HPW_i calculated as a key of symmetric encryption in order to have the new random salt generated for the user U_i: $RS_i^{new} = E_{HPW_i}(CS_i^{new})$.
  - If the decryption is successful, then the server is authenticated by the client and also the confidentiality and integrity of RS_i^{new} are ensured.
  - Then, calculates:
    - ∗ The new virtual user U_i password by the dynamic rotation (DR) applied on the concatenation of its new original password valid PW_i^{new} and new random salt RS_i^{new}: $PWV_i^{new} = DR(PW_i^{new} \| RS_i^{new})$.
    - ∗ The new final password of the user U_i by hashing of the new virtual password PWV_i^{new} with an one-way hash function H: $HPW_i^{new} = H(PWV_i^{new})$.
    - ∗ The new encryption password calculated with the ancient password as symmetric encryption key: $RCC_i^{new} = E_{HPW_i}(HPW_i^{new})$.
  - Sends RCC_i^{new} as a challenge of authentication and a new final valid password to the server.

- The server:
  - Decrypts the received message in order to have the new password passes final calculated by the browser : $HPW_i^{new} = E_{HPW_i}(RCC_i^{new})$. If the decryption is successful, then, the browser is authenticated by the server. Thus, the mutual authentication of the server and of the browser is guaranteed.
  - Updates of authentication settings: HPW_i^{new}, $CSRS_i^{new}$ and N_i^{new}.

4 Security Analysis

In order to prove the degree of adaptation and robustness of our strong zero knowledge authentication proposal, we have to estimate their capacity to resist various attacks. The majority of attacks against Web applications are relied on the theft, the traceability and the weaknesses of critical data.

4.1 Defends Against Theft of Data

In companies the confidence is a range of users to preserve. More critically, the protection of data exchanged must be well protected against the theft or any other leak. In general, the space of attacks is a vast environment affects all web applications. In our proposal, we must estimate their impacts on the physical and digital security of data exchanged between the communicating entities in the following three subspaces: Client, Server and Network.

4.1.1 Client Side

In order to prevent attacks by Spyware and also to help the users who are unable to memorize of the random pass-

words. We recommend the use of ObPwd [16] that generate strong enough passwords based on the digital objects.

4.1.2 Server Side

The passwords stored in a server are strengthened by safe cryptographically random salts, are totally deformed by the dynamic rotation and their cryptographic qualities, and are assured by an one-way hash function: $HPW_i = H(DR(PW_i \| RS_i))$.

4.1.3 On the Network

In most of the existing systems of authentication passwords submission is done in plaintext or hashed. Also, for a server these passwords play the role of an original password. More critically, this process encourages attacks to sniff the network. In this situation, the attacker does not need to find the original password entered by the user. But, it suffices for him to build a script which contains the passwords intercepted on the network. Thus, to cope with this situation, we add $HTTPS$ in our proposal, and we use the passwords as key of encryption/decryption mutual authentication messages between the client and the server. Therefore, we assure the undisclosure, the untraceability and the confidentiality of the passwords that transit on the wire.

4.2 Defends Against Phishing Attacks

The phishing attack is a set of very effective attempts to data theft online. To cope with this attack, we propose the following technique:

4.2.1 A Cryptographically Safe Random Salts

To prevent the weaknesses and the problems of a salt generated from a given domain name. We propose this solution which allows to have and to verify the integrity of a random salt appropriate to each user: $CVL(CSRS_i, N_i)$. This verification can be taken to ensure the origin authentication settings. In addition, the recovery of these parameters is conditioned on the existence of a given user in order to prevent the falsification of the original sites. In this case, the attacker does not only need to create a site for acquire deceitfully the sensitive information from users, but it must answer their challenges which are impossible.

4.2.2 Mutual Authentication

In case of success of the check of the integrity of a salt. This attack rests on the hypothesis: "The password stored in the database during the recording phase will retransmit on the network". What is wrong in our proposal. The recalculated passwords never will retransmit on the wire. But, they will be used as keys of encryption of the messages of mutual authentication $E_{HPW_i}(RS_i), E_{HPW_i}(RS_i^{new}), E_{HPW_i}(Ts_i), \ldots$. For this interest, we have watched over the complexity and untraceability of generated passwords based on the cryptographic nature of regenerated random salts, dynamic rotation of binary strings generated in order to break the link between the original and virtual password and one-way hash function: $PWV_i = DR(PW_i \| RS_i)$, $HPW_i = H(PWV_i)$.

4.3 Defends Against the Shoulder Surfing

This attack is strongly related to consciousness and habits followed by users to protect their privacy especially in public spaces. But, in the case of highly sensitive web applications, we recommend the integration of the technical of password object [16]. Because, this technique allows to hide all the movements of the users and also to have very complicated passwords meeting the requirements of the computer security.

4.4 Defend Against SQL Injection

This attack presents a serious threat for the security of the dynamics of Web sites. To check well the validity and the robustness of the parameters of authentication chosen by the user. It is recommended to use the grey list and the methods of filtering (validation and cleaning) to make sure on the reliability of data. It is very effective in standard architectures which are based on a positive answer to a given request. In our proposal, we introduce a process of identification that can eliminate this problem. In reality, we propose an interactive system of authentication. More critically, the communicating entities must verify and respond to authentication challenges (for encryption / decryption nonce) to assure mutual authentication. Specifically, all responses must be confirmed by the previous challenge and accompanied by a new challenge: $Tb_i \oplus Ts_i = E_{HPW_i}(RCS_i)$, $Ts_i = Tb_i \oplus Tb_i \oplus Ts_i$, $RC_i = E_{HPW_i}(Ts_i)$. And taking into account the internal characteristic of our system, the first request allows only to verify the existence of user U_i and to get back

its own random salt. Where from, the inclusion of metacharacters in username/password fields will have no influence on the safety of user accounts. Otherwise, it will generate error messages at verification or identification of users. Consequently, our proposal resists against this attack.

4.5 Defends Against the Collisions

The proof of security of any hash functions (compression function) is measured by these capacities to resist collisions attacks (pseudo-collisions exist on the compression function in certain iteration). The domain extender algorithm defined by Merkle Damgard has known a wide range of collision attacks. The attack of extension of length which was remedied by Coron et al. [6]. Also, Joux [12] discovered the multicollision attack which looks for k internal collisions from k different messages. This vulnerability affects almost at the bottom the security of any domain extender algorithm whose internal state length equal to that cadence. But, according to Lucks [15] recommendation to remedy this problem is to increase the internal state length of the compression function to $N \geqslant 2n$ (with n is the length of the hash). In general, there are two types of attacks affecting the quality of cryptographic hash functions, namely: the probabilistic and structural attacks. In this article, we interest a improving the robustness of hash functions against probabilistic attacks. These types of attacks are based on the inability of users to choose passwords that can meet the requirements of computer security. Hence, the interest to introduce our system that is able to extend the length and to evolve the cryptographic quality of passwords. Thus, through [1] and the results obtained in Section 3.7, we deduce, on one hand, that the regenerated virtual passwords are of cryptographic nature, and on the other hand the uncorrelation, the untraceability and unpredictable of the primitive signals regenerated are assured for a weak original password. In addition, if we combine the different chosen passwords, the cryptographic quality of random salts [1], the algorithm of dynamic rotation and the robustness of an one-way hash function ($HPW_i = H(DR(PW_i \| RS_i))$ this collision problem will be actually very far.

4.6 Defends Against Man in the Middle Attack

In this technique, the attacker should be able to observe and intercept (Sniffing) the encrypted data exchanged between two victims in a valid time. It is particularly applicable in the original protocol of exchange of keys Diffie-Hellman, when it is used without authentication. In this proposed protocol, for more complexity against the attacks, we exploit the symmetric cryptographic primitives. Consequently, the attacker should intercept the connection request messages $RCC_i^{new} = E_{HPW_i}(HPW_i^{new})$ sent by a user U_i to the server and to replay the responses to the challenges of mutual authentication such as $CC_i = E_{HPW_i}(Tb_i)$,$RCS_i = E_{HPW_i}(Ts_i \oplus Tb_i)$ and $RC_i = E_{HPW_i}(Ts_i)$. But, as the attacker does not have value of HPW_i^{new}, it will be unable to replay nor connect messages nor responses to mutual authentication challenges. Thus, the resistance of our protocol is assured against this attack.

4.7 Defends Against Brute Force Attack

According to [1, 24], the resistance of the passwords against this attack is strongly bound to their complexities. The attacker should get back the file of the passwords then launch a software of brute forces "cracking" in order to test in a exhaustive way all the possible combinations of the passwords. In our proposal, the attacker does not only need to find the virtual password hashed by an one-way hash function $HPW_i = H(PWV_i)$, nevertheless, he should extract the original password which has been totally deformed in a random salt by a dynamic rotation of their concatenation $PWV_i = DR(PW_i \| RS_i)$. In addition to the cryptographic quality of the salts used [1] and according to the part 3.7, the dynamic rotation allows to break any correlation between the original and virtual passwords. Hence, we confirmed the unpredictable nature of virtual passwords generated. Therefore, the proposed protocol is secure against the attacks of brute forces.

4.8 Defends Against the Dictionary Attack

This type of attack is very effective in case of passwords with weak entropy or of authentication systems based on breakable hash functions. In our system, the cryptographic quality of the passwords is strongly bound to salts generated appropriate to every user, the dynamic rotation and the one-way hash function: $RS_i = CVL(CSRS_i, N_i)$, $PWV_i = DR(PW_i \| RS_i)$, $HPW_i = H(PWV_i)$. According to Subsection 3.6, the range of lengths of the complexity of the generated virtual passwords is $[\mathbf{2.572\ 10^{61}}, \mathbf{9.047\ 10^{74}}]$, and to Subsection 3.7,

the uncorrelation and the unpredictability of the passwords are assured for a minimal original password. Therefore, our system is actually protected against this attack.

5 Conclusion

In computer environment, the security or rather the privacy of users is the heritage of any company or organization on the wire. According to all the studies on user habits have shown their limits to meet the requirements of computer security in this discipline. In particular their incapacities to memorize random passwords. Then, they resort to habits facilitate attacks. More critical, it is impossible to rely on the users as key factors of the computer security. All these difficulties push us to the conception of a new system of authentication SAVP. This work comes in the optics to strengthen and to improve the mutual authentication of web users based on virtual passwords.

Taking account of the evolution of attacks and constraints of user systems, the cryptographic quality authentication system should not be linked to their ability to meet of the recommendations of computer security. Strongly, their consciences, their behaviors and passwords choices have very remarkable influences on the survival of their accounts. For this, web application security must be seen as an inter-connected environment requiring input from all entities constituting our system. Therefore, in our proposal, the security is required for all elements of our system. The interest is to have a system of mutual authentication based on virtual passwords capable of resisting multiple types of attacks in particular phishing, dictionary, brute force, spyware, man in the middle and replay attacks. So, we propose a strong system of authentication with zero knowledge based on:

- Salts generated by a cryptographically secure regenerator.
- An algorithm for the dynamic rotation of binary strings in order to ensure uncorrelation, unpredictability and untraceability of passwords for minimal disturbance to the initial condition.
- The symmetric cryptographic primitives for more privacy authentication settings.
- An one-way hash function, random nonce to ensure mutual authentication of communicating entities and the updating of the parameters of authentication during the renewal phase.

Generally, we can quote its characteristics as follows:

- The distribution of lengths and periods of virtual passwords generated are random and unlimited.
- The nature of virtual password generated is pseudo-random and in some situations seems chaotic.
- The untraceability and the reuse of original passwords are handled securely by integrating cryptographically secure salts algorithm and dynamic rotation of binary strings to withstand multiple types of attacks.
- The integrity of salts is assured by integration of the mechanism of CRC code of variables lengths.
- The transparency and portability of our system in all steps of executions to ensure non-occupation of the users and to hide any sensitive information can help an attacker to attack our application.
- The complexity of our system SAVP comes from the unpredictable nature of any regenerated salt.
- The simplicity in all operations building our proposal to be feasible in all programming languages.

References

[1] Y. Asimi, A. Asimi, Y. Sadqi, "New random generator of a safe cryptographic salt per session (RGSCS)," *International Journal of Network Security*, vol. 18, no. 3, pp. 445–453, May 2016.

[2] S. M. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secureAgainst dictionary attacks," in *Proceedings of IEEE Symposium on Security and Privacy (SP'92)*, pp. 72, Washington, DC, USA, 1992.

[3] J. Bonneau and S. Preibusch, "The password thicket: technical and market failures in human authentication on the web," in *The Ninth Workshop on the Economics of Information Security (WEIS'10)*, pp. 1–49, 2010.

[4] N. Chou, R. Ledesma, Y. Teraguchi, and J. Mitchell, "Client-side defense against web-based identity theft," in *Proceedings of Network and Distributed Systems Security (NDSS'04)*, pp. 1–16, 2004.

[5] R. M. Conlan and P. Tarasewich, "Improving interface designs to help users choose better passwords",

in *Extended Abstracts on Human Factors in Computing Systems (CHI'06)*, pp. 652–657, New York, USA, 2006.

[6] J. S. Coron, Y. Dodis, C. Malinaud and P. Puniya, "Merkle-damgard revisited: How to construct a hash function," in *Advances in Cryptology (CRYPTO'05)*, LNCS 3621, pp. 430–448, Springer-Verlag, 2005.

[7] D. Florncio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th ACM International Conference on World Wide Web*, pp. 657–666, 2007.

[8] P. Dourish, E. Grinter, J. D. de la Flor, and M. Joseph, "Security in the wild: User strategies for managing security as an everyday, practical problem," *Personal Ubiquitous Computing*, vol. 8, no. 6, pp. 391–401, 2004.

[9] S. Gaw and E. W. Felten, "Password management strategies for online accounts," in *Proceedings of the Second ACM Symposium on Usable Privacy and Security (SOUPS'06)*, pp. 44–55, New York, USA, 2006.

[10] S. Goldwasser, S. Micali, and C. Racko, "The knowledge complexity of interactive proof-systems," in *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing (STOC'85)*, pp. 291–304, 1985.

[11] J. A. Halderman, B. Waters, and E. Felten, "A convenient method for securely managing passwords," in *Proceedings of the 14th International World Wide Web Conference (WWW'05)*, pp. 471–479, 2005.

[12] A. Joux, "Multi-collisions in iterated hash functions. Application to cascaded constructions", in *Advances in Cryptology (CRYPTO'04)*, LNCS 3152, pp. 306–316, Springer-Verlag, 2004.

[13] L. Lamport, "Password authentication with insecure communication," *Communications of ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[14] M. Lei, Y. Xiao, S. V. Vrbsky, C. C. Li, and L. Liu, "A virtual password scheme to protect passwords," in *Proceedings of IEEE International Conference on Communications (ICC'08)*, pp. 1536–1540, 2008.

[15] S. Lucks, "A failure-friendly design principle for hash functions," in *Advances in Cryptology (ASIACRYPT'05)*, LNCS 3788, pp. 474–494, Springer-Verlag, 2005.

[16] M. Mannan and P. C. van Oorschot, *Digital Objects as Passwords*, Carleton University, Canada, July 14, 2008.

[17] B. Miller, L. Huang, A. D. Joseph, J. D. Tygar, "I know why you went to the clinic: risks and realization of https traffic analysis," in *14th International Symposium on Privacy Enhancing Technologies (PETS'14)*, pp. 143–163, 2014.

[18] R. Morris and K. Thompson, "Password security: A case history," *Communications of ACM*, vol. 22, no. 11, pp. 594–597, 1979.

[19] G. Notoatmodjo and C. Thomborson, "Passwords and perceptions," in *Seventh Australasian Information Security Conference (AISC'09)*, pp. 71–78, Wellington, New Zealand, 2009.

[20] N. Ojha and S. Padhye, "Cryptanalysis of multi prime RSA with secret key greater than public key", *International Journal of Network Security*, vol. 16, no. 1, pp. 53–57, Jan. 2014.

[21] A. Prakash, "A biometric approach for continuous user authentication by fusing hard and soft traits", *International Journal of Network Security*, vol. 16, no. 1, pp. 65–70, Jan. 2014.

[22] S. Riley, "Password security: What users know and what they actually do," *Usability News*, vol. 8, no. 1, pp. 2833–2836, 2006.

[23] B. Ross, C. Jackson, N. Miyake, D. Boneh, J. C. Mitchell, "Stronger password authentication using browser extensions", in *Proceedings of Usenix Security*, pp. 17-32, 2005.

[24] T. Rowan, "Password protection: The next generation," *Network Security*, vol. 2009, no. 2, pp. 4–7, Feb. 2009.

[25] A. Rukhin, et al., *A Statistical Test Suite for Random and Pseudorandom Number Generators For Cryptographic Applications*, NIST Special Publication 800-22, Apr. 2010.

[26] Y. Sadqi, A. Asimi, A. Younes, "Short: A lightweight and secure session management protocol", in *The Second International Conference of NETworked sYStems (NETYS'14)*, LNCS 8593, pp. 319–323, Springer-Verlag, 2014.

[27] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: User attitudes and behaviors," in *Proceedings of the Sixth ACM Symposium on Usable privacy and Security (SOUPS'10)*, Article no. 2, 2010.

[28] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong, "Password sharing: Implications for security design based on social practice," in *Proceedings of ACM SIGCHI Conference on Human Factors*

in Computing Systems (CHI'07), pp. 895–904, New York, USA, 2007.

[29] S. K. Sood, A. K. Sarje, and K. Singh, "Inverse cookie-based virtual password authentication protocol", *International Journal of Network Security*, vol. 13, no. 2, pp. 98–108, Sept. 2011.

[30] B. Tanti, N. Doshi, "A secure email login system using virtual password," Cryptology ePrint Archive, Report 1009.5729, 2010. (`http://eprint.iacr.org/2010/481.pdf`)

[31] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password authentication schemes: Current status and key issues", *International Journal of Network Security*, vol. 3, no. 2 , pp. 101–115, Sept. 2006.

[32] D. Weirich and M. A. Sasse, "Pretty good persuasion: A first step towards effective password security in the real world," in *Proceedings of the 2001 ACM Workshop on New Security Paradigms*, pp. 137–143, New York, NY, USA, 2001.

Younes ASIMI received his Master's degree in Computer Science and Distributed Systems in 2012 from Departments of Mathematics and Computer Sciences, Faculty of Science, University Ibn Zohr, Agadir,Morocco. He is currently pursuing Ph.D in Departments of Mathematics and Computer Sciences, Information Systems and Vision Laboratory,Morocco. His research interests include Authentication Protocols, Computer and Network Security and Cryptography.

Abdallah AMGHAR is a Professor in the Physics Department, Faculty of Science, University Ibn Zohr,Morocco. He received his DEA and DES degree in 1994 from Department of Physics, Faculty of Science, University Hassan II, Morocco. In January 2002, he has Ph.D degree in microelectronic from Department of Physics, Faculty of Science, University Ibn Zohr, Morocco. His areas of research interests include Cryptography, DNT, embedded systems and microelectronic.

Ahmed ASIMI received his PhD degree in Number theory from the University Mohammed V - Agdal in 2001. His research interest includes Number theory, Code theory, and Computer Cryptology and Security. He is a full professor at the Faculty of Science at Agadir since 2008.

Yassine SADQI received his Master in the field of Computer Science and Distributed Systems at the Ibn Zoher University in 2012. He is currently a Ph.D. candidate of the Ibn Zoher University, Agadir, Morocco. His main field of research interest is computer security, cryptography and authentication in Web applications.

An Integratable Verifiable Secret Sharing Mechanism

Yanjun Liu[1,2] and Chin-Chen Chang[2,3]
(Corresponding author: Chin-Chen Chang)
Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education,
School of Computer Science and Technology, Anhui University[1]
No. 111 Jiulong Rd., Hefei 230601, China
Department of Computer Science and Information Engineering, Asia University[2]
No. 500, Lioufeng Rd., Wufeng, Taichung 413, Taiwan
Department of Information Engineering and Computer Science, Feng Chia University[3]
No. 100 Wenhwa Rd., Seatwen, Taichung 407, Taiwan
(Email: alan3c@gmail.com)
(Received Nov. 26, 2013; revised and accepted Mar. 5 & May 13, 2014)

Abstract

Threshold secret sharing (SS), also denoted as (t, n) SS, has been used extensively in the area of information security, such as for group authentication, cloud storage schemes, secure parallel communication and wireless multipath routing protocols. However, a (t, n) SS cannot detect any deceptions among the dealer and shareholders. Verifiable secret sharing (VSS) overcomes the weakness of (t, n) SS in such a way that it is able to detect cheaters by verifying the validity of shares or the correctness of the recovered secret under the condition that both shares and the secret are not compromised. Recently, two non-interactive VSSs based on Asmuth-Bloom's SS were proposed by Harn et al. and Liu et al., respectively. Both VSSs require shareholders to examine the range of values of some integers related to the secret before recovering the secret, which is a time-consuming operation. In this paper, we propose a novel integratable VSS mechanism that integrates the concepts of the generalized Chinese remainder theorem (GCRT), Shamir's SS and Asmuth-Bloom's SS. Our proposed VSS can verify that the secret reconstructed by any t or more shareholders is the same as the one that the dealer has generated. Analysis shows that our proposed VSS can provide perfect secrecy and better efficiency.

Keywords: Generalized Chinese remainder theorem (GCRT), hash function, secret sharing (SS), verifiable secret sharing (VSS)

1 Introduction

Threshold secret sharing (SS) [1, 3, 6, 9, 10, 11, 12, 20, 21, 22, 23, 25, 26] is a widely-used cryptographic mechanism for managing a secret or a key among a set of participants. A threshold SS is also denoted as a (t, n) SS in which a dealer does not release the secret itself, but divides the secret into n shares that are distributed among n shareholders. By using a specific algorithm, any subset of t shares can recover the original secret. There are two security goals that a (t, n) SS should achieve: 1) the secret can be recovered by any t or more than t shares; and 2) the secret cannot be determined by fewer than t shares.

Shamir's (t, n) SS [25] is the first (t, n) SS and was proposed in 1979. It is based on the Lagrange interpolating polynomial and can ensure perfect secrecy. Perfect secrecy means that even if no computational assumption is made, both security goals can still be achieved. Later in 1983, Mignotte [22] introduced another (t, n) SS that is based on the Chinese remainder theorem (CRT) [5, 9, 20]. Mignotte's (t, n) SS generates a particular integer sequence and selects the secret in the t-threshold range [11, 12, 21]. According to the sequence, any t or more than t shares can recover the secret by using the CRT. However, Mignotte's (t, n) SS is not perfectly secure since it cannot accomplish the second security goal. In the same year, Asmuth and Bloom [1] proposed an enhanced version of Mignotte's (t, n) SS which can guarantee perfect secrecy. Nowadays, Shamir's (t, n) SS, Mignotte's (t, n) SS and Asmuth-Bloom's (t, n) SS have become fundamental tools applied in many areas of information security, such as for key distribution protocols, group authentication, cloud storage schemes, secure parallel communication and multipath routing protocols in wireless networks [6, 9, 10, 20, 23, 26].

A (t, n) SS assumes that the dealer and shareholders are all honest, but this is not always the case. There-

fore, the weakness of a (t, n) SS is that it cannot discover whether the dealer has transmitted inconsistent shares to shareholders or whether shareholders have released invalid shares when recovering the secret. An incorrect secret may be reconstructed without detection in these two cases. In order to overcome this weakness, in 1985, Chor et al. [7] introduced the concept of verifiable secret sharing (VSS). Verifiability is the property of detecting cheaters by verifying the validity of shares or the correctness of the recovered secret under the condition that both the shares and the secret are not compromised. Interactive and non-interactive VSSs are two types of VSS. Interactive VSSs require shareholders to interact with the dealer to execute the verification, which consumes a large amount of communication time. To reduce the communication cost, non-interactive VSSs have been proposed to replace interactive VSSs.

VSS expands the range of applications of SS and has been researched deeply in a great number of recently published literature [2, 8, 11, 12, 13, 14, 21, 24]. Benaloh [2] defined the concept of t-consistency and proposed an interactive VSS to verify that shares generated by the dealer are t-consistent (i.e. any subset of t shares defines the same secret). Feldman [8] proposed the first non-interactive VSS using encrypted functions. The security of Feldman's VSS depends on the hardness of solving the discrete logarithm. Qiong et al. [24] and Iftene [13] presented non-interactive VSSs based on Asmuth-Bloom's SS and Mignotte's SS, respectively. Kaya et al. [14] pointed out the security weaknesses in these two VSSs and developed a VSS based on Asmuth-Bloom's SS. Harn and Lin [11] extended a (t, n) VSS to a (n, t, n) VSS in which each shareholder also acts as a dealer. Based on Benaloh's VSS [2], their VSS can verify that shares satisfy the requirement of strong t-consistency. In 2013, Harn et al. [12] proposed a non-interactive VSS based on Asmuth-Bloom's SS in which additional verification secrets are used during the verification. Later, Liu et al. [21] proposed a more efficient VSS by also using Asmuth-Bloom's SS as a building block. Both VSSs require shareholders to examine the range of values of some integers related to the secret before recovering the secret, which is a time-consuming operation.

In this paper, we propose a novel integratable VSS mechanism based on the generalized Chinese remainder theorem (GCRT) [4, 15, 16, 17, 18, 19]. Our proposed VSS can verify that the secret reconstructed by any t or more shareholders is the same as the one that the dealer has generated. The contributions of our proposed VSS are listed below:

1) Our proposed VSS integrates the concepts of Shamir's SS, Asmuth-Bloom's SS, and GCRT. To the best of our knowledge, no research on VSS has adopted this approach. Thus, we are the first to combine these three fundamental elements in a VSS.

2) A one-way hash function is used to verify the correctness of the secret, thereby removing the operation of examining the range of values of additional integers.

3) Our proposed VSS can provide perfect secrecy.

4) Our proposed VSS simplifies two related works [12, 21] on VSS and achieves better efficiency.

The rest of this paper is organized as follows. Section 2 addresses some background knowledge related to VSS. Our proposed VSS is described in Section 3. Section 4 gives security and performance analyses of our proposed VSS. Finally, conclusions appear in Section 5.

2 Preliminaries

This section introduces some background knowledge related to VSS. We first introduce two famous SSs: Shamir's [25] and Asmuth-Bloom's (t, n) SS [1]. Then, we address the principle and features of the GCRT [4, 15, 16, 17, 18, 19]. Finally, we review two recently developed VSSs [12, 21].

2.1 Shamir's (t, n) SS

Shamir's (t, n) SS [25] is one of the most famous SSs, which is based on the Lagrange interpolating polynomial. Shamir's (t, n) SS has been adopted widely in the design of VSSs since it was proposed in 1979. Assume that there is one dealer D and n users $U = \{u_1, u_2, ..., u_n\}$. Dealer D first generates a secret s and divides it into n shares, and then issues these shares to n users secretly, in such a way that each user obtains one share. To achieve the objective that any t users (also called shareholders) can collaborate with each other by using their shares to recover the secret s generated by dealer D, Shamir's (t, n) SS executes the following two phases as follows.

Share Generation:

Step 1. Dealer D randomly selects a polynomial $g(x)$ of degree t-1: $g(x) = s+a_1x+a_2x^2+...+a_{t-1}x^{t-1} \bmod p$, where $s = g(0)$ is the secret, and t coefficients $s, a_1, a_2, ..., a_{t-1}$ are in the finite field $GF(p)$.

Step 2. Dealer D generates n shares $s_i = g(x_i)$ for $i = 1, 2, ..., n$, where x_i can be considered as some information of shareholder u_i, such as u_i's ID number.

Step 3. Dealer D sends share s_i to shareholder u_i in a private channel.

Secret Reconstruction:

Any t shareholders can use their received shares to reconstruct the secret s generated by dealer D. Supposing that $s_{lj} \in \{s_1, s_2, ..., s_n\}$ for $j = 1, 2, ..., t$ denote shares of t shareholders, secret s can be reconstructed by computing $s = g(0) = \sum_{j=1}^{t} g(x_{lj}) \prod_{m=1, m\neq j}^{t} \frac{x_{lm}}{x_{lm}-x_{lj}} \bmod p$.

According to these two phases, parameter t is usually regarded as a threshold value that defines the fewest number of shares for recovering the secret. Shamir's (t, n) SS

is quite simple and can ensure perfect secrecy. Due to this merit in security, Shamir's (t, n) SS has become a practical tool in realizing secret sharing and a common building block in VSSs.

2.2 Asmuth-Bloom's (t, n) SS

Different from Shamir's (t, n) SS that is based on the Lagrange interpolating polynomial, Asmuth and Bloom [1] proposed a novel SS based on the CRT. Asmuth-Bloom's (t, n) SS can also provide perfect secrecy, which has gathered increasing attention in VSS research. If a dealer D and n shareholders $U = \{u_1, u_2, ..., u_n\}$ participate in this SS, it can be described as follows.

Share Generation:

Step 1. Dealer D selects $n+1$ pairwise, co-prime integers, $p_0, p_1, p_2, ..., p_n$, that satisfy two requirements, i.e., $p_1 < p_2 < ... < p_n$ and $p_0 \cdot p_{n-t+2} \cdot p_{n-t+3} \cdot ... \cdot p_n < p_1 \cdot p_2 \cdot ... \cdot p_t$.

Step 2. Dealer D generates an integer s as the secret such that $0 \leq s < p_0$.

Step 3. Dealer D generates another integer $A = s + bp_0$, where b is an arbitrary integer such that $0 \leq A < \prod_{i=1}^{t} p_i$.

Step 4. Dealer D creates n shares $s_i = A(\mathrm{mod} p_i)$ for $i = 1, 2, ..., n$, and then sends s_i to shareholder u_i in a private channel.

Secret Reconstruction:

Any t shareholders can use their received shares to reconstruct secret s generated by dealer D. Supposing that $s_{lj} \in \{s_1, s_2, ..., s_n\}$ for $j = 1, 2, ..., t$ denote shares of t shareholders, the secret s can be reconstructed according to the following steps:

Step 1. Integer A is recovered by using the CRT. First, the following system of equations is constructed:

$$s_{l1} = A(\mathrm{mod} p_{l1}),$$

$$s_{l2} = A(\mathrm{mod} p_{l2}),$$

$$\vdots$$

$$s_{lt} = A(\mathrm{mod} p_{lt}).$$

Then, the unique integer A can be computed as $A = \sum_{j=1}^{t} M_j \cdot M_j^{'} \cdot s_{lj} (\mathrm{mod} P)$, where $P = \prod_{j=1}^{t} p_{lj}$, $M_j = \frac{P}{p_{lj}}$, and $M_j \cdot M_j^{'} \equiv 1 (\mathrm{mod} p_{lj})$.

Step 2. Secret s is reconstructed by computing $s = A(\mathrm{mod} p_0)$.

However, Harn et al. [12] pointed out that if integer A selected by dealer D is in the range of $[0, p_1 \cdot p_2 \cdot ... \cdot p_t)$, Asmuth-Bloom's (t, n) SS is actually not perfectly secure. This is because in this case, secret s could be recovered by fewer than t shares, which indicates that both security goals cannot be fulfilled at one time. Harn et al. modified Asmuth-Bloom's (t, n) SS by confining A in a smaller range, $(p_{n-t+2} \cdot p_{n-t+3} \cdot ... \cdot p_n, p_1 \cdot p_2 \cdot ... \cdot p_t)$. They called this range as the ***t-threshold range*** [12] and denoted it as $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot ... \cdot p_n, p_1 \cdot p_2 \cdot ... \cdot p_t}$. They proved that only if A is selected in the t-threshold range, Asmuth-Bloom's (t, n) SS can ensure perfect secrecy.

2.3 Generalized Chinese Remainder Theorem (GCRT)

The generalized Chinese remainder theorem (GCRT) is an extension of CRT that adds a parameter k into the theorem. GCRT uses the following basic elements:

1) n positive integers, $x_1, x_2, ..., x_n$;

2) n positive, pairwise, co-prime integers, $p_1, p_2, ..., p_n$;

3) an integer k satisfying $\mathrm{Max}\{x_i\}_{1 \leq i \leq n} < k < \mathrm{Min}\{p_i\}_{1 \leq i \leq n}$.

To build the system of equations below:

$$x_1 = \lfloor X/p_1 \rfloor (\mathrm{mod} k),$$

$$x_2 = \lfloor X/p_2 \rfloor (\mathrm{mod} k),$$

$$\vdots$$

$$x_n = \lfloor X/p_n \rfloor (\mathrm{mod} k).$$

From the GCRT, the unique integer X can be computed as $X = \sum_{i=1}^{n} N_i \cdot N_i^{'} \cdot B_i (\mathrm{mod} k \cdot P)$, where $P = \prod_{i=1}^{n} p_i$, $N_i = k \cdot \frac{P}{p_i}$, $N_i \cdot N_i^{'} \equiv k (\mathrm{mod} k \cdot p_i)$, and $B_i = \lceil \frac{x_i \cdot p_i}{k} \rceil$.

The GCRT can accomplish the same functionality as the CRT. However, the flexibility of the GCRT is better than the CRT due to the use of integer k. In the GCRT, only a change of k can generate a new integer X. On the contrary, if integer X needs to be updated, all parameters, such as $x_1, x_2, ..., x_n$, and $p_1, p_2, ..., p_n$, need to be modified. Therefore, the GCRT is regarded as an enhanced version of the CRT and it has been extensively applied in the fields of cryptography. As stated in Subsection 2.2, the CRT is used to recover the secret in Asmuth-Bloom's (t, n) SS. In 2012, Guo and Chang [9] analyzed the correctness of Asmuth-Bloom's (t, n) SS based on the GCRT. Inspired by their approach, we will use the GCRT-based Asmuth-Bloom's (t, n) SS as one of the building blocks of our novel VSS.

2.4 Review of Related VSS Work

In this subsection, we review two VSSs, one by Harn et al. [12] and the other by Liu et al. [21]. Both VSSs can verify whether the shares received by shareholders are consistent under the condition that the secrecy of both shares and the secret are not compromised. Their common characteristics are listed below:

1) Both VSSs rely on the assumption that dealer D may transmit a fake share to a shareholder; however, all shareholders behave honestly;

2) They are based on Asmuth-Bloom's (t, n) SS that depends on the CRT;

3) In the verification, all shareholders work together to verify that their shares are t-threshold consistent [12] by examining the range of values of some integers related to secret s;

4) They can verify all shareholders' shares simultaneously and conclude whether there exist any invalid shares, but invalid shares cannot be identified.

Next, we investigate the detailed processes of these two VSSs, respectively. In Harn et al.'s VSS, dealer D generates secret s and n shares according to Asmuth-Bloom's (t, n) SS. Moreover, the dealer selects additional r secrets (also called ***verification secrets***) in the t-threshold range and creates their corresponding shares. Afterwards, the dealer distributes one share of the secret s along with one share of each verification secret to each shareholder u_i secretly. In order to verify the validity of shares, shareholders should first open (recover) $r/2$ verification secrets and inspect whether they are in the t-threshold range. If this holds, it indicates that the remaining, unopened $r/2$ verification secrets are also in the t-threshold range. Based on $(r/2+1)$ shares owned by each shareholder, the liner combinations of secret s and each unopened verification secret can be recovered by using the CRT. If the recovered values are in a certain range [12], the secret can be proven as in the t-threshold range, thereby verifying the t-threshold consistency of shares. If the verification is passed, any t or more than t shareholders can reconstruct secret s by using the CRT; otherwise, shareholders require that the dealer redistribute shares.

In comparison, Liu et al.'s VSS is an improvement over that proposed by Harn et al. It uses a similar, but simpler method to accomplish share verification. In Liu et al.'s VSS, each shareholder generates an adjustment value instead of receiving r verification secrets as in Harn et al.'s VSS. All shareholders combine their shares with adjustment values to recover an integer that has a relationship with secret s by using the CRT. Consequently, this strategy saves considerable time by eliminating the recovery of opened and unopened verification secrets. If the recovered integer is in the modified t-threshold range, the secret is proven to be in the t-threshold range, thereby verifying the t-threshold consistency of shares. In addition, the process of secret reconstruction in Liu et al.'s VSS is the same as that in Harn et al.'s VSS. According to the performance analysis in [21], Liu et al.'s VSS reduces both computational and communication costs.

3 Our Proposed VSS Mechanism

In this section, we first discuss the motivations for improving the two previously described VSSs, and then propose an integratable VSS that is based on the concepts of Shamir's SS, Asmuth-Bloom's SS, and the GCRT.

3.1 Motivations

In Subsection 2.4, we described the main properties of Harn et al.'s VSS [12] and Liu et al.'s VSS [21]. In these two VSSs, share verification and secret reconstruction are two separate phases. In the share verification, all shareholders must collaborate with each other to recover some integers that have a relationship with the secret. Then the range of value of the recovered integer is investigated to ensure the validity of shares. If the verification is passed, it implies that each shareholder received a correct share from the dealer. Thus, t distinct shares can reconstruct the real secret. However, if the verification is not passed, there is no need to reconstruct the secret and the VSS stops at this point.

From the process in these two VSSs, it can be inferred that an integer related to the secret and the secret itself must be reconstructed by the CRT in the share verification and the secret reconstruction, respectively, if the shareholder shares are valid. These are two time-consuming operations where the efficiency can be improved. In fact, the phases of share verification and secret reconstruction can be integrated into a single phase that verifies whether the secret reconstructed by any t or more shareholders is the same as the one that the dealer has generated. Therefore, the validity of shares can also be verified without recovering another integer before secret reconstruction. This strategy can increase the efficiency to some extent. Moreover, the two previously proposed VSSs can only detect the cheating behavior of the dealer based on the assumption that all shareholders act honestly. This can be improved to detect the honesty of either the dealer or any shareholder.

3.2 Proposed VSS

Inspired by the VSSs presented by Harn et al. and Liu et al., we propose a novel integratable VSS that improves on their work. The word "integratable" means that the proposed mechanism integrates three fundamental methods used in secret sharing: Shamir's SS, Asmuth-Bloom's SS and the GCRT. In the following, we first address the model of our design and then give the detailed VSS mechanism.

Like the two previously discussed VSSs, our proposed VSS involves two parties: a dealer D and n shareholders $U = \{u_1, u_2, ..., u_n\}$. Dealer D generates a secret

s and divides it into n shares that are shared among n shareholders. t or more shareholders are responsible for reconstructing secret s. However, dealer D may deceive shareholders and deliver an invalid share to a shareholder. On the other hand, shareholders may also act dishonestly by releasing invalid shares when performing the reconstruction of secret s. Consequently, our proposed VSS must be able to verify the correctness of the reconstructed secret to check whether there exists any deception among either the dealer or shareholders.

In our proposed VSS, dealer D selects the secret s and then computes a one-way hash function $k = h(s)$. The hash code k is used as a parameter in the GCRT and n shares of the secret s are generated by the approach used in the GCRT-based Asmuth-Bloom (t, n) SS. In addition, dealer D constructs a Shamir (t, n) SS scheme in which the dealer selects a polynomial $g(x)$ of degree t-1 such that $g(0) = k$. Then, dealer D distributes shares of s and shares of k to shareholders. After receiving all the messages sent by dealer D, t shareholders recover k and then use k to recover the secret s via the GCRT. In the end, we check whether $h(s)$ is equal to the recovered k. If it is true, shareholders can conclude that the recovered secret s is identical to the real secret generated by the dealer.

Our proposed VSS consists of two phases, a setup phase and a verification phase. Figure 1 illustrates the flowchart of the setup phase and the detailed steps are presented as follows.

Setup Phase:

Step 1. Dealer D selects n+1 pairwise, co-prime integers, p_0, p_1, p_2, ..., p_n, that satisfy two requirements: (1) $p_0 < p_1 < p_2 < ... < p_n$, and (2) $p_0 \cdot p_{n-t+2} \cdot p_{n-t+3} \cdot ... \cdot p_n < p_1 \cdot p_2 \cdot ... \cdot p_t$.

Step 2. Dealer D generates the secret s such that $0 \leq s < p_0$.

Step 3. Dealer D computes $k = h(s)$, where h is a collision-free, one-way hash function and $0 < k < \text{Min}\{p_i\}_{1 \leq i \leq n}$.

Step 4. Dealer D generates an integer $A = s + bp_0$, where b is an arbitrary integer which should make sure that $A \in Z_{k \cdot p_{n-t+2} \cdot p_{n-t+3} \cdot ... \cdot p_n, k \cdot p_1 \cdot p_2 \cdot ... \cdot p_t}$.

Step 5. Dealer D creates n shares $s_i = \lfloor A/p_i \rfloor (\text{mod} k)$ for $i = 1, 2, ..., n$.

Step 6. Dealer D selects a polynomial $g(x)$ of degree t-1: $g(x) = k + a_1 x + a_2 x^2 + ... + a_{t-1} x^{t-1} \text{mod} q$, where $k = g(0)$ and t coefficients $k, a_1, a_2, ..., a_{t-1}$ are in the finite field $GF(q)$.

Step 7. Dealer D generates n shares of k as $s_i^{'} = g(x_i)$ for $i = 1, 2, ..., n$.

Step 8. Dealer D sends s_i and $s_i^{'}$ to shareholder u_i in a private channel.

Verification Phase:

Assume that $u_{l1}, u_{l2}, ..., u_{lt} \in U$ are t shareholders and shareholder u_{lj} $(j = 1, 2, ..., t)$ received s_{lj} and $s_{lj}^{'}$ in the setup phase.

Step 1. $u_{l1}, u_{l2}, ..., u_{lt}$ use $s_{l1}^{'}, s_{l2}^{'}, ..., s_{lt}^{'}$ to recover k following Shamir's (t, n) SS.

Step 2. u_{lj} uses s_{lj}, p_{lj}, and the recovered k to release $C_j = N_{lj} \cdot N_{lj}^{'} \cdot B_{lj} (\text{mod} k \cdot P^{'})$, where $P^{'} = \prod_{j=1}^{t} p_{lj}$, $N_{lj} = k \cdot \frac{P^{'}}{p_{lj}}$, $N_{lj} \cdot N_{lj}^{'} \equiv k (\text{mod} k \cdot p_{lj})$, and $B_{lj} = \lceil \frac{s_{lj} \cdot p_{lj}}{k} \rceil$.

Step 3. $u_{l1}, u_{l2}, ..., u_{lt}$ work together to compute $A = \sum_{j=1}^{t} C_j (\text{mod} k \cdot P^{'})$ following the GCRT. Then, the secret s is reconstructed by computing $s = A (\text{mod} p_0)$.

Step 4. Check whether $h(s)$ is equal to k. If these two values are identical, we can conclude that the reconstructed secret s is correct; otherwise, the reconstructed s is not a valid value.

Remark 1. *In the setup phase, dealer D needs to generate two secret messages: s and k. s is the real secret needed to recover and k is used to verify the correctness of s. More specifically, k has multiple functionalities that can be described as follows: (1) Dealer D makes k as the hash code of the one-way hash function h(s) in the setup phase. (2) k is an important parameter in the GCRT to generate shares of secret s as* $s_i = \lfloor A/p_i \rfloor (mod k)$. *Later, shareholders will use their shares and k to recover s according to the GCRT-based Asmuth-Bloom (t, n) SS. (3) To increase the degree of security, dealer D does not transmit k directly to shareholders, but establishes Shamir's (t, n) SS scheme in which k is considered as the secret. Then, in the verification phase, shareholders can recover k easily according to the method of Shamir's (t, n) SS. (4) We can check whether h(s) is equal to k to verify the correctness of the recovered secret s. In summary, the use of k provides an additional level of security for our proposed VSS.*

Remark 2. *The verification phase of our proposed VSS can verify that the recovered secret s is identical to the real secret generated by the dealer. This verification process is completed by the one-way hash function h(s). Thus, it is unnecessary to recover some integers related to the secret and to examine the range of this integer like in the two VSSs mentioned before. This can simplify the verification process. Furthermore, if the verification fails, we can conclude that either the dealer or the shareholder is dishonest. However, it is impossible to identify two situations: (1) the dealer sends invalid shares to shareholders; and (2) shareholders release invalid shares to recover the secret. Lastly, similar to Harn et al. and Liu et al.'s VSSs, our proposed VSS can verify all shares at one time.*

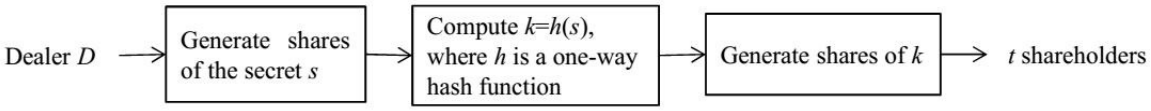


Figure 1: Flowchart of the setup phase

4 Security and Performance Analyses

In this section, we first give security analysis of our proposed VSS, and then compare the performance among our proposed VSS and two other VSSs.

4.1 Security Analysis

Now we analyze that our proposed VSS can provide perfect secrecy. Our proposed VSS uses Shamir's (t, n) SS to share k among n shareholders, and later, t shareholders recover k and use it in the GCRT to recover secret s. Since Shamir's (t, n) SS is perfectly secure, fewer than t shares cannot recover k. Therefore, secret s cannot be recovered from fewer than t shares. Moreover, each shareholder u_{lj} releases a value $C_j = N_{lj} \cdot N_{lj}^{'} \cdot B_{lj} (\mathrm{mod} k \cdot P^{'})$, which combines s_{lj}, p_{lj}, and k. Thus, hidden in the value of C_j, share s_{lj} cannot be compromised during the verification phase.

In the following, we will analyze a situation where even if k is compromised, our proposed VSS is still perfectly secure, since fewer than t shareholders cannot obtain any useful information about secret s. Firstly, if fewer than t shareholders know the value of k, they cannot obtain secret s from $h(s) = k$ due to the intrinsic characteristic of the hash function. Next, we will prove that fewer than t shareholders cannot recover secret s from the GCRT.

Assume that $u_{l1}, u_{l2}, ..., u_{l(t-1)}$ are t-1 shareholders and each shareholder u_{lj} receives share s_{lj}. According to the GCRT, these t-1 shareholders cooperate to compute an integer $A^{'} = \sum_{j=1}^{t-1} N_{lj} \cdot N_{lj}^{'} \cdot B_{lj} (\mathrm{mod} k \cdot P^{''})$, where $P^{''} = \prod_{j=1}^{t-1} p_{lj}$, $N_{lj} = k \cdot \frac{P^{''}}{p_{lj}}$, $N_{lj} \cdot N_{lj}^{'} \equiv k (\mathrm{mod} k \cdot p_{lj})$, and $B_{lj} = \lceil \frac{s_{lj} \cdot p_{lj}}{k} \rceil$. However, $A^{'}$ is not equal to the real secret A since the range of $A^{'}$ is $Z_{k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{t-1}}$, which is quite different from that of A as $Z_{k \cdot p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n, k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_t}$. Consequently, fewer than t shareholders cannot reconstruct the secret directly by using the GCRT. However, this does not mean fewer than t shareholders cannot obtain the real secret A from the recovered $A^{'}$. The use of GCRT implies that A and $A^{'}$ have a relation as $A = A^{'} + \varphi \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{t-1}$. Thus, A can be computed from $A^{'}$ if φ can be determined by fewer than t shareholders. Unfortunately, it is very hard to determine the correct φ. This is because $(p_1 \cdot p_2 \cdot \ldots \cdot p_t - p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n) / p_1 \cdot p_2 \cdot \ldots \cdot p_{t-1} > p_0$ values of φ can make $A^{'} + \varphi \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{t-1}$ in the range of $Z_{k \cdot p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n, k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_t}$, but only one value of $A^{'} + \varphi \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{t-1}$ is equal to A. Therefore, the probability of finding the exact value of φ is not greater than the probability of guessing the secret A. Based on this security analysis, our proposed VSS ensures perfect security based on the fact that fewer than t shareholders cannot obtain the real secret A from the recovered $A^{'}$.

4.2 Performance Analysis

In this section, we provide performance analysis of our proposed VSS and compare it with the other two related VSSs [12, 21] in terms of computational and communication costs.

Now we analyze the computational cost. In the setup phase, Harn et al.'s VSS creates and distributes shares of the real secret and r additional verification secrets to n shareholders. In contrast, the VSS by Liu et al. and our proposed VSS do not need to generate verification secrets. The difference between our VSS and Liu et al.'s VSS is that our VSS generates an additional polynomial of degree t-1 according to Shamir's SS. In the verification phase of the other two VSSs, n shareholders need to first cooperate to recover one or several integers related to the secret, and then t out of n shareholders recover the real secret, both by using the CRT. [21] analyzes that the time complexity of the VSSs proposed by Harn et al. and Liu et al. are $O(rn^2d^2)$ and $O(n^2d^2)$, respectively, where d is the number of bits of p_i and r is the number of verification secrets.

In comparison, in the verification phase of our proposed VSS, t out of n shareholders first recover the secret k in Shamir's (t, n) SS and then reconstruct the real secret with the recovered k by the GCRT. The time complexity of recovering k is $O(t \log^2 t)$ [25] and the time complexity of recovering the real secret is analyzed as follows. Secret A is computed as $A = \sum_{j=1}^{t} N_{lj} \cdot N_{lj}^{'} \cdot B_{lj} (\mathrm{mod} k \cdot P^{'})$ by the GCRT, where $P^{'} = \prod_{j=1}^{t} p_{lj}$, $N_{lj} = k \cdot \frac{P^{'}}{p_{lj}}$, $N_{lj} \cdot N_{lj}^{'} \equiv k (\mathrm{mod} k \cdot p_{lj})$, and $B_{lj} = \lceil \frac{s_{lj} \cdot p_{lj}}{k} \rceil$. Assume that d is the number of bits of both the operands, p_{lj} and k. Considering that $k \cdot P^{'}$ and $N_{lj} \cdot N_{lj}^{'}$ can be computed offline, this computational process totally contains (t-1) additions, t divisions, $2t$ multiplications, and one modular operation. Therefore, the number of bit operations required is $(t-1) \times d + t \times d^2 + 2t \times d^2 + ((t+1) \times d)^2$, and the time complexity is $O(t^2 d^2)$.

Tables 1 and 2 summarize the communication and computational costs of our proposed VSS and the other two VSSs [12, 21]. From the comparisons among these VSSs, we can imply that our proposed VSS has better compu-

Table 1: Comparison of communication cost in setup phase

Scheme	Dealer sends messages	Each u_i sends messages	Each u_i receives messages
VSS in [12]	$n(r+1)$	-	$r+1$
VSS in [21]	n	-	1
Our VSS	$2n$	-	2

tational efficiency than the other two VSSs and our communication efficiency is also satisfactory.

Table 2: Comparison of computational cost

Scheme	Setup phase	Verification phase
VSS in [12]	$O(rn)$	$O(rn^2d^2)$
VSS in [21]	$O(n)$	$O(n^2d^2)$
Our VSS	$O(n)$	$O(t^2d^2)$

Note: n is the number of shares; d is the number of bits of operands; and r is the number of verification secrets.

5 Conclusions

In the paper, we propose a novel integratable VSS mechanism that integrates the concepts of the generalized Chinese remainder theorem (GCRT), Shamir's SS and Asmuth-Bloom's SS. Our proposed VSS improves Harn et al.'s VSS and Liu et al.'s VSS by using a one-way hash function to verify the correctness of the secret. While maintaining the advantages of the other two related VSSs, our proposed VSS is more efficient. In addition, we proved that our proposed VSS is perfectly secure.

Acknowledgments

This research was supported in part by the National Nature Science Foundation of China (grant number: 61202228) and the College Natural Science Key Project of Anhui Province of China (grant number: KJ2012A008). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. IT-29, no. 2, pp. 208–210, 1983.

[2] J. C. Benaloh, "Secret sharing homomorphisms: Keeping shares of a secret," in *Advances in Cryptology (Crypto'86)*, pp. 251–260, Santa Barbara, USA, August 1986.

[3] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of American Federation of Information Processing Societies National Computer Conference*, pp. 313–317, New York, USA, June 1976.

[4] C. C. Chang and Y. P. Lai, "A fast modular square computing method based on the generalized `Chinese` remainder theorem for prime module," *Applied Mathematics and Computation*, vol. 161, no. 1, pp. 181–194, 2005.

[5] C. C. Chang, J. S. Yeh, and J. H. Yang, "Generalized `Aryabhata` remainder theorem," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 4, pp. 1865–1871, 2010.

[6] S. Chen and M. Wu, "Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 22, no. 3, pp. 519–527, 2011.

[7] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science*, pp. 383–395, Portland, USA, Oct. 1985.

[8] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *Proceedings of 28th IEEE Symposium on Foundations of Computer Science*, pp. 427–437, Los Angeles, USA, Oct. 1987.

[9] C. Guo and C. C. Chang, "An authenticated group key distribution protocol based on the generalized `Chinese` remainder theorem," *International Journal of Communication Systems*, vol. 27, no. 1, pp. 126–134, 2014.

[10] L. Harn, "Group authentication," *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1893–1898, 2013.

[11] L. Harn and C. Lin, "Strong (n, t, n) verifiable secret sharing scheme," *Information Sciences*, vol. 180, no. 16, pp. 3059–3064, 2010.

[12] L. Harn, F. Miao, and C. C. Chang, "Verifiable secret sharing based on the `Chinese` remainder theorem," *Security and Communication Networks*, vol. 7, no. 6, pp. 950–957, 2014.

[13] S. Iftene, *Secret Sharing Schemes with Applications in Security Protocols*, Technical Report TR 07-01, Oct. 2006.

[14] K. Kaya and A. A. Selcuk, "A verifiable secret sharing scheme based on the `Chinese` remainder theorem," in *Advances in Cryptology (INDOCRYPT'08)*, pp. 414–425, Kharagpur, India, Dec. 2008.

[15] Y. P. Lai and C. C. Chang, "Parallel computational algorithms for generalized `Chinese` remainder theorem," *Computers and Electrical Engineering*, vol. 29, no. 8, pp. 801–811, 2003.

[16] C. H. Lin, C. C. Chang, and R. C. T. Lee, "A record-oriented cryptosystem for database sharing," *The Computer Journal*, vol. 35, no. 6, pp. 658–660, 1992.
[17] Y. Liu, C. C. Chang, and S. C. Chang, "An efficient oblivious transfer protocol using residue number system," *International Journal of Network Security*, vol. 15, no. 3, pp. 212–218, 2013.
[18] Y. Liu, C. C. Chang, and S. C. Chang, "A residual number system oriented group key distribution mechanism," *International Journal of Information Processing and Management*, vol. 4, no. 3, pp. 146–155, 2013.
[19] Y. Liu, C. C. Chang, and S. C. Chang, "An access control mechanism based on the generalized `Aryabhata` remainder theorem," *International Journal of Network Security*, vol. 16, no. 1, pp. 58–64, 2014.
[20] Y. Liu, L. Harn, and C. C. Chang, "An authenticated group key distribution mechanism using theory of numbers," *International Journal of Communication Systems*, vol. 27, no. 11, pp. 3502–3512, Nov. 2014.
[21] Y. Liu, L. Harn, and C. C. Chang, "A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets," *International Journal of Communication Systems*, vol. 28, no. 7, pp. 1282–1292, May 2015.
[22] M. Mignotte, "How to share a secret," in *Proceedings of the Workshop on Cryptography*, pp. 371–375, 1983.
[23] A. Parakh and S. Kak, "Space efficient secret sharing for implicit data security," *Information Sciences*, vol. 181, no. 2, pp. 335–341, 2011.
[24] L. Qiong, W. Zhifang, N. Xiamu, and S. Shenghe, "A non-interactive modular verifiable secret sharing scheme," in *Proceedings of International Conference on Communications, Circuits and Systems (ICCCAS 2005)*, pp. 84–87, Hong Kong, May 2005.
[25] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[26] H. Zhu, T. Liu, D. Zhu, and H. Li, "Robust and simple n-party entangled authentication cloud storage protocol based on secret sharing scheme," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 2, pp. 110–117, 2013.

Yanjun Liu received her B.S. degree in 2005, in School of Computer Science and Technology from Anhui University, Hefei, China. She received her Ph.D. degree in 2010, in School of Computer Science and Technology from University of Science and Technology of China, Hefei, China. She is currently serving in Anhui University. Meanwhile, she is a postdoctor at Asia University, Taichung, Taiwan. Her current research interests include information security and computer cryptography.

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan. Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. And since his early years of career development, he consecutively won Outstanding Talent in Information Sciences of the R. O. C., AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of the R. O. C., Outstanding Engineering Professor Award of the R. O. C., Distinguished Research Awards of National Science Council of the R. O. C., Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. His current research interests include database design, computer cryptography, image compression and data structures.

PPAM: Privacy-preserving Attributes Matchmaking Protocol for Mobile Social Networks Secure against Malicious Users

Solomon Sarpong, Chunxiang Xu, and Xiaojun Zhang
(Corresponding author: Solomon Sarpong)

Department of Computer Science, University of Electronic Science and Technology of China
Main Building A1-406, No. 2006, Xiyuan Avenue, West Hi-Tech Zone, Chengdu 611731, China
(Email: sarpong.uestc@gmail.com)
(Received June 12, 2015; revised and accepted Aug. 12 & Aug. 31, 2015)

Abstract

People often associate with others who share their hopes, aspirations, beliefs and experiences. This sense of belonging influences people when making friends be it physically or on social networks. Most of the existing matchmaking protocols just match-pair people without regards to the number of attributes they have in common. In lieu of these, we are proposing a hybrid matchmaking protocol that seeks to help match-pair seekers find the most appropriate pair. In our protocol, all private attributes are certified by a mutually trusted third party. Also, a candidate becomes a matching-pair of an initiator when s/he meets a criteria set by the initiator. In our protocol, the number of attributes in the intersection set is known mutually by both the initiator and the candidate but only the matched-pair gets to know the actual attributes they have in common. Furthermore, the protocol guards against malicious and semi-malicious attacks.

Keywords: Attributes, hybrid, matchmaking, nonspoofability

1 Introduction

1.1 Contextualization

In recent times, mobile telephony has changed the way we socialize and communicate. Currently, social networking has made a lot of gains in the cyberspace. The Internet has brought a new perspective about friends making and socializing. People no longer makes friends only in their neighborhoods and communities but also from all over the world.

The hardware specifications of smartphones have been dramatically improved to the level of personal computers along with friendly interfaces, improvements and usability enhancements. The smartphones have WiFi and Bluetooth interfaces that allow physically-close persons to communicate. Hence, with these improved features of smartphones, there is a growing tendency to access our social networks on our smartphones than on our desktop computers or laptops.

Furthermore, improvement in smartphones and people's eagerness to get information anytime-anywhere has increased the usage of Internet on mobile devices. This has brought the need for security of personal information. Data owners online have a problem with their data being used by unintended persons. Hence, the need to protect information of users has become very important. However, individuals can protect their own private or sensitive information by restricting the intended purpose of data access by denying the right to access for some purposes [7].

1.2 Relevance of the Theme

Matchmaking is a key component of mobile social networking [37]. In mobile social networking, persons form social networks based on a predefined criteria; for example former school mates, members of a club e.t.c. However, in a scenario where a person is looking for a recommendation, any individual(s) is not good enough but an individual(s) with specific qualities is appropriate. This is the premise of our research. The matchmaking protocol in this paper has an initiator looking for a person(s) with some particular characteristics to be his/her match-pair. Hence, the person(s) who qualifies to be a match-pair of the initiator should have a minimum number of attributes in common with the initiator.

1.3 Research Question

In matchmaking protocols, the matched-pair can terminate the protocol as a result of insufficient number of attributes they have in common. When the protocol is terminated, the individual's attributes would have been

known hence compromising the privacy and secrecy of the attributes. Hence, how can a pair know they have enough attributes in common before they exchange their attributes? This question has necessitated this research.

1.4 Objectives

Protocols for matchmaking such as [1, 3, 6, 12, 16, 17, 24, 37] simply match-pair the initiator and the candidate(s) without checking if they have enough attributes in common. The matched-pair at times terminate the protocol as a result of insufficient number of attributes they have in common compromising their attributes. However, protocols in [18, 19, 35, 36] sort to solve this problem by assuming that the candidate with the maximum intersection set with the initiator is the best matching-pair. We have realized that using this criteria is not good enough. Hence, as our contribution to research, we formulate matchmaking protocol that enables the initiator to check the number of attributes s/he has in common with a candidate before being match-paired. The initiator of the matchmaking sets a threshold number of attributes that candidate should have in common with him/her. If a candidate possesses at least these number of attributes, then the initiator and the candidate exchange their attributes. The novelty of our matchmaking protocol is that: (1) the initiator finds a match-pair that has at least the preset threshold number of attributes (2) the number of common attributes is known mutually by the persons in the protocol (3) the actual attributes are known only by the matched-pair in the protocol (4) the protocol can resist semi-honest and malicious attacks.

1.5 Limitations of the Paper

The matched-pair will know the actual attributes of the each other after they have exchanged them. Hence, a malicious person can do attribute profiling of the other persons s/he executed the protocol with. This protocol cannot prevent such a person from doing this. This is the main limitation of the protocol in this paper.

1.6 Structure of the Paper

The rest of this paper is organized as follows: we take a look at private set intersection in Section 2. In Section 3, we present related work. Our protocol, the algorithm for the matchmaking, the experimental implementation and the security of our algorithms are presented in Section 4. Finally, we conclude this paper in Section 5.

2 Private Set Intersection

When two persons want to find the common items in their individual private sets, they cannot just disclose the content of their sets so as to know the common items. This is what happens in matchmaking. Hence this brings the need for private set intersection protocols, PSI [1, 11, 13, 14, 15, 38]. PSI is a cryptographic protocol that allows two persons to compute the intersection of their private sets without disclosing any other information apart from what they have in common.

In PSI, the private inputs are chosen arbitrarily. This facilitates attacks from malicious users to gain extra information from other users [2]. In order to prevent this form of attack, authorized private set intersection, APSI [5, 10, 34] is used. In APSI, private inputs are certified by mutually trusted authority. Hence, in matchmaking protocols with variants of APSI, all the private input sets are certified by a mutually trusted party. The certification of attributes binds the private data sets to the data owners. This prevents the data owners from modifying their inputs so as to gain extra-information from other users. Certification of private data sets is important as no secure multi-party protocol can prevent a person in a protocol from cheating by changing his/her input before the protocol begins [2].

Certification of private inputs prevents malicious persons from claiming possession of fictitious data items in an attempt to find out if the other users possess those data items. In a distributed system framework, mutual authentication is becoming very important. Hence, it has become necessary for a user in such a system to verify the identity of the system or another user or node in the system verifies itself to him/her. Consequently, both user and the system may require some degree of authentication before information about them is released [9]. This mutual authentication is usually done by contacting a trusted third party. The use of a trusted third party may encounter the following challenges: (1) it may not be practical in a highly distributed system (2) sometimes the parties may not be willing to trust the third party (3) though the trusted third party may exist, it may not be available to all parties at all times. In light of all these problems, a solution researchers has developed is the use of cryptographic techniques. These cryptographic techniques enable users with private sets to verify whether or not their sets agree without revealing the content of their private sets.

3 Related Work

Baldwin and Gramlich [3] laid the foundation for matchmaking in social network with the use of a trusted third party protocol. Meldew [24] later proposed a protocol that did not rely on the use of a trusted third party. This protocol seemed to be more efficient than [3] as there was no need for trusted third party to be continuously available. In the matchmaking protocol proposed by Zhang and Needham [40], the matchmaking protocol depended on the availability of a public database service. Even though this protocol is efficient, the security of this protocol depends on the security of the hash function and the encryption algorithm used. Freedman, Nissim and Pinkas [38] also considered the problem of computing the

intersection of private data sets of two parties, where the data sets contain lists of elements taken from a large domain.

Shin and Gligor [32] observed that anonymity of protocol users, authentication of wishes and security in matchmaking was fundamental to private matchmaking. Hence, their proposed protocol sort to provide authentication for users and wish matches; privacy resistance to off-line dictionary attacks and forward privacy of users′ identities and their wishes. In their paper, Sang and Shen [25] addressed privacy preserving set intersection (PPSI) problem. Their paper sort to solve the problems associated with finding the intersection of data sets that are distributed on different sources while preserving the privacy of the data sets.

Shamir [31] proposed a scheme that enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories and without using the services of a third party. Camenisch et al. [4], proposed the searchable encryption scheme that provides an important mechanism to cryptographically protect data while keeping it available to be searched and accessed for matching information. In the scheme, they proposed two encryptions; public key encryptions with oblivious keyword search (PEOKS) and committed blind anonymous identity-based encryption. Lin et al. [21] proposed efficient blind-key encryption protocols for anonymous identity-based encryption and an anonymous hierarchical identity-based encryption. These schemes were used in privacy preserving profiles searching (PPPS) problem.

Sun et al. [33] proposed a privacy-preserving scheme for data sharing in social networks with efficient revocation for deterring a contact′s access right to the private data once the contact is removed from the social group. Zhang et al. [39] also propose a privacy-preserving verifiable profile matching scheme which is based on symmetric cryptosystem and thus improves efficiency. It relies on a pre-determined ordered set of attributes and uses it as a common secret shared by users. However, the scheme is not applicable to unordered sets of attributes such as random capabilities. Cristofaro and Tsudik [9] considered several flavors of private set intersection and constructed some provably secure protocols. They proposed efficient protocols for plain and authorized private set intersection and noted that, the choice between them depends on whether there is a need for client authorization and/ server unlinkability, as well as on servers ability to engage in pre-computation.

In matchmaking, persons make friends by match-pairing. A match-pair is made when two persons have some characteristics in common. In the quest to find the attributes two persons have in common, some protocols use either the trusted third party, the fully distributed technique or the hybrid technique.

With the use of the trusted third party, the trusted third party is involved in each step of the matchmaking process. The trusted third party collects personal attributes and location information, computes the intersection and notifies the matched-pair. Such protocol applications can be found in [12, 16, 17]. The use of the trusted third party has got some well-known problems.

The fully distributed technique requires no trusted third party in the whole matchmaking process. The operations such as the distribution of personal attributes data, the computation of the intersection set, and the dissemination of results are performed among multi-parties, without any trusted third party. The attributes of the users of this protocol are shared among multi-parties using Shamir secret sharing scheme, the computing of common attributes set are conducted among multi-parties as well [36]. The fully distributed technique can be found in matchmaking protocols in [6, 18, 22, 23].

The third technique in use is the hybrid technique − a combination of the two fore-mentioned techniques. In his technique, the trusted third party is needed only for the purpose of management and verification, and it does not participate in the matchmaking. In [8, 19, 20, 26, 27, 28, 29, 30, 35, 36] are matchmaking protocols based on the hybrid technique.

4 Our Matchmaking Protocol

In our quest to enable match-pair seekers find the most appropriate pair while at the same time prevent their private attributes from leaking, these protocols were formulated. In order for the users of this algorithm to achieve these said objectives, Algorithm 1 helps the initiator find a user who has enough attributes with him/her. In our protocol, the initiator sets a threshold number of attributes, $A_{Threshold}$ that a user should possess so as to qualify as a match-pair. Hence, a user of this protocol becomes a match-pair of the initiator if the number of attributes s/he has in common with the initiator is at least $A_{Threshold}$. The notations used in this paper are listed in Table 1.

The matchmaking protocol we are proposing comprise a certification authority (CA) that cannot be compromised and other users. These users consist an initiator, Alice and other persons called candidates. Each user has a portable device that has wireless interfaces such as Bluetooth or WiFi that is in communication range with each other. Among the m candidates, $k = 1, \ldots, m$ Alice wishes to find a candidate(s) who possesses attributes that are at least $A_{Threshold}$. The CA generates an RSA key-pair, (e_{CA}, d_{CA}) and $N = pq$, where p and q are large prime numbers. The CA makes N and e_{CA} public. Each person in the protocol also chooses a username and an ID, creates an RSA key-pair, (e, d). Alice creates an RSA key-pair (e_A, d_A) and each candidate also creates an RSA key-pair, (e_k, d_k). Alice makes e_A and her username public. Each candidate also makes e_k and username public.

The attributes of Alice are $A = \{a_1, a_2, \ldots, a_p\}$. Also, for all the $k = 1, \ldots, m$ candidates and $h = 1, \ldots, w$ attributes, the attributes of each candidate is $C_k =$

Table 1: Notations

Notation	Explanation
R_A	Random number chosen by Alice, $R_A \longleftarrow_r Z_{N/4}$
R_k	Random number chosen by each candidate, $R_k \longleftarrow_r Z_{N/4}$, $k = 1, \ldots, m$
R_B	Random number chosen by Bob, $R_A \longleftarrow_r Z_{N/4}$
ID_k	Identity of each candidate, $k = 1, \ldots, m$
ID_A	Identity of Alice
γ_{kh}	Computation to certify each candidates's attributes, $\gamma_{kh} = Sign_{d_{CA}}(ID_k \| C_{kh})$
α_j	Computation to certify Alice's attributes, $\alpha_j = Sign_{d_{CA}}(ID_j \| \alpha_j)$
$\mid I_{Ak} \mid$	Number of attributes Alice and each candidate have in common
$\mid I_{kA} \mid$	Number of attributes each candidate and Alice have in common

$\{c_{k1}, c_{k2}, \ldots, c_{kw}\}$.

Alice chooses a random number, $R_A \leftarrow_r Z_{N/4}$. Each candidate also chooses a random number $R_k \leftarrow_r Z_{N/4}$, $k = 1, \ldots, m$. In this matchmaking protocol, attributes are the same if they are semantically the same. Alice and each candidate then encrypt their attributes, ID, their random number, username, and the public key-pair of his/her RSA key using the public key of the CA. Each of the persons in the protocol sends his/her encrypted set to the CA.

Alice sends $E_{e_{CA}}\{A \parallel ID_A \parallel R_A \parallel username_A \parallel RSA_{publickey}, e_A\}$ to the CA. The CA certifies the attributes of Alice and the attributes become $A = \{(a_1, \alpha_1), (a_2, \alpha_2), \ldots, (a_p, \alpha_p)\}$, where $\alpha_j = sign_{d_{CA}}(ID_A \| a_j)$, $j = 1, \ldots, p$. The CA returns $A = \{(a_1, \alpha_1), (a_2, \alpha_2), \ldots, (a_p, \alpha_p)\}$ to Alice. Alice then exponentiates each of her attributes with her random number and sends to each candidate. Each candidate receives $\{a_1^{R_A}, a_2^{R_A}, \ldots, a_p^{R_A}\}$ from Alice.

Each candidate also sends $E_{e_{CA}}\{C_k \parallel ID_k \parallel R_k \parallel username_k \parallel RSA_{publickey}, e_k\}$ to the CA for certification. After certification of each candidate's attributes by the CA, the attributes become $C_k = \{(c_{k1}, \gamma_{k1}), (c_{k2}, \gamma_{k2}), \ldots, (c_{kw}, \gamma_{kw})\}$, where $\gamma_{kh} = sign_{d_{CA}}(ID_k \| c_{kh})$. Each candidate receives $C_k = \{(c_{k1}, \gamma_{k1}), (c_{k2}, \gamma_{k2}), \ldots, (c_{kw}, \gamma_{kw})\}$ from the CA. Each candidate exponentiates his/her attributes with the random number and sends to Alice. Hence, Alice receives $\{c_{k1}^{R_k}, c_{k2}^{R_k}, \ldots, c_{kw}^{R_k}\}$ from each candidate.

When Alice received $\{c_{k1}^{R_k}, c_{k2}^{R_k}, \ldots, c_{kw}^{R_k}\}$, she exponentiates it with her random number and returns $\{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\}$ to each candidate. Each candidate also exponentiates $\{a_1^{R_A}, a_2^{R_A}, \ldots, a_p^{R_A}\}$ with his/her random number and returns $\{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\}$ to Alice.

With the knowledge of $\{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\}$ and $\{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\}$, Alice computes the intersection between her and each candidate and outputs $|I_{Ak}| \in \{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\} \cap \{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\}$. Also, with the knowledge of $\{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\}$ and $\{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\}$, each candidate computes the intersection between him/her and Alice and outputs $|I_{kA}| \in \{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\} \cap \{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\}$. The intersections $|I_{Ak}|$ and $|I_{kA}|$ computed in Steps 11 and 12 of Algorithm 1 by Alice and each candidate respectively allow them to know the number of attributes they have in common with each other. The initiator, Alice then checks which candidate has attributes $|I_{Ak}| \geq A_{Threshold}$.

Algorithm 1 Computing the Number of Common Attributes

Require: The CA has an RSA key-pair, (e_{CA}, d_{CA}) makes N and e_{CA} public.

1: Alice creates an RSA key-pair (e_A, d_A) and chooses a random number $R_A \leftarrow_r Z_{N/4}$.
Also, each candidate creates an RSA key-pair (e_k, d_k) and chooses a random number $R_k \leftarrow_r Z_{N/4}$, for all $k = 1, \ldots, m$.
Alice and each candidate make their RSA-keys e_A and e_k public.

2: Alice has private attributes $A = \{a_1, a_2, \ldots, a_p\}$. Alice sends $E_{e_{CA}}\{A \| ID \| username_{Alice} \| e_A\}$ to the CA.

3: After certification by the CA, the attributes of Alice become $A = \{(a_1, \alpha_1), (a_2, \alpha_2), \ldots, (a_p, \alpha_p)\}$, where $\alpha_j = sign_{d_{CA}}(ID_A \| a_j)$.

4: Each of the k candidates has $C_k = \{c_{k1}, c_{k2}, \ldots, c_{kw}\}$ attributes, for all $k = 1, \ldots, m$ and $h = 1, \ldots, w$. Each candidate sends $E_{e_{CA}}\{C_k \| ID \| username_k \| e_k\}$ to the CA.

5: After certification by the CA, the attributes become $C_k = \{(c_{k1}, \gamma_{k1}), (c_{k2}, \gamma_{k2}), \ldots, (c_{kw}, \gamma_{kw})\}$, where $\gamma_{kh} = sign_{d_{CA}}(ID_k \| c_{kh})$.

6: Alice exponentiates each of her attributes with her random number and sends $\{a_1^{R_A}, a_2^{R_A}, \ldots, a_p^{R_A}\}$ to each candidate.

7: For all $k = 1, \ldots, m$ and $h = 1, \ldots, w$, each candidate exponentiates his/her attributes with the random number and sends $\{c_{k1}^{R_k}, c_{k2}^{R_k}, \ldots, c_{kw}^{R_k}\}$ to Alice.

8: Alice computes $\{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\}$ and sends to each candidate.

9: Each candidate also computes and sends $\{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\}$ to Alice.

10: Alice computes the intersection between her and each candidate and outputs $|I_{Ak}| \in \{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\} \cap \{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\}$.

11: Each candidate computes the intersection between him/her and Alice and outputs $|I_{kA}| \in \{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\} \cap \{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\}$.

12: The intersections $|I_{Ak}|$ and $|I_{kA}|$ computed in Steps 11 and 12 by Alice and each candidate respectively allows each of them to know the number of attributes each has in common with the other.

Alice sends her username, the intersection she computed and the username of the candidate whose attributes is at least $A_{Threshold}$ to the CA. Alice sends

$E_{e_{CA}}\{username_{Alice}|||I_{Ak}|||username_k\}$ to the CA. Each candidate also sends his/her username, the intersection computed and the username of Alice to the CA. Thus each candidate sends $E_{e_{CA}}\{username_k|||I_{kA}|||username_{Alice}\}$ to the CA. The CA verifies $|I_{Ak}|$ and $|I_{kA}|$. If $|I_{Ak}| = |I_{kA}|$, the CA notifies Alice and the candidate(s) of a successful match. However, if $|I_{Ak}| \neq |I_{kA}|$ the CA checks who cheated. The CA the removes the cheat from the protocol users.

For simplicity, lets us assume Bob was the only candidate whose attributes was at least $A_{Threshold}$. Let R_B be the random number of Bob. Alice and Bob exchange their random numbers using Algorithm 2. Algorithm 2 is an authenticated Diffie-Hellman protocol. Alice and Bob agree on a primitive prime number, g. At the end of Algorithm 2, both Alice and Bob will know each other's random number. Alice receives Bob's random number, R_B and Bob also receives Alice's random number, R_A. At the end of Algorithm 2, Alice sends the random number received from Bob to the CA. Thus Alice sends $E_{e_{CA}}\{username_{Alice}||username_{Bob}||R_B\}$ to the CA. Bob also sends the random number he received from Alice to the CA by sending $E_{e_{CA}}\{username_{Bob}||username_{Alice}||R_A\}$. The CA verifies if the random number Alice sent to Bob is the same as that in Step 1 of Algorithm 1. Also, the CA verifies if the random number Bob sent to Alice is the same as that in Step 1 of Algorithm 1. If the CA observes that the random numbers are the same, the CA then notifies them. Hence, with the knowledge of R_A and R_B both Alice and Bob can be able to know the actual attributes they have in common.

Algorithm 2 Authenticated Diffie-Hellman protocol for exchanging the random numbers of the matched-pair

Require: Alice has a random number R_A and Bob also has a random odd number R_B.

1: Using the generator g, Alice computes and sends $g^{R_A} = Enc(g^{R_A} \parallel ID_A)$ to Bob.
2: Bob using the generator, g, computes $g^{R_B} = Enc(g^{R_B} \parallel ID_B)$ and sends $g^{R_A} \parallel g^{R_B} \parallel Sign_{Bob}(g^{R_A} \parallel g^{R_B} \parallel ID_A)$ to Alice.
3: Alice computes and sends $Sign_{Alice}(g^{R_A} \parallel g^{R_B} \parallel ID_A)$ to Bob.
4: Alice computes $(g^{R_A})^{R_B}$ and Bob also computes $(g^{R_B})^{R_A}$

4.1 Experimental Implementation

Our protocol for computing the number of common attributes was simulated in java. We focused only on the execution time without considering the communication time. In this simulation, the execution time is mainly decided by the number of participants and the number of attributes they possess. The prime numbers p and q we chosen to be 1024 bits with RSA modulus of 1024 bits. Also, each attribute was represented by 64 bits. The execution time for the protocol was measured. The time duration to run the protocol between an initiator and a candidate constituted the execution time. The number of attributes of the initiator was kept constant whilst the number of attributes of the candidates were varied. In the experiment, the number of users was varied $k = 1, 5, 10, 15, 20, 25$. The initiator has the same number of attributes but the number of attributes of each candidate varied $h = 5, 10, 15, 20$. The protocol was simulated on an hp-compaq laptop with 2.10 GHz processor and 4G RAM. In order to ensure the accuracy of the execution time, the average of 80 repeated execution times was used. Figure 1 is the graph of the execution times for our protocol for the users and their attributes. The x-axis shows the number of users and the y-axis shows the execution time. The graph shows the execution times for the varying number of users and users attributes. It can be observed that the execution times increases as the number of users and attributes increases.

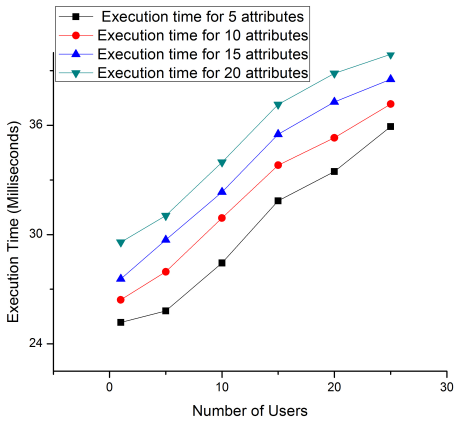


Figure 1: Comparison of execution time for the number of attributes

4.2 Security Analysis

In Algorithm 1, CA certifies users' private attributes to be used in the protocol. The certification of the attributes binds the attributes to the attribute owners. Hence, a user(s) cannot modify the attributes so as to gain more information from others in the protocol. Also, in order to prevent the attribute owners from modifying their attributes after the certification, the CA does the following computation. The CA computes and sends $A = \{(a_1, \alpha_1), (a_2, \alpha_2), \ldots, (a_p, \alpha_p)\}$ and $C_k = \{(c_{k1}, \alpha_{k1}), (c_{k2}, \alpha_{k2}), \ldots, (c_{kw}, \alpha_{kw})\}$ to Alice and each of the other candidates respectively.

In Step 6 of Algorithm 1, in order to prevent a candidate from knowing her attributes, Alice exponentiates her attributes with her random number. This exponentiation will prevent a candidate from being able to know the attribute a_i from $a_i^{R_A}$, $i = 1, \ldots, p$ in polynomial time. Each candidate also in Step 7 of Algorithm 1 exponentiates each of the attributes so as to prevent Alice from being able to know c_{kh} from $c_{kh}^{R_k}$, $k = 1, \ldots, m$ and $h = 1, \ldots, w$ in polynomial time.

In Step 11 of Algorithm 1, Alice computes the intersection set between her and each candidate. The computation of the intersection, $|I_{Ak}|$ ϵ

$\{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\} \cap \{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\}$ allows Alice know only the number of attributes she has in common with each candidate. Likewise, the computation of the intersection, $|I_{kA}| \in \{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\} \cap \{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\}$ by each candidate allows him/her know only the number of attributes the candidate has in common with Alice. At the end of Algorithm 1, the initiator as well as each candidate will know the number of attributes they have in common with each other. Alice then checks which candidate's $|I_{Ak}| \geq A_{Threshold}$. The candidate with $|I_{Ak}| \geq A_{Threshold}$ then becomes her match-pair. In this protocol, only candidates with $|I_{Ak}| \geq A_{Threshold}$ proceed to Algorithm 2. If a person decides to terminate the protocol because the number of attributes they have in common is small, the actual attributes will be preserved.

In order to prevent semi-honest attack on Algorithm 1, Alice and the candidate(s) who has $|I_{Ak}| \geq A_{Threshold}$ attributes send their intersection to the CA. The CA then verifies if $|I_{Ak}| = |I_{kA}|$. If $|I_{Ak}| = |I_{kA}|$ is verified successfully, the protocol continues to Algorithm 2. However if $|I_{Ak}| \neq |I_{kA}|$, the protocol is terminated and the CA checks who has cheated and removes the cheat from the list of the protocol users.

In order to exchange their random numbers securely, Alice and Bob execute Algorithm 2. The authenticated Diffie-Hellman protocol in Algorithm 2 ensures that, there is no meet-in-the middle attack by a malicious persons. To further ensure that the protocol for this matchmaking is secured, Alice and Bob send the random number they received from each other to the CA. The CA then verifies if the correct random numbers have been exchanged. This is done so as to prevent semi-honest attack on the protocol. When the CA observes that the random numbers are not the same, the protocol is terminated. The CA then checks who might have cheated and remove the cheat from the list of the protocol users.

4.2.1 Correctness of the Protocol

In Step 8 of Algorithm 1, Alice sends $\{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \cdots, c_{kw}^{R_k R_A}\}$ to each candidate. Likewise, each candidate sends $\{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\}$ to Alice in step 9. Alice computes and outputs the intersection $|I_{Ak}| \in \{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\} \cap \{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\}$. Each candidate also computes and outputs the intersection $|I_{kA}| \in \{c_{k1}^{R_k R_A}, c_{k2}^{R_k R_A}, \ldots, c_{kw}^{R_k R_A}\} \cap \{a_1^{R_A R_k}, a_2^{R_A R_k}, \ldots, a_p^{R_A R_k}\}$. The number of attributes in $|I_{Ak}|$ and $|I_{kA}|$ are the same, ($|I_{Ak}| = |I_{kA}|$). Hence, Algorithm 1 is correct. Also, at the end of Algorithm 2, Alice computes $(g^{R_A})^{R_B}$; Bob also computes $(g^{R_B})^{R_A}$. Since $(g^{R_A})^{R_B}$ and $(g^{R_B})^{R_A}$ are the same, Algorithm 2 is also correct.

4.2.2 Preventing Other Attacks on the Protocol

In this paper, attack by persons outside the protocol is not possible as a person needs to register with the CA to be able to run the protocol. Also, part from Alice who knows the number of candidates that are running the protocol with her, no other protocol user does. As the candidates do not know about the other candidates in the protocol, they cannot collude to know all of Alice's attributes. Hence, our protocol is collusion resistant. Nonspoofability of the other users' attributes is another characteristic of our protocol. The attributes of the users in the protocol are certified hence, a user cannot query another$'s$ attributes without his/her knowledge.

5 Discussion, Implication, and Conclusion

in real life, people who have many characteristics in common tend to be good friends. This behavior is also used on social networks. Hence on social networks, the ability to know the number of attributes a person has in common with the other before they become friends is also very important.

Knowing the number of attributes a person has in common with the other before they exchange their attributes prevents the termination of the protocol; keeps the privacy and security of the attributes. Hence, by implication helps users feel more confident in using such protocols.

Matchmaking has becoming very popular on mobile social networks. Hence, there is the need for secure and privacy-preserving matchmaking protocol for MSN. This research paper has effective proposed a matchmaking protocol that will enable an individual find a match on MSN.

The quest to know the number of attributes two individuals, each having a private set of attributes have in common is becoming very important in matchmaking. This knowledge can be extended to any database to ascertain the items they have in common. Cloud computing is gaining more popularity as a data storage facility hence it is recommended the application of the knowledge from this paper to compare the content of clouds.

References

[1] R. Agrawal, A. Evfimievski, and R. Srikant, "Information sharing across private databases," in *Proceedings of ACM SIGMOD International Conference on Management of Data*, pp. 86–97, New York, USA, 2003.

[2] G. Ateniese, E. De Cristofaro, and G. Tsudik, "(if) size matters: Size-hiding private set intersection," in *14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography (PKC'11)*, pp. 156–173, Springer-Verlag, 2011.

[3] R. W. Baldwin and W. Gramlich, "Cryptographic protocol for trustable match making," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 92–100, 1985.

[4] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in *Proceedings of 12th International Conference on Practice and Theory in Public Key Cryptography (PKC'09)*, LNCS 5445, pp. 196–214, Springer, 2009.

[5] J. Camenisch and G. M. Zaverucha, "Private intersection of certified sets," in *Financial Cryptography and Data Security*, LNCS 5628, pp. 108–127, Springer, 2009.

[6] A. C. Champion, Z. Yang, B. Zhang, J. Dai, D. Xuan, and Du Li, "E-smalltalker: A distributed mobile system for social networking in physical proximity," *IEEE Transactions on Parallel Distribution Systems*, vol. 24, no. 8, pp. 1535–1545, 2013.

[7] M. Yu Chen, C. C. Yang, and M. S. Hwang, "Privacy protection data access control," *International Journal of Network Security*, vol. 15, no. 6, pp. 411–419, 2013.

[8] E. De Cristofaro, A. Durussel, and I. Aad, "Reclaiming privacy for smartphone applications," in *Proceedings of Ninth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'11)*, pp. 84–92, Seattle, USA, 2011.

[9] E. De Cristofaro, Y. Lu, and G. Tsudik, "Efficient techniques for privacy-preserving sharing of sensitive information," in *Proceedings of the 4th International Conference on Trust and Trustworthy Computing (TRUST'11)*, pp. 239–253, Springer-Verlag, 2011.

[10] E. De Cristofaro and G. Tsudik, "Practical private set intersection protocols with linear complexity," in *Proceedings of 14th International Conference on Financial Cryptography and Data Security*, pp. 143–159, 2010.

[11] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient robust private set intersection," *International Journal of Applied Cryptology*, vol. 2, no. 4, pp. 289–303, 2012.

[12] N. Eagle and A. Pentland, "Social serendipity: Mobilizing social software," *IEEE Pervasive Computing*, vol. 4, no. 2, pp. 28–34, 2005.

[13] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in *Advances in Cryptology (EUROCRYPT'04)*, LNCS 2267, pp. 1–9, Springer, 2004.

[14] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," in *Proceedings of 5th Conference on Theory of Cryptography (TCC'08)*, pp. 155–175, 2008.

[15] L. Kissner and D. X. Song, "Privacy-preserving set operations," in *Advances in Cryptology (CRYPTO'05)*, pp. 241–257, 2005.

[16] J. Kjeldskov and J. Paay, "Just-for-us: A context-aware mobile information system facilitating sociality," in *Proceedings of 7th ACM International Conference on Human Computer Interaction with Mobile Devices & Services (MobileHCI'05)*, pp. 23–30, New York, USA, 2005.

[17] K. A. Li, T. Y. Sohn, S. Huang, and W. G. Griswold, "Peopletones: A system for the detection and notification of buddy proximity on mobile phones," in *Proceedings of 6th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'08)*, pp. 160–173, New York, USA, 2008.

[18] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in *Proceedings of 30th IEEE International Conference on Computer Communications*, pp. 2435–2443, Shanghai, China, 2011.

[19] M. Li, S. Yu, N. Cao, and W. Lou, "Privacy-preserving distributed profile matching in proximity-based mobile social networks," *IEEE Wireless Communications*, vol. 12, no. 5, pp. 2024–2033, 2013.

[20] X. Liang, R. Lu, X. Lin, and X. Shen, *Security and Privacy in Mobile Social Networks*, Springer Briefs in Computer Science, Springer Berlin Heidelberg: Springer, 2013.

[21] H. Lin, S. M. Chow, D. Xing, Y. Fang, and Z. Cao, "Privacy-preserving friend search over online social networks," *IACR Cryptology ePrint Archive*, pp. 445, 2011.

[22] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," *Mobile Network Applications*, vol. 16, no. 6, pp. 683–694, 2011.

[23] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Transactions on Parallel Distribution Systems*, vol. 24, no. 3, pp. 614–624, 2013.

[24] C. Meadows, "A more efficient cryptographic matchmaking protocol for use in the absence of a continuously available third party," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 134–137, 1986.

[25] Y. Sang and H. Shen, "Privacy preserving set intersection protocol secure against malicious behaviors," in *Proceedings of Eighth IEEE International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'07)*, pp. 461–468, 2007.

[26] S. Sarpong and C. Xu, "Efficient privacy-preserving attribute matchmaking protocol for proximity-based mobile social networks," in *Proceedings of A10th International Conference on dvanced Data Mining and Applications (ADMA'14)*, LNCS 8933, pp. 305–318, Springer-Verlag, 2014.

[27] S. Sarpong and C. Xu, "Provably secure attribute matchmaking protocol for mobile social network secure against malicious users," in *1st International Conference on Computer, Network Security and Communication Engineering (CNSCE'14)*, pp. 362–366, Shenzhen, China, 2014.

[28] S. Sarpong and C. Xu, "A collusion-resistant privacy-preserving attribute matchmaking for mobile social

networks," *International Journal of Innovative Science, Engineering and Technology*, vol. 2, pp. 485–495, 2015.

[29] S. Sarpong and C. Xu, "Privacy-preserving attribute matchmaking for proximity-based mobile social networks," *International Journal of Security and its Applications*, vol. 9, no. 5, pp. 217–230, 2015.

[30] S. Sarpong, C. Xu, and X. Zhang, "An authenticated privacy-preserving attribute matchmaking protocol for mobile social networks," *International Journal of Network Security*, vol. 17, no. 3, pp. 357–364, 2015.

[31] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Advances in Cryptology (CRYPTO'85)*, pp. 47–53, Springer-Verlag, 1985.

[32] Ji S. Shin and V. D. Gligor, "A new privacy-enhanced matchmaking protocol," *IEICE Transactions on Communications*, vol. E96-B, no. 8, pp. 2049–2059, 2013.

[33] J. Sun, X. Zhu, and Y. Fang, "A privacy-preserving scheme for online social networks with efficient revocation," in *Proceedings 29th IEEE Conference on Information Communications (INFOCOM'10)*, pp. 2516–2524, 2010.

[34] J. Vaidya and C. Clifton, "Secure set intersection cardinality with application to association rule mining," *Journal of Computer Security*, vol. 13, no. 4, pp. 593–622, 2005.

[35] Y. Wang, J. Hou, Y. W. Tan, and X. Nie, "A recommendation-based matchmaking scheme for multiple mobile social networks against private data leakage," in *Proceedings of 1st International Conference on Information Technology and Quantitative Management (ITQM'13)*, pp. 781–788, 2013.

[36] Y. Wang, T. T. Zhang, H. Z. Li, L. P. He, and J. Peng, "Efficient privacy preserving matchmaking for mobile social networking against malicious users," in *1Proceedings of 1th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TRUSTCOM'12)*, pp. 609–615, 2012.

[37] Qi Xie and U. Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users," in *Proceedings of Ninth IEEE Annual Conference on Privacy, Security and Trust (PST'11)*, pp. 252–259, 2011.

[38] Q. Ye, H. Wang, and J. Pieprzyk, "Distributed private matching and set operations," in *Proceedings of the 4th International Conference on Information Security Practice and Experience (ISPEC'08)*, pp. 347–360, 2008.

[39] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," *IEEE Network*, vol. 24, no. 4, pp. 13–18, 2010.

[40] K. Zhang and R. Needham, "A private matchmaking protocol," 2001. (`http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.54.835&rep=rep1&type=pdf`)

Solomon SARPONG , is a Ph.D. student in University of Electronic Science and Technology of China, Chengdu, (UESTC). His research interests include Information Security and Cryptography.

Chunxiang XU, received her B.Sc., M.Sc. and Ph.D. degrees at Xidian University, P. R. China, in 1985, 1988, 2004 respectively. She is currently engaged in Information Security, Cloud Computing Security and Cryptography as a professor at University of Electronic Science and Technology of China, Chengdu, (UESTC).

Xiaojun ZHANG, received his B.Sc. degree in mathematics and applied mathematics at Hebei Normal University in 2009. He also received his M.Sc. degree in pure mathematics at Guangxi University, P. R. China, in 2012. He is currently pursuing his Ph.D degree in Information Security at University of Electronic Science and Technology of China (UESTC). He is currently engaged in Cryptography, Network Security and Cloud Computing Security.

Dual-Image Based Reversible Data Hiding Scheme Using Pixel Value Difference Expansion

Biswapati Jana[1], Debasis Giri[2] and Shyamal Kumar Mondal[3]
(Corresponding author: Biswapati Jana)
Department of Computer Science, Vidyasagar University[1]
Midnapore, Pin-721102, India
(Email: biswapatijana@gmail.com)
Department of Computer Science and Engineering, Haldia Institute of Technology[2]
Department of Applied Mathematics with Oceanology and Computer Programming, Vidyasagar University[3]
(Received June 22, 2015; revised and accepted Aug. 12 & Aug. 22, 2015)

Abstract

In this paper, we propose a dual-image based reversible data hiding scheme. Here, we divide a secret message into sub-stream of size n bits, where $n-1$ bits are embedded using Pixel Value Differencing (PVD) and 1 bit is embedded using Difference Expansion (DE). We consider two consecutive pixels from cover image, calculate the difference between them and then embed $n-1$ bits secret message by modifying the pixel pair. Again, we consider that modified pixel pair to embed 1 bit secret message using embedding function. After that, we distribute these two stego pixel pairs among dual image depending on a shared secret key bit stream. At the receiver end, we extract the secret message successfully and recover original cover image from dual stego image without any distortion. Finally, we compare our scheme with other state-of-the-art methods and obtain reasonably better performance in terms of data embedding capacity.

Keywords: Difference expansion, dual image, pixel value differencing, reversible data hiding

1 Introduction

Steganography is one of the most commonly used protective method for information security. Steganography can be classified into two categories: irreversible and reversible. In irreversible technique, the secret data can be embedded and extracted successfully, but the original image might not be recovered [1, 5, 6, 8, 23]. On the other hand, reversible data hiding schemes [9, 10, 16, 17, 19, 20, 22, 24] are capable of embedding the secret message as well as can extract the secret message and recover the original image. Two important measures of reversible data hiding are embedding capacity and distortion of cover work. In recent years, a bunch of research [7, 13, 14, 15, 21, 27] have been performed to improve the embedding capacity and to minimize the distortion which is the objective of data hiding schemes. Wu and Tsai [26] proposed a data embedding method based on PVD, where, the difference of two adjacent pixels in the cover image is calculated. The number of bits to be embedded into these two pixels are determined by their absolute difference and a pre-defined reference table. By modifying these two pixel values, data bits can be embedded. Because the same range in the reference table will be referred before and after data embedding, the same number of secret data bits can be determined and thus the embedded secret data bits can be exactly extracted. Tian [22] proposed a difference expansion data hiding approach to conceal the secret data into the difference of a pair consecutive pixel values with high payload size. Lee et al. [13] utilized the histogram of the difference of pixel values to embed the secret data in host image for improving the quality of marked-images. Ni et al. [16] proposed reversible data hiding technique which is based on histogram shifting with zero or minimum change of the pixel gray values. Being reversible, both the original and the embedded data can be completely restored. Thodi et al. [21] presented a method that combines histogram-shifting and difference expansion reversible data hiding.

Chang et al. [2] proposed dual-image based data hiding technique using exploiting modification direction (EMD) method. They first established a (256×256) modulus function magic matrix. In their scheme, a binary secret message is first converted into secret digits in the base-5 numeral system. Then, two secret digits are taken to embed into a pixel pair at a time by embedding each secret digit into each steganographic image. Lee et al. [7] introduced a lossless steganographic technique that utilized centralized difference expansion to hide more secret data into smoother areas of host image. Later, Lee et al. [12] embed secret data using the four directions of the center point of pixels to obtain the stego-pixels of the two images. Lee and Huang [11] converted secret data into

quinary-based secret symbols and combined every two secret symbols as a set for embedding. Qin et al. [18] embedded the first image using EMD, and the second image through three rules which were dependent on the first image. Lu et al. [14] used the least-significant-bit (LSB) matching method for embedding. They obtained the stego-pixels of two images through the modulus function and the LSB, checked whether the stego-pixels are reversible via an averaging method, and then modified the non-reversible stego-pixels based on a rule table to successfully restored the image. Lee et al. [12] embedded secret data using directions to achieve high image quality, but the embedding capacity could only reach 0.75 bits per pixel (bpp). Chang et al. [2] embed secret data through the modulus function matrix to achieve a higher capacity that is 1.00 bpp, but image quality was inferior to that using the method by Lee et al. Thus, the challenge to enhance embedding capacity while maintaining high image quality through the use of dual-image techniques is still an important issue.

In this paper, we introduced a new dual-image based reversible data hiding scheme through Pixel Value Difference Expansion (PVDE).

- Our motivation is to enhance the embedding capacity and achieve reversibility in data hiding. Data embedding using PVD was not reversible. We have applied DE data embedding scheme to keep the distance parameter of sub range of reference table within the pixel pair. The lower bound of sub range of reference table help us to achieve reversibility in PVDE. The proposed scheme also enhance embedding capacity.

- One of the important modification that we have propose in our scheme is uniform sub range in the reference table. In PVD, the width of sub range varies and the number of embedding bits depends on the pixel value difference. More number of data bits are embedded in the complex area of an image which will effect more. To maintain the uniform effect after data embedding in all area, we propose uniform width of sub range in the reference table. Although data could be embedded without reference table, we use reference table to make PVD as reversible. The lower label of sub range in each embedding pair is essential for PVD to recover original image.

- Another motivation is to enhance security in data hiding. We distribute modified pixel pair among dual stego image, stego major (SM) and stego auxiliary (SA) based on shared secret key bit stream. The secret message bits are distributed among dual image. The receiver applies extraction technique using either PVD or DE that depends on the share secret key. Without key none can extract secret message. Finally, we recover original image using our extraction algorithm from dual image without any distortion.

The rest of the paper is organized as follows. Section 2 describes some preliminary techniques of data hiding scheme. Proposed data hiding scheme PVDE in detail is discussed in Section 3. The issue regarding overflow and underflow situation are described in Section 4. Experimental results with comparisons are discussed in Section 5. Section 6 present security analysis. Finally, we conclude our paper with some interesting insights and possible future directions in Section 7.

2 Preliminaries

Reversible data hiding become a very important and challenging task in hidden data communication specially in medical and military application for ownership identification, authentication and copy right protection. We propose dual-image based reversible data hiding scheme called PVDE. In this section, Wu and Tsai's PVD and Tian's DE techniques are discussed briefly.

2.1 Wu and Tsai's Scheme

Pixel Value Differencing (PVD), proposed by Wu and Tsai [26] is one of the popular data hiding techniques in spatial domain. Consider a two consecutive pixels P_x and P_{x+1} from cover image C of size $(M \times N)$. The difference value d of P_x and P_{x+1} can be derived by

$$d = |P_x - P_{x+1}|.$$

A reference table R is used which consists of n contiguous sub-blocks with fixed interval. The main function of the reference table is to provide data hiding information. Each sub-range has its lower bound (lb) and upper bound (ub) values and the width w of each sub-range is selected to be a power of 2. The hiding capacity of two consecutive pixels can be obtained by

$$t = \lfloor log_2\ w \rfloor. \tag{1}$$

Here, t is the number of bits that is hidden within pixel pair. A new parameter $d^{'}$ is generated using

$$d^{'} = m_1 + lb.$$

Now the secret data is embedded into pixel pair (P_x, P_{x+1}) by modifying it such that d and $d^{'}$ belongs to the same range in the reference table. The details of the embedding criteria are as follows:

$$(P_x^{'}, P_{x+1}^{'}) = \begin{cases} (P_x + \lceil d^{''}/2 \rceil, P_{x+1} - \lfloor d^{''}/2 \rfloor), & \\ \text{if } P_x \geq P_{x+1} \text{ and} & d^{'} > d; \\ (P_x - \lceil d^{''}/2 \rceil, P_{x+1} + \lfloor d^{''}/2 \rfloor), & \\ \text{if } P_x < P_{x+1} \text{ and} & d^{'} > d; \\ (P_x - \lceil d^{''}/2 \rceil, P_{x+1} + \lfloor d^{''}/2 \rfloor), & \\ \text{if } P_x \geq P_{x+1} \text{ and} & d^{'} \leq d; \\ (P_x + \lceil d^{''}/2 \rceil, P_{x+1} - \lfloor d^{''}/2 \rfloor), & \\ \text{if } P_x < P_{x+1} \text{ and} & d^{'} \leq d; \end{cases}$$

where $d^{''} = |d^{'} - d|$. An illustration of how $P_x^{'}$ and $P_{x+1}^{'}$ can be adjusted by Wu and Tsai 's scheme for the purpose of hiding secret data is shown in Figure 1. The recovery

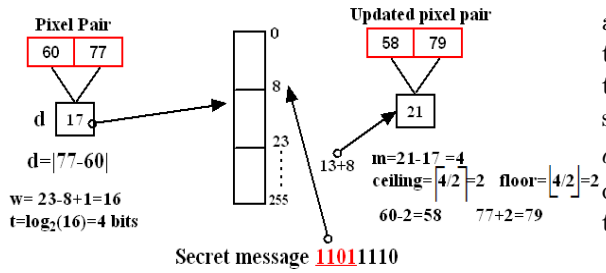


Figure 1: Data embedding through PVD with example

process of Wu and Tsai 's method is quite simple and easy. Given two consecutive pixels $P_x^{'}$ and $P_{x+1}^{'}$ of the stego image, we compute their difference value $d^{'}$ and obtain $d^{'}$=$|P_{x+1}^{'}$ - $P_x^{'}|$. Then we use the original reference table R in the embedding phase to obtain the same sub range. The length t of the hiding capacity can also be gained by using Equation (1). Then we extract message $m_1 = d^{'}$ - lb and convert the decimal value m_1 into a binary string whose length is t bits. For example, in Figure 1, m_1= $21-8=(13)_{10}$ and $t=4$, and then secret data $(1101)_2$ is extracted.

2.2 Tian 's Scheme

Tian [22] presented a reversible data hiding technique based on a difference expansion for gray-scale images. Consider a pixel pair of cover image P_x and P_{x+1}. After embedding 4 bits secret data using PVD, we obtained modified pixel $P_x^{'}$ and $P_{x+1}^{'}$. For embedding secret data within consecutive pixel pair $P_x^{'}$ and $P_{x+1}^{'}$, where $0\leq$ ($P_x^{'}$, $P_{x+1}^{'}$) ≤ 255 the following process is discussed. The average value A and the difference value d is computed by

$$A=\lfloor\frac{P_x^{'}+P_{x+1}^{'}}{2}\rfloor,\ d=|P_x^{'}-P_{x+1}^{'}|. \quad (2)$$

The inverse integer transform of Equation (2) is

$$P_x^{'}=A+\lfloor\frac{d+1}{2}\rfloor, P_{x+1}^{'}=A-\lfloor\frac{d}{2}\rfloor. \quad (3)$$

Such a transform in Equation (2) and Equation (3) are called integer Haar wavelet transform or S transform. Obviously, the transform is a one-to-one correspondence between ($P_x^{'}$, $P_{x+1}^{'}$) and (A,d). That means, it meets the requirement of reversibility. Tian expands the difference twice for vacate a space and embed a secret bit s, where $s\in\{0,1\}$ is the binary secret and generates a new difference value $d^{'}$ by

$$d^{'}=2\times d+s.$$

The new pixel values $P_x^{''}$ and $P_{x+1}^{''}$ are obtained by

$$(P_x^{''},P_{x+1}^{''})=(A+\lfloor\frac{d^{'}+1}{2}\rfloor, A-\lfloor\frac{d^{'}}{2}\rfloor).$$

Finally, the embedding operation is completed, and it produces a stego-image pixel pair by modifying ($P_x^{'}$ and $P_{x+1}^{'}$) to ($P_x^{''}$ and $P_{x+1}^{''}$). Figure 2 is the illustration of Tian's difference expansion scheme. During extraction the secret message, the difference value of consecutive pixel pair ($P_x^{''}$, $P_{x+1}^{''}$) is obtained by calculating $d^{'}=|P_x^{''}-P_{x+1}^{''}|$. The secret bit s can be extracted by computing $s=d^{'}\ mod\ 2$. Then, the average value A and the original difference value d are obtained by

$$A^{'} = \lfloor\frac{P_x^{''}+P_{x+1}^{''}}{2}\rfloor$$
$$d = \lfloor\frac{d^{'}}{2}\rfloor.$$

Now, the original pixel values are recovered using

$$(P_x^{'},P_{x+1}^{'})=(A^{'}+\lfloor\frac{d+1}{2}\rfloor,\ A^{'}-\lfloor\frac{d}{2}\rfloor).$$

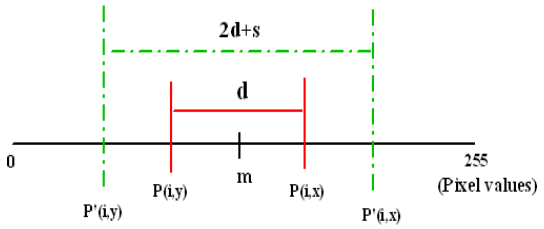


Figure 2: Difference expansion

3 Proposed PVDE Scheme

In this paper, we propose a new reversible data hiding scheme by combining Pixel Value Difference (PVD) and Difference Expansion (DE) on dual image called PVDE. According to this approach, first we have to select two consecutive pixels x_i and x_{i+1} from cover image C. Then we calculate the pixel value difference d between x_i and x_{i+1} that is

$$d=|x_i-x_{i+1}|.$$

The number of secret bits which will be embedded in the cover image is determined with the help of a reference table R. The reference table have equal sub range $[lb,ub]$ having length w that is $w=ub-lb+1$. In our proposed PVDE scheme, w is taken as 16. Hence forth the contiguous sub-ranges are $\{0-15,\ 16-31,\ 32-47,\ \ldots,\ 240-255\}$ which have capability to embed 4 secret bits within each pixel pair through PVDE in cover image. Now to embed 4 bits, two new parameters $d^{'}$ and $d^{''}$ are introduced as follows:

$$d^{'} = lb+m_1$$
$$d^{''} = d^{'}-d$$

where m_1 is decimal value of the secret message of size 4 bits. After that the pixel values x_i and x_{i+1} are adjusted into two new pixel values $x_i^{'}$ and $x_{i+1}^{'}$ by following

modifications.

$$\begin{aligned} x_i^{'} &= x_i - \delta \\ x_{i+1}^{'} &= x_{i+1} + \gamma \end{aligned}$$

where $\delta = \lceil \frac{d^{''}}{2} \rceil$ and $\gamma = \lfloor \frac{d^{''}}{2} \rfloor$. Then we apply DE on the pixels $x_i^{'}$ and $x_{i+1}^{'}$ to embed one bit. Now, we determine the lower range from the reference table R where the difference d belongs to. Then we calculate the parameters h, A and $h^{'}$ as follows

$$\begin{aligned} h &= (d - lb) \\ A &= (x_i^{'} + x_{i+1}^{'})/2 \\ h^{'} &= (2 \times h + m_2) \end{aligned}$$

where m_2 is one bit secret message. After this the pixel pair $x_i^{'}$ and $x_{i+1}^{'}$ are again modified by

$$\begin{aligned} x_i^{''} &= A + \delta_1 \\ x_{i+1}^{''} &= A - \gamma_1 \end{aligned}$$

where $\delta_1 = \lceil (h^{'}/2) \rceil$ and $\gamma_1 = \lfloor (h^{'}/2) \rfloor$. Finally, the stego pixel pairs $(x_i^{'}, x_{i+1}^{'})$ and $(x_i^{''}, x_{i+1}^{''})$ are distributed among dual stego image, Stego Major (SM) and Stego Auxiliary (SA) based on shared secret key K. If $K = 1$, then the pixel pair $(x_i^{'}, x_{i+1}^{'})$ is stored within the stego image SM and the pixel pair $(x_i^{''}, x_{i+1}^{''})$ is stored within the stego image SA. Again if $K = 0$ then the pixel pair $(x_i^{'}, x_{i+1}^{'})$ is stored within the stego image SA and the pixel pair $(x_i^{''}, x_{i+1}^{''})$ is stored within the stego image SM. The detailed schematic diagram of our proposed PVDE method for embedding process are shown in Figure 3 and the corresponding algorithm is shown in Algorithm 1.

Algorithm 1: Data embedding of PVDE

Input: Original image I $(M \times N)$, Secret message M, Shared secret key K.
Output: Two stego images, Stego Major (SM) and Stego Auxiliary (SA) of size $(M \times N)$.

1: Select pixel pair (x_i, x_{i+1}) from I in raster scan order;
2: Calculate difference $d = |x_i - x_{i+1}|$;
3: Select 4 bits secret message from M and convert into decimal value m_1 and 1 bit as m_2;
4: Calculate $d^{'} = m_1 + lb$; where, lb is the lower bound of the sub range of reference table R in which d belongs to;
5: Calculate $d^{''} = d^{'} - d$;
6: Compute $\delta = \lceil \frac{d^{''}}{2} \rceil$ and $\gamma = \lfloor \frac{d^{''}}{2} \rfloor$;
7: **if** $(x_i > x_{i+1})$ **then**
8: $x_i^{'} = x_i + \gamma$; $x_{i+1}^{'} = x_{i+1} - \delta$;
9: **else**
10: $x_i^{'} = x_i - \delta$; $x_{i+1}^{'} = x_{i+1} + \gamma$;
11: **end if**
12: Calculate $h = (d - lb)$;

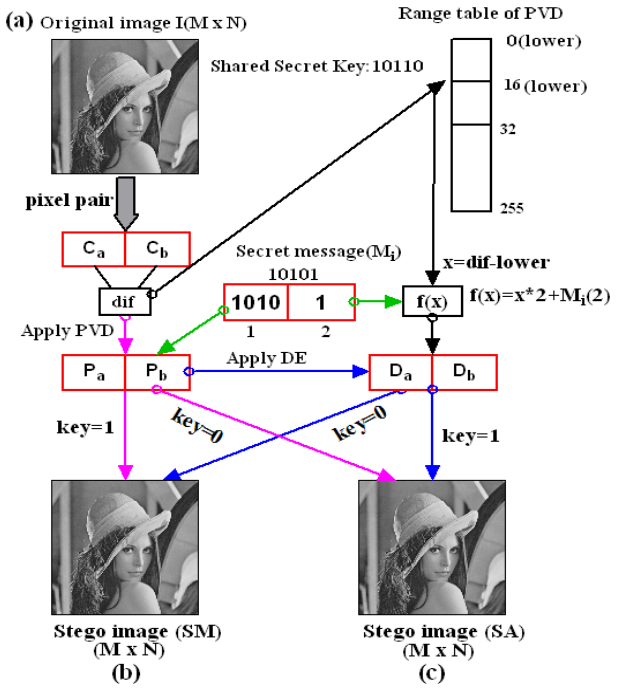


Figure 3: Schematic diagram of PVDE for data embedding process

13: Calculate $h^{'} = 2 \times h + m_2$; where, m_2 is 1 bit secret message;
14: Calculate Average $A = \lfloor \frac{(x_i^{'} + x_{i+1}^{'})}{2} \rfloor$;
15: Calculate $\delta_1 = \lceil \frac{h^{'}}{2} \rceil$; and $\gamma_1 = \lfloor \frac{h^{'}}{2} \rfloor$;
16: **if** $(x_i^{'} > x_{i+1}^{'})$ **then**
17: $x_i^{''} = A + \delta_1$; $x_{i+1}^{''} = A - \gamma_1$;
18: **else**
19: $x_i^{''} = A - \gamma_1$; $x_{i+1}^{''} = A + \delta_1$;
20: **end if**
21: **if** $(K = 1)$ **then**
22: Store $(x_i^{'}, x_{i+1}^{'})$ within stego image SM and store $(x_i^{''}, x_{i+1}^{''})$ within stego image SA;
23: **else**
24: Store $(x_i^{'}, x_{i+1}^{'})$ within stego image SA and store $(x_i^{''}, x_{i+1}^{''})$ within stego image SM;
25: Repeat **Line-1** through **Line-24** until $length(M) = 0$;
26: Dual stego image SM and SA are generated;
27: **end if**
28: End

At the receiver end, both the data extraction and original image reconstruction are performed by taking pixel from both the stego images SM and SA based on K. If $K = 1$, then select pixel pair $(x_i^{'}, x_{i+1}^{'})$ from SM and apply data extraction using PVD and at the same time select pixel pair $(x_i^{''}, x_{i+1}^{''})$ from SA and apply data extraction using DE. If $K = 0$, then apply the pixel pair selection process opposite manner, that means select pixel pair $(x_i^{'}, x_{i+1}^{'})$ from stego image SA and $(x_i^{''}, x_{i+1}^{''})$ from

stego image SM. Now the data extraction and original image reconstruction process are described as follows:

$$\begin{aligned} d &= |x_i^{'} - x_{i+1}^{'}| \\ m_1 &= d - lb \end{aligned}$$

where lb is the lower bound of the sub range of the reference table R to which d belongs to and m_1 is the 4 bits secret data. To recover another secret bit, we perform

$$h^{'} = x_i^{''} - x_{i+1}^{''}$$

and collect one bit secret message (m_2) from LSB of $h^{'}$. To recover the original image, we perform the following calculations

$$\begin{aligned} h &= \lfloor \frac{h^{'}}{2} \rfloor \\ d^{'} &= (h + lb) \\ d^{''} &= d^{'} - d \\ \delta &= \lceil \frac{d^{''}}{2} \rceil \\ \gamma &= \lfloor \frac{d^{''}}{2} \rfloor. \end{aligned}$$

Now, the original image pixel (x_i, x_{i+1}) is recovered by

$$(x_i, x_{i+1}) = \begin{cases} x_i^{'} - \gamma,\ x_{i+1}^{'} + \delta & \text{if } x_i^{'} > x_{i+1}^{'} \\ x_i^{'} + \delta,\ x_{i+1}^{'} - \gamma & \text{otherwise} \end{cases}$$

The extraction process of our proposed PVDE scheme is explained using a schematic diagram in Figure 4. The corresponding algorithm for data extraction and original image reconstruction is explained in Algorithm 2.

Algorithm 2: Data extraction of PVDE

Input: Two stego images SM and SA, Shared secret key K.

Output: Original Image $I(M \times N)$; Secret Message M;

1: Select pixel pair from SM and SA in raster scan order;
2: **if** $(K = 1)$ **then**
3: Collect $(x_i^{'}, x_{i+1}^{'})$ from SM and collect $(x_i^{''}, x_{i+1}^{''})$ from SA;
4: **else**
5: Collect $(x_i^{'}, x_{i+1}^{'})$ from SA and collect$(x_i^{''}, x_{i+1}^{''})$ from SM;
6: **end if**
7: Calculate $d^{'} = |x_i^{'} - x_{i+1}^{'}|$;
8: Secret message $m_1 = d^{'} - lb$, where lb is the lower bound of the sub range of range table R;
9: Calculate $h^{'} = (x_i^{''} - x_{i+1}^{''})$; (Extract secret message bit m_2 from LSB of $h^{'}$);
10: Calculate $h = \lfloor \frac{h^{'}}{2} \rfloor$;
11: Calculate $d = (h + lb)$; where lb is the lower bound of the sub range of the reference table R in which d belongs;

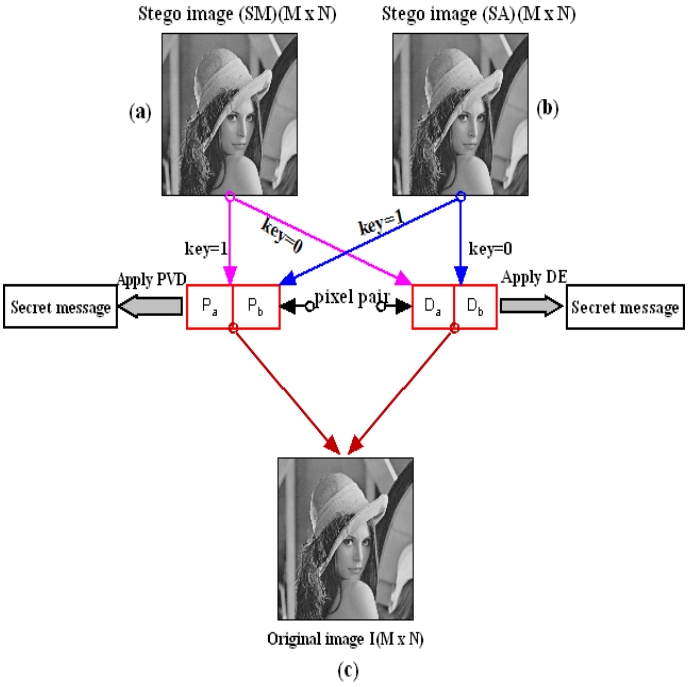


Figure 4: Schematic diagram of PVDE for data extraction process

12: Calculate $d^{''} = d^{'} - d$;
13: Calculate $\delta = \lceil \frac{d^{''}}{2} \rceil$;
14: Calculate $\gamma = \lfloor \frac{d^{''}}{2} \rfloor$;
15: **if** $(x_i^{'} > x_{i+1}^{'})$ **then**
16: $x_i = x_i^{'} - \gamma$; $x_{i+1} = x_{i+1}^{'} + \delta$;
17: **else**
18: $x_i = x_i^{'} + \delta$; $x_{i+1} = x_{i+1}^{'} - \gamma$;
19: **end if**
20: Repeat **Line-1** through **Step-19** until all data are extracted;
21: End

4 Overflow and Underflow

When the stego pixel value cross the upper range of gray scale then overflow occur and cross the lower limit of gray scale then underflow occur. We have use 8 bit image where gray scale is [0-255]. Suppose we have a pixel pair (C_a, C_b) with pixel values $C_a = 250$ and $C_b = 255$ and 4 bits secret data is $(1101)_2$ that is $(13)_{10}$. The difference between two pixels d is $|\ 250 - 255\ |$=5 and the new difference $d^{'}$ is 13+0=13. Therefore, m =13-5=8, c=4 and f=4. After embedding, the stego pixel pair becomes $P_a = 246$ and $P_b = 259$ which cross the upper limit that means $P_b > 255$ which shows overflow problem.

For underflow, suppose C_a=0 and C_b=7 and 4 bits secret data is $(1010)_2$ that is $(10)_{10}$. The difference between two pixels d is $|\ 0 - 7\ |$=7 and the new difference $d^{'}$ is 10+0=10. Therefore, m =10-7=3, c=2 and f=1. The

stego pixel pair becomes $P_a = -2$ and $P_b = 8$. We observe that $P_a < 0$ which shows underflow problem.

To overcome this problem, we do not embed any secret data within those specified pixel pair. We observed that after data embedding, the difference between two pixels is not much more than 31. To overcome the overflow problem, we use difference expansion method and set the difference 32 when data hiding by difference expansion is 0 and subtracting 32 from the average of two pixels. So, the modified pixel pair becomes $(D_a = avg-32, D_b = P_b)$ and set the difference 33 when data is 1 by subtracting 33 from the average of two pixels. So, the modified pixel pair becomes $(D_a = avg - 33, D_b = P_b)$.

To overcome the underflow problem, we set the difference 32 when data is 0 by adding 32 with the average of two pixels. So, the modified pixel pair will be $(D_a = avg + 32, D_b = P_b)$ and set the difference 33 when data is 1 by adding 33 with the average of two pixels. So, the modified pixel pair will be $(D_a = avg + 33, D_b = P_b)$.

In the receiver side, when difference between the pixels D_a and D_b is 32 or 33 the receiver understand that secret message is not embedded within that pair (P_a, P_b) corresponding to (D_a, D_b).

Figure 5: Standard test images with (256×256) pixel

5 Experimental Results and Comparison

In this section, our proposed method (PVDE) is verified and tested using gray scale image of size (256×256) pixels collected from [25] shown in Figure 5. After embedding the secret messages, dual stego image, Stego Major (SM) and Stego Auxiliary (SA) are generated as shown in Figure 6. Our developed algorithms: PVDE embedding and extraction are implemented in MATLAB Version 7.6.0.324 (R2008a). Here, the distortion is measured by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio $(PSNR)$. The MSE is calculated as follows:

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j) - Y(i,j)]^2}{(M \times N)}$$

where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image respectively.

Figure 6: Dual stego images of (256×256) pixels after data embedding

$X(i,j)$ represents the pixels in the cover image and $Y(i,j)$ represents the pixels of the stego image. The difference between the original and stego images were assessed by the Peak Signal to Noise Ratio $(PSNR)$. The formula of PSNR is as follows:

$$PSNR = 10\ log_{10}\frac{255^2}{MSE}$$

Table 1: Data embedding capacity with PSNR

Image	Data(bits)	PSNR(SM)	PSNR(SA)	Avg. PSNR
cameraman	40,000	43.40	42.72	36.77
	80,000	35.75	38.84	
	1,60,000	30.77	36.19	
	1,63,592	30.35	36.14	
house	40,000	47.00	41.88	38.95
	80,000	40.59	38.53	
	1,60,000	35.84	36.01	
	1,63,592	35.79	35.97	
F16	40,000	47.07	43.29	37.88
	80,000	37.18	39.36	
	1,60,000	31.65	36.48	
	1,63,592	31.62	36.41	
lake	40,000	36.95	43.15	36.08
	80,000	33.47	39.70	
	1,60,000	30.82	37.03	
	1,63,592	30.63	36.93	
Lena	40,000	40.31	43.78	36.93
	80,000	35.31	40.19	
	1,60,000	30.77	37.28	
	1,63,592	30.67	37.18	
livingroom	40,000	38.93	43.47	36.69
	80,000	34.18	40.02	
	1,60,000	31.37	37.19	
	1,63,592	31.31	37.11	
peppers	40,000	39.67	43.47	37.27
	80,000	35.45	39.93	
	1,60,000	32.92	36.98	
	1,63,592	32.86	36.89	
pirate	40,000	39.79	43.75	37.05
	80,000	35.29	40.28	
	1,60,000	31.58	37.15	
	1,63,592	31.48	37.09	
bridge	40,000	34.57	43.54	35.85
	80,000	32.39	40.47	
	1,60,000	30.50	37.51	
	1,63,592	30.44	37.42	
Tiffany	40,000	40.44	43.75	37.36
	80,000	36.32	40.20	
	1,60,000	32.00	37.19	
	1,63,592	31.92	37.12	
Zelda	40,000	42.20	43.76	38.87
	80,000	39.10	40.09	
	1,60,000	36.08	36.98	
	1,63,592	35.86	36.90	
Goldhill	40,000	45.84	42.85	38.66
	80,000	39.77	39.48	
	1,60,000	34.09	36.80	
	1,63,592	34.06	36.76	

Higher the values of PSNR between two images indicates better the quality of the stego image and very similar to the cover image where as low PSNR demonstrates the opposit. Table 1 shows the experimental result upon Cameraman, House, Jet Plane, Lake, Lena, Living Room, Peppers, Pirate, Walk bridge and Woman images. Table 1 shows the average $PSNR$ of SM and SA with cover image. To asses the embedding capacity, we calculate payload (B) in terms of bits per pixel (bpp) using the following expression.

$$B = \frac{(\lfloor \frac{M}{2} \rfloor - 1) \times N \times 5}{(2M \times 2N)}$$

For example, if $M = 512$ and $N = 512$ then $B = \frac{255 \times 512 \times 5}{2 \times (512 \times 512)} = 1.25$. The bpp B of our dual image based PVDE scheme is 1.25.

To measure the complexity, we assume that the size of the cover image is $(M \times N)$ and the data embedding process embed five secret bits within a pixel pair. Two copies of cover image is used to distribute the stego pixel and each pixel pair from cover image produce two copies of pixel pair. So, the time complexity is O(MN). On the other hand, during data extraction, we need to scan the pixel pair from dual image depending on key. So, the time complexity is O($2MN$).

Table 2 lists the average PSNR values with payload of different existing dual image based data hiding scheme. The average PSNR of the stego images of the proposed scheme is lower than the method proposed by Qin et al.'s [18], Lu et al.'s [14, 15], Chang et al.'s [2, 3] and Lee et al.'s [11, 12] schemes. But the average PSNR is higher than the method proposed by Lee et al.'s [10] and Zeng et al.'s [27] schemes. The embedding payload of our scheme is 1.25 bpp which is higher than the other existing dual image based schemes. The embedding payload of the methods proposed by Qin et al. [18] is approximately 0.09 bpp less than that of our proposed PVDE method. The payload of Lu et al. [15] and Chang et al. [2, 3] is approximately 0.25 bpp less than our PVDE method. It is observed that our PVDE is superior than the other dual image based schemes in terms of embedding payload (bpp). From the above discussion, one can conclude that PVDE is better than other existing scheme in terms of payload, and the PSNR is also reasonable which implies the quality of the stego image is good.

Table 2: Comparison of average PSNR and payload (bpp) with existing schemes

Scheme	Avg. PSNR (dB)	Capacity (bpp)
Chang et al.(2007)	45.1225	1.00
Chang et al.(2009)	48.14	1.00
Lee et al. (2009)	52.3098	0.74
Lee et al. (2010)	34.38	0.91
Zeng et al. (2012)	32.74	1.04
Lee and Huang (2013)	49.6110	1.07
Qin et. al. (2014)	52.11	1.16
Lu et al. (2015)	49.20	1.00
Proposed PVDE	38.95	1.25

6 Steganalysis

Steganalysis is the art of discovering whether or not a secret message is exist in a suspected image. Steganalysis does not however consider the successful extraction of the message. Now a days, steganographic systems does not achieve perfect security. So, they all leave hints of embedding in the stegogramme. This gives the steganalyst a useful way in to identifying whether a secret message exists or not. Steganalyst perform this work in various ways. The way is divided into two main categories-Targeted and Blind steganalysis. Some of the targeted steganalysis are visual attack, statistical attack and structural attack and one of the famous blind steganalysis method is RS analysis.

6.1 RS Analysis

We analyzes our stego images by RS analysis [4]. Let us assume that we have a cover image of size (M × N). In RS analysis method, first the stego image is divide into disjoint groups G of n adjacent pixels $(x_1, \ldots, x_n)$. Each pixel value is in a set P that is $p = \{0, 1, \ldots, 255\}$. Here, each group consist of 4 consecutive pixels in a row. Define a discrimination function f that returns a real number $f(x_1, \ldots, x_n) \in R$ to each pixel group $G = (x_1, \ldots, x_n)$. The main goal of use the discrimination function is to identify the "Smoothness" or "Regularity" of each group of pixels G. The discrimination function f is define as:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|$$

An invertible function F is define which is operates on P, called "flipping". Flipping consists of two-cycles which permutes the pixels value. So, F^2= Identity or $F(F(x)) = x$ for all x belongs to P. Flipping the LSB of each pixel value and the corresponding permutation F1 is: $0 \leftrightarrow 1, 2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255$. Define another function, named shift LSB flipping and treated as F_{-1}. So the permutation F_{-1}: $-1 \leftrightarrow 0, 1 \leftrightarrow 2, \ldots, 255 \leftrightarrow 256$. In the other word, F_{-1} flipping can be define as:

$$F_{-1}(x) = F_1(x + 1) - 1, \quad \text{for all } x.$$

There are three types of groups Regular groups (R), Singular groups (S) and Unusable groups (U) which are define depend on the discrimination function f and the flipping operation F. Depending on the condition groups are define below.

$$\begin{cases} G \in R & \text{if } f(F(G)) > f(G) \\ G \in S & \text{if } f(F(G)) < f(G) \\ G \in U & \text{if } f(F(G)) = f(G) \end{cases}$$

where $F(G) = F(x_1), \ldots, F(x_n)$.
The flipping operation will be execute with the help of a mask value M, which is a n tuples with values -1, 0, and 1. The flipped group $F_M(G)$ is defined as $(F_M(1)(x1)$, $F_M(2)(x2)$, ..., $F_M(n)(xn))$. The RS analysis based on analyzing how the number of regular and singular groups changes with the increased message length embedded in the LSB plane.

Then calculate the value of RS analysis using the following equation.

$$((|R_M - R_{-M}| + |S_M - S_{-M}|)/(R_M + S_M))$$

where R_M and R_{-M} is the total number of regular group with mask M and -M respectively. S_M and S_{-M} is the total number of singular group with mask M and -M respectively. When the value of RS analysis is closed to zero means the scheme is secure. The stego images are tested under the RS analysis. It is observed from Tables 3 and 4 that the values of R_M and R_{-M}, S_M and S_{-M} are nearly equal for stego image SM and SA. Thus rule $R_M \cong R_{-M}$ and $S_M \cong S_{-M}$ is satisfied for the stego image in our scheme. So, the proposed method is secure against RS attack. In our experiment, the ration of R and S lies between 0.0051 to 0.0616 for SM and 0.0043 to 0.0267 for SA of Cameraman image.

Table 3: RS analysis of PVDE method (Stego image SM)

Image	Data	SM				
		R_M	R_{-M}	S_M	S_{-M}	RS value
Cameraman	20000	7118	7107	3551	3594	0.0051
	50000	6768	6851	3944	3895	0.0123
	75000	6304	5947	4943	5279	0.0616
	114582	6207	6035	4997	5173	0.0311
Lena	20000	5617	5607	4067	4068	0.0011
	50000	5563	5476	4291	4337	0.0135
	75000	5636	5539	4517	4589	0.0166
	114582	5641	5387	4509	4709	0.0447
Baboon	20000	5893	5815	4960	5105	0.0205
	50000	5897	5875	5076	5131	0.0070
	75000	6018	5813	5107	5313	0.0369
	114582	5844	5986	5256	5123	0.0248

Table 4: RS analysis of PVDE method (Stego image SA)

Image	Data	SA				
		R_M	R_{-M}	S_M	S_{-M}	RS value
Cameraman	20000	6945	7078	3877	3721	0.0267
	50000	6506	6535	4490	4472	0.0043
	75000	6514	6528	4287	4224	0.0071
	114582	6538	6647	4283	4225	0.0154
Lena	20000	5575	5565	4139	4133	0.0016
	50000	5590	5514	4239	4299	0.0138
	75000	5587	5442	4579	4665	0.0227
	114582	5652	5621	4592	4553	0.0123
Baboon	20000	5876	5881	4995	5092	0.0094
	50000	5821	5878	5121	5147	0.0076
	75000	5895	5827	5196	5283	0.0140
	114582	5874	5830	5194	5206	0.0051

6.2 Relative Entropy

To measure the security in our proposed method, the relative entropy (D) between the probability distributions of the original image (P) and the stego image (Q) is calculated by

$$D(Q||P) = \sum q(x) log \frac{q(x)}{p(x)}.$$

When relative entropy between two probability distribution functions is zero then the system is perfectly secure. D($Q||P$) is a nonnegative continuous function and equals to zero if and only if p and q are coincide. Thus D($Q||P$) can be normally considered as a distance between the measures p and q. Relative entropy of the probability distribution of the original image and the stego image varies depending upon number of bits of secret message. In our experiment, it is shown that when the number of characters in the secret message increases, the relative entropy in stego image is also increases. The relative entropy in our experiment is varies between 0.0027 to 0.0131 for lena image which implies the proposed scheme provides

Table 5: Relative entropy between I and SM

Image	Data(Bytes)	Entropy I	Entropy SM	Difference
Lena	5000	7.4451	7.4451	0.0027
	10000	7.4451	7.4452	0.0058
	20000	7.4451	7.4452	0.0105
	20249	7.4451	7.4453	0.0131
Barbara	5000	7.0480	7.0480	0.0031
	10000	7.0480	7.0482	0.0064
	20000	7.0480	7.0485	0.0112
	20249	7.0480	7.0486	0.0134
Tiffany	5000	7.2925	7.2925	0.0029
	10000	7.2925	7.2925	0.0057
	20000	7.2925	7.2926	0.0122
	20249	7.2925	7.2926	0.0129
Pepper	5000	7.2767	7.2767	0.0039
	10000	7.2767	7.2768	0.0077
	20000	7.2767	7.2770	0.0142
	20249	7.2767	7.2771	0.0169
Gold hill	5000	7.2367	7.2367	0.0034
	10000	7.2367	7.2371	0.0056
	20000	7.2367	7.2375	0.0112
	20249	7.2367	7.2379	0.0143

secure hidden communication. Other relative entropy values with SM are depicted in Table 5.

6.3 Histogram Attack

Figure 7 depicted the histogram of the cover and stego image and their difference histogram are obtained. The stego image are produced from cover image employing the maximum data hiding capacity. It is observed that the shape of the histogram is preserved after embedding the secret data. Histogram of cover image is represented as h whereas histogram of stego image is represented as $h^{'}$. The change of histogram can be measured by

$$D_h = \sum_{m=1}^{255} |h_m^{'} - h_m|.$$

The difference of the histogram is very small. It is observed that, bins close to zero are more in numbers and the bins which are away from zero are less in numbers. This confirm the quality of stego image. There is no step pattern observed which ensure the proposed method is robust against histogram analysis.

6.4 Statistical Attack

The proposed scheme is also assessed based on statistical distortion analysis by some image parameters like Standard Deviation (SD) and Correlation Coefficient (CC) to check the impact on image after data embedding. The SD before and after data embedding and CC of cover and stego images are summarized in Table 6. Minimizing parameters difference is one of the primary aims in order to get rid of statistical attacks. From the Table 6 it is seen that there is no substantial divergence between the SD of the cover-image and the stego-image. This study shows that the magnitude of change in stego-image based on image parameters is small from a cover image. Since the image parameters have not changed much, the method

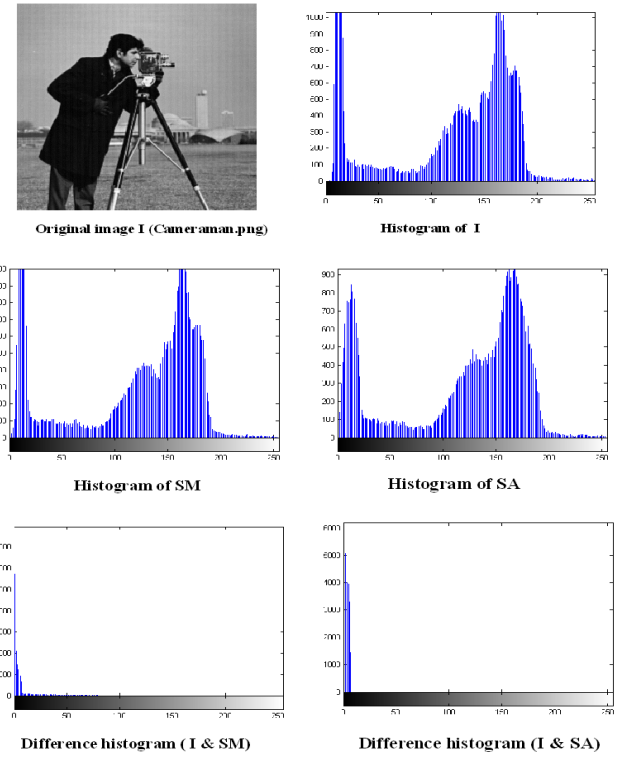


Figure 7: Histogram of Original, SM, SA and difference

Table 6: Standard Deviation (SD) and Correlation Coefficient (CC)

Image	SD			CC		
	I	SM	SA	I&SM	I&SA	SM & SA
Baboon	38.37	37.85	38.54	0.98	0.99	0.97
Cameraman	61.59	61.12	61.73	0.99	0.99	0.99
Lena	47.83	47.43	47.97	0.98	0.99	0.98

offers a good concealment of data and reduces the chance of the secret data being detected. Thus, it indicates a perfectly secure steganographic system.

6.5 Attacks with Unknown Secret Key

We have used 128 bits shared secret key K to distribute pixel among dual images. The scheme is secure to prevent possible malicious attacks. The proposed scheme constructs two stego images which protect original information by hiding secret information in both images SM and SA. The Figure 8 shows the revelation example where with key and without key stego images are used to revel the hidden message. If the malicious attacker holds the original image and dual images and is fully aware of the proposed scheme, the hidden message still cannot be correctly revealed without knowing the correct secret key. The result indicate that the attacker only acquires noise -like images when applying incorrect secret key to reveal the hidden message. Furthermore, the attacker may employ the brute force attack that tries all possible permu-

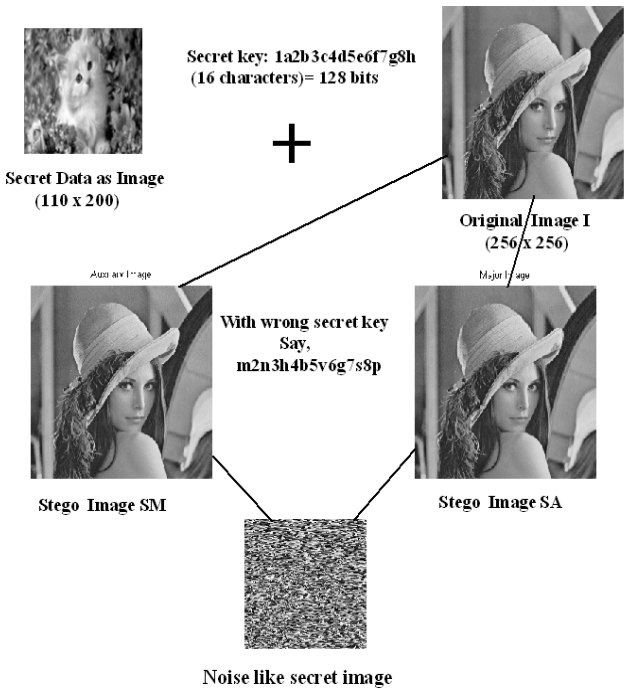


Figure 8: Noise like secret data with wrong secret key

tation to reveal the hidden message. The secret key are 128 bits length, so, the number of required trials to reveal the hidden message are 2^{128} which are computationally infeasible for current computers. The proposed scheme achieve stronger robustness against several attacks when compared with existing data hiding. Furthermore, the secret information can be retrieved without encountering any loss of data and recovered original image successfully from dual image.

7 Conclusion

In this paper, on the basis of pixel value difference and difference expansion a dual image based reversible data hiding scheme (PVDE) is introduced. Here, the reference table is modified allowing fix size four bits data embedding capacity. During difference expansion we keep the difference value of a subrange from the reference table which helps to recover the original image from stego images. In our proposed PVDE method, PVD achieved reversibility which demands the originality of our method. Also PVDE achieves security using the shared secret key by which stego pixels are distributed among two stego images. A shared secret key K has been used which guarantees security. The RS analysis provide low value which fulfilled the art of steganography. The visual attacks are analyzed by histogram analysis and statistical attacks are performed by SD and CC which provide robustness against several attacks. Also, the scheme maintains low relative entropy. In addition, it gains good PSNRs and higher payload than other existing methods of dual image based data hiding.

References

[1] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[2] C. C. Chang, Y. C. Chou. "Reversible data hiding scheme using two steganographic images" in *IEEE Region 10 Conference on TENCON*, pp. 1–4, 2007.

[3] C. C. Chang, Y. C. Chou, and T. D. Kieu, "Information Hiding in Dual Images with Reversibility", *Proceedings of Third International Conference on Multimedia and Ubiquitous Engineering*, pp. 145–152, 2009.

[4] J. Fridrich, J. Goljan, R. Du, "Invertible authentication", in *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents*, vol. 4314, pp.197208, SanJose, CA, Jan. 2001.

[5] T. D. Kieu and C. C. Chang, "A steganographic scheme by fully exploiting modification directions", *Expert Systems with Applications*, vol. 38, pp. 10648–10657, 2011.

[6] H. J. Kim, C. Kim, Y. Choi, S. Wang, and X. Zhang, "Improved modification direction methods", *Computers and Mathematics with Applications*, vol. 60, no. 2, pp. 319–325, 2010.

[7] C. C. Lee, H. C. Wu, C. S. Tsai, Y. P. Chu, "Lossless Steganographic scheme with Centralized Difference Expansion", *Pattern Recognition*, vol. 41, pp. 2097–2106, 2008.

[8] C. F. Lee, C. C. Chang, P. Y. Pai, and C. M. Liu, "Adjustment hiding method based on exploiting modification direction", *International Journal of Network Security*, vol. 17, no. 5, pp. 607–618, 2015.

[9] C. F. Lee and H. L. Chen, "Adjustable prediction-based reversible data hiding", *Digital Signal Processing*, vol. 22, no. 6, pp. 941–953, 2012.

[10] C. F. Lee, H. L. Chen, and H. K. Tso, "Embedding capacity raising in reversible data hiding based on prediction of difference expansion", *Journal of Systems and Software*, vol. 83, no. 10, pp. 1864–1872, 2010.

[11] C. F. Lee, Yu L. Huang, "Reversible data hiding scheme based on dual stegano-images using orientation combinations", *Telecommunication Systems*, vol. 52, pp. 2237–2247, 2013.

[12] C. F. Lee, K. H. Wang, C. C. Chang, Y. L. Huang, "A reversible data hiding scheme based on dual steganographic images", in *Proceedings of the Third International Conference on Ubiquitous Information Management and Communication*, pp. 228–237, 2009.

[13] S. K. Lee, Y. H. Suh, Y. S. Ho, "Lossless data hiding based on histogram moification of difference images", in *Pacific Rim Conference on Multimedia*, LNCS 3333, pp. 340–347, Springer-Verlag, 2004.

[14] T. C. Lu, C. Y. Tseng, and J. H. Wu, "Dual imaging-based reversible hiding technique using LSB matching", *Signal Processing*, vol. 108, pp. 77–89, 2015.

[15] T. C. Lu, J. H. Wu, and C. C. Huang, "Dual-image-based reversible data hiding method using center folding strategy", *Signal Processing*, vol. 115, pp. 195–213, 2015.

[16] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[17] C. Qin, C. C. Chang, and Y. C. Chen, "Efficient reversible data hiding for VQ-compressed images based on index mapping mechanism" *Signal Processing*, vol. 93, no. 9, pp. 2687–2695, 2013.

[18] C. Qin, C. C. Chang, and T. J. Hsu, "Reversible data hiding scheme based on exploiting modification direction with two steganographic images" *Multimedia Tools and Applications*, pp. 1–12, 2014.

[19] C. Qin, C. C. Chang, Y. H. Huang, and Li T. Liao, "An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 7, pp. 1109–1118, 2013.

[20] C. Qin, C. C. Chang, and Li T. Liao, "An adaptive prediction-error expansion oriented reversible information hiding scheme", *Pattern Recognition Letters*, vol. 33, no. 16, pp. 2166–2172, 2012.

[21] D. M. Thodi, J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking", *IEEE Translations on Image Processing*, vol. 16, no. 3, pp. 1057–7149, Mar. 2007.

[22] J. Tian, "Reversible data embedding using a difference expansion", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[23] Y. Yu Tsai, J. T. Chen, and C. S. Chan, "Exploring LSB substitution and pixel-value differencing for block-based adaptive data hiding", *International Journal of Network Security*, vol. 16, no. 5, pp. 359–364, 2014.

[24] H. W. Tseng and C. P. Hsieh, "Prediction-based reversible data hiding", *Information Sciences*, vol. 179, no. 14, pp. 2460–2469, 2009.

[25] University of Southern California, *The USC-SIPI Image Database*, Sept. 15, 2015. (`http://sipi.usc.edu/database/database.php`)

[26] D. Wu, W. Tsai, "A steganographic method for images by pixel-value differencing", *Pattern Recognition Letters*, vol. 24, pp. 1613–1626, 2003.

[27] X. T. Zeng, Z. Li, L. D. Ping, "Reversible data hiding scheme using reference pixel and multi-layer embedding", *AEU International Journal of Electron Communication*, vol. 66, no. 7, pp. 532–539, 2012.

Biswapati Jana is currently working as an Assistant Professor in the Department of Computer Science, Vidyasagar University, Paschim Medinipur, India. He received his B. Tech. and M. Tech. degrees in Computer Science and Engineering from University of Calcutta in 1999 and 2002 respectively. His research interests include Image Processing, Data Hiding and Steganography. He has published more than ten papers in National and International Conferences.

Dr. Debasis Giri did his masters (M.Tech and M.Sc) both from IIT Kharagpur, India and also completed Doctorate from IIT Kharagpur, India. He is ten-th all India rank holder in Graduate Aptitude Test in Engineering in 1999. He has published more than 25 papers in international journal/ conference. His current research interests include Cryptography, Information Security, E-commerce security and Design & Analysis of Algorithms. He is Editorial Board Member and Reviewer of many International Journals. He is also Program Committee Member of International Conferences. He is a life member of Cryptology Research Society of India.

Dr. Shyamal Kumar Mondal is currently Associate Professor in the Department of Applied Mathematics With Oceanology And Computer Programming, Vidyasagar University. He did his Ph.D. from Vidyasagar University in 2004, M.Tech from ISM, Dhanbad in 1999 and M.Sc from Vidyasagar University in 1994. His research interest include Operations Research, Meteorology, Fuzzy Set Theory, Soft Set Theory, Soft Computing and Data Hiding. He has published more than 50 papers in National and International Journals/Conferences.

An Improved Automatic Search Method for Differential Trails in TEA Cipher

Kaihao Chen[1], Xiaoming Tang[1], Peng Xu[2], Man Guo[3], Weidong Qiu[1], Zheng Gong[4,5]
(Corresponding author: Peng Xu)

School of Information Security Engineering, Shanghai Jiao Tong University[1]
Dongchuan Road 800 Minhang, 200240 Shanghai, P.R. China
Institute of Information Technology, Police Training Institute[2]
250002 Shandong, P.R. China
(Email: 18053122000@189.cn)
Torch High Technology Industry Development Center, Ministry of Science and Technology[3]
School of Computer Science South China Normal University[4]
State Key Laboratory of Information Security, Institute of Information Engineering[5]
(Received Dec. 23, 2014; revised and accepted July 4 & Aug. 12, 2015)

Abstract

TEA (Tiny Encryption Algorithm) is a block cipher with simple ARX (addition, rotation, exclusive-OR) based Feistel network, designed for both hardware and software scenario. Inspired by the auto search algorithm for ARX cipher introduced by Biryukov and Velichkov in 2014, we proposed an improved version of auto search algorithm for ARX cipher and verified in block cipher TEA. By introducing a sorted partial difference distribution table (sorted pDDT), our algorithm can eliminate lots of branches in advance during differential trail search phase. As time of the search algorithm increase exponentially with the rounds increasing, our algorithm make a great improvement in the search performance.

Keywords: ARX, automatic search, differential trail, sorted pDDT, TEA

1 Introduction

In the past decades, lots of light weight primitives are published for the application of limited resource scenario. For the purpose of simplicity, some of those light weight block ciphers, such as TEA [12], and XTEA [8], use the ARX based design concept, which is combined by a small set of simple operations such as modular addition, bit shift and XOR (exclusive-OR). The ARX based design concept is simple and can be implemented efficiently both in software and hardware.

For the cryptanalysis of ARX based primitives, many techniques is used for the security evaluation such as rotational cryptanalysis [3], integral Zero-Correlation attack [11], etc. However Differential cryptanalysis is still a basic tools during the cryptanalysis of ARX cipher. In differential attack, attackers try to recover the secret key by exploiting the high differential probability pattern of the cipher. Finding a good differential pattern became a key step of the attack. Originally, the search procedure of a good differential pattern is a manual work, therefore the search of high probability differential alway fails for modern block cipher due to the high diffusion properties.

In [6], a branch-and-bound strategy is firstly applied to an automatic search approach of differential and linear trail proposed by Matsui. The author demonstrate a search algorithm for the differential and linear trail and practically apply to block cipher DES. Matsui's algorithm treated the the search procedure of differential and linear trail as a search over a tree of possible solution, in which every non-linear operation is a node with many possible difference or linear mask. By cutting off the paths which is not leading to an optimal solution, the author efficiently derive the best differential and linear trail of DES.

In [2], Biryukov and Velichkov proposed the first extension of Matsui's automatic search algorithm for differential trails in ARX based block cipher. Since the DDT (differential distribution table) for one round ARX operation requires $2^{3n} \times 4$ bytes of memory for n bit block size, it is unlikely to delivery an optimized result using the original Matsui's search algorithm on current computation power. To solve this memory and computation complexity issue, the author introduced a pDDT (partial differential distribution table) to search algorithm, which contains all the high probability differentials with respect to a fixed threshold. By using pDDT and high way & country road concept, the author successfully find the first full differential trails for block cipher TEA. The best result covers 18 round with one round advance comparing to the best differential attack on TEA(17 rounds). Also the author

present a lot of differential trails search result in XTEA, RAIDEN [9] and SPECK [1].

Contribution. In this paper, we proposed an improved version of threshold search algorithm based on Biryukov's differential search algorithm. By using a sorted pDDT approach, our improved version of search algorithm can cut off more unnecessary branches in advance. Comparing to the original search algorithm, our search algorithm is more efficiency and make a great improvement in the time complexity. We verify the search result practically in block cipher TEA, and we present the detail of comparison results with original search algorithm in the second part of our paper.

The contents of this paper are organized as follows. Part 2 gives a brief introduction of block cipher TEA and differential. Part 3 introduces automatic search for differential trail in ARX ciphers. In Part 4, we give a detailed description of our improved version of differential search algorithm and analyze the improvement it makes. We did the experiments in Part 5 and show the comparison with original algorithm. At last we give our conclusion in Part 4.

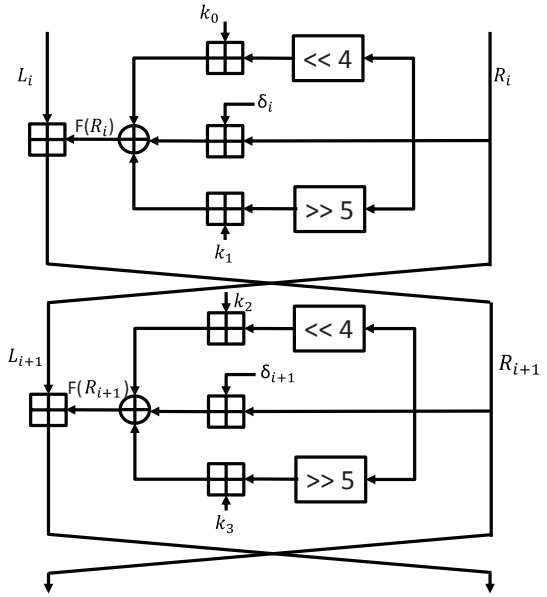


Figure 1: Two-round Feistel structure of TEA

2 Preliminaries

2.1 Notation

We use following notions in this paper:

L_i:	The left half of the i round input.
R_i:	The right half of the i round input.
K:	128-bit master key.
k_i:	The round key ($i = 0, 1, 2, 3$).
δ_i:	The round constant used in the i-th round.
$+$:	Addition modular 2^n
$\oplus$:	Exclusive-OR
$x\|y$:	Concatenation of two bit strings x and y.
$\#A$:	The number of elements in the set A
B_n:	Probability of the best n-round trail
$\widehat{B}_n$:	Probability of the best found n-round trail
$\bar{B}_n$:	An estimation for the best n-round probability

2.2 A Brief Introduction of Block Cipher TEA

Block cipher TEA was designed by Wheeler and Needham of the Cambridge Computer Lab and first presented at the FSE in 1994 [12]. It has a Feistel structure with a ARX based F function. Block cipher TEA takes a 64-bit plaintext as input and has a total of 64 iteration rounds. For the purpose of less memory usage, the round keys of block cipher TEA are derived from the 128-bit master key directly as $K = k_3|k_2|k_1|k_0$. A round constant δ_i is added in every round to prevent the slide attacks. We define the F-function as (for odd rounds):

$$F(x) = ((x \ll 4) + k_0) \oplus (x + \delta_r) \oplus ((x \gg 5) + k_1)$$

The encryption procedure are depicted more intuitively in Figure 1. Given the inputs L_i and R_i of round i, the output is calculated as: $L_{i+1} = R_i$, $R_{i+1} = L_i + F(R_i)$. The operations used in its Feistel structure is modular addition instead of XOR. More details of block cipher TEA, readers can refer to the paper [12].

3 Differential Analysis in ARX and Threshold Search

3.1 Differential Analysis in ARX Based Cipher

In traditional differential cryptanalysis, differential trail is considered using XOR differences. However, for lots of primitives, such as TEA, additive differences are more appropriate for the differential cryptanalysis since the round key and round constants are add-ed. In such primitives, the estimation of differential probability using ADD is more accurate than using XDP (XOR differential probability). Moreover, the number of ADD vs. XOR operations in TEA in one round is larger and then more components are linear in the round function, it is more suitable to use ADD difference instead of XOR difference in differential cryptanalysis in such primitives. The definition of ADP (addition differential probability) as below:

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) =$$
$$2^{-2n} \cdot \#\{(x, y) : ((x + \alpha) \oplus (y + \beta)) - (x \oplus y) = \gamma\}$$

In paper [4] and [5], the efficient computation method of probabilities $\mathrm{adp}^{\oplus}$and xdp^{+} have been demonstrated, and further generalized using S-function concept in [7] and [10]. We will not present a detailed description here due to the space limitation.

3.2 Partial Difference Distribution Table (pDDT)

Finding a good differential trail remains a great challenge in ARX based block cipher cryptanalysis. Comparing with S-box (substitution box) based block cipher, the ARX design concept uses the operations which is based on bit-level instead of word-level operations of S-box based design. In cryptanalysis of those S-box based block ciphers, the analysis of differential trails is usually considered at word level, and the upper bound of differential trails can be estimated easily through counting of active s-box. However, for the ARX based block cipher, it is inconvenient to estimate the upper bound of differential trails in traditional way since the size of differential table of ARX based block cipher can be considered as extremely large. As a sacrifice of completeness, Biryukov and Velichkov proposed a partial DDT with a pre-defined threshold probability $\mathbf{p}_{\text{thres}}$ in [2] to reduce the search space, which is defined as:

$$(\alpha, \beta, \gamma) \in \text{pDDT} \Leftrightarrow \text{DP}(\alpha, \beta \to \gamma) \geq \mathbf{p}_{\text{thres}}$$

In [2], Biryukov and Velichkov have proved that xdp^+ and $\text{adp}^{\oplus}$ are monotonously decreasing with the word size n bits:

$$p_n \leq p_{n-1} \leq \cdots \leq p_k \leq \cdots \leq p_1 \cdots p_0. \quad (1)$$

In Equation (1), $p_k = \text{DP}(\alpha_k, \beta_k \to \gamma_k)$, $1 \leq k \leq n$. With the property above, they proposed an algorithm using a recursive procedure rather than exponential computation to compute the pDDT. The time complexity of the algorithm depends on $\mathbf{p}_{\text{thres}}$.

3.3 Threshold Search

In [2], Biryukov and Velichkov proposed an extended algorithm to search for the best found differential trail in ARX ciphers named Threshold Search, which is similar to Matsui's branch-and-bound algorithm [6]. The probability of the best found trail so far for the first n rounds is notated as $\bar{B}_n$. Respectively, the probability of the best found trail is $\widehat{B}_n$. Besides, they came up with the concept of highways and country roads. Highways are differentials in pre-computed pDDT H with the probabilities above a pre-defined threshold $\mathbf{p}_{\text{thres}}$, while country roads are differentials with fixed input difference computed on-demand in an intervening round. The country roads are stored in table C with probabilities lower than $\mathbf{p}_{\text{thres}}$ and satisfy following two conditions:

1) Their probabilities are above a minimum value that may still improve $\widehat{B}_n$ i.e. in round r, the country road (α_r, β_r, p_r) (suffix r means round r instead of r-bit word) satisfies that $p_r \geq p_{min} = \bar{B}_n/(p_1 p_2 \cdots p_{r-1} \widehat{B}_{n-r})$;

2) Their output differences β_r ensure that the input difference for the next round is in H i.e. $\alpha_{r-1} + \beta_r = \alpha_{r+1} \in H$ such that it prevents the overload of the size of C.

In Threshold Search, the first two rounds search only explore differential in H as the input differences and the output differences can be freely chosen, therefore restricting the search range into H ensures the search for differential in these rounds are not overloaded. However, from the third round, the input difference is fixed due to the Feistel structure, the algorithm explores differential not only in H but also in C. If one trail search reaches the last round successfully, $\bar{B}_n$ will be updated. The final best found differential trail usually contains as many differentials in H as possible.

4 Improved Differential Search

4.1 Improved Threshold Search Using Sorted pDDT

Our improved Threshold Search is also a branch-and-bound algorithm based on Biryukov's algorithm. We introduced a sorted pDDT to search algorithm to improve elimination rate of unnecessary branches. One of key factors for time complexity of the threshold search is the branch numbers during search phase. If we can cut off the unnecessary branches in earlier phase, the time we used for differential trail search will be less. Therefore, we propose a sorted pDDT to cut off most unnecessary branches in advance. In sorted pDDT, the entries are sorted by input differences in ascending order, probabilities in descending order and output differences in ascending order in sequence. The pseudo-code is given in Algorithm 1.

Temporary table C is used as a pDDT with threshold p_{min} when $p_{min} < \mathbf{p}_{\text{thres}}$. We assume that if the largest probability in certain round r is chosen at the beginning stage, it has more chance to reach last round and p_{min} will be updated as well as $\bar{B}_n$. If p_{min} increased, less entries in H or C need to be traversed probably. It's easy to stop traversing efficiently if p_{min} isn't satisfied due to their sorting sequence. In original algorithm, C and H may have some entries in common. To solve this issue, we add maximum probability condition i.e. $\mathbf{p}_{\text{thres}}$ when building C to avoid traversing repeated entries.

We optimize the algorithm in the following routine:

1) Process in the first two and the last round is the same as Threshold Search;

2) From the third round onwards to round r, determine the required minimum probability, i.e. $p_{min} = \bar{B}_n/(p_1 p_2 \cdots p_{r-1} \widehat{B}_{n-r})$;

3) If $p_{min} \geq \mathbf{p}_{\text{thres}}$, it is unnecessary to calculate table C, and we only explore the entries in H with certain fixed input difference α_r and probabilities above p_{min} rather than all with certain fixed input difference, since H is a sorted pDDT;

Algorithm 1 Improved Threshold Search Based on Sorted pDDT

Input: **n**: number of rounds; **r**: current round; **H**: sorted pDDT; $\widehat{\mathbf{B}} = (\widehat{\mathbf{B}}_\mathbf{1}, \widehat{\mathbf{B}}_\mathbf{2}, \cdots, \widehat{\mathbf{B}}_{\mathbf{n-1}})$: probabilities of best found trails for the first $(n-1)$ rounds; $\widehat{\mathbf{B}}_\mathbf{n}$: initial estimate; $\bar{\mathbf{T}} = (\bar{\mathbf{T}}_\mathbf{1}, \bar{\mathbf{T}}_\mathbf{2}, \cdots, \bar{\mathbf{T}}_{\mathbf{n-1}})$: trail for n rounds with probability $\bar{B}_n$; $\mathbf{p}_{\text{thres}}$: probability threshold.
Output: $\widehat{\mathbf{B}}_\mathbf{n}, \widehat{\mathbf{T}} = (\widehat{\mathbf{T}}_\mathbf{1}, \widehat{\mathbf{T}}_\mathbf{2}, \cdots, \widehat{\mathbf{T}}_{\mathbf{n-1}})$: trail for n rounds with probability $\widehat{B}_n$.

function THRES_SEARCH_SORTED_PDDT($n, r, H, \widehat{B}, \bar{B}_n, \bar{T}$, p$_{\text{thres}}$)
  if $((r = 1) \vee (r = 2)) \wedge (r \neq n)$ **then**
    for all (α, β, p) in H **do**
      $p_r \leftarrow p, \widehat{B}_n \leftarrow p_1 p_2 \cdots p_r \widehat{B}_{n-r}$
      if $\widehat{B}_n \geq \bar{B}_n$ **then**
        $\alpha_r \leftarrow \alpha, \beta_r \leftarrow \beta$
        add $\widehat{T}_r \leftarrow (\alpha_r, \beta_r, p_r)$ to $\widehat{T}$
        THRES_SEARCH_SORTED_PDDT($n,\ r+1,\ H,\ \widehat{B},\ \bar{B}_n,\ \widehat{T}$, p$_{\text{thres}}$)
      end if
    end for
  end if
  if $(r > 2) \wedge (r \neq n)$ **then** $\alpha_r \leftarrow (\alpha_{r-2} + \beta_{r-1})$
    $P_{r-1} \leftarrow p_1 p_2 \cdots p_{r-1} \widehat{B}_{n-r}, p_{r,min} \leftarrow \bar{B}_n / P_{r-1}$
    if $p_{r,min} \leq 1.0$ **then**
      for all $\beta_r : (p_r(\alpha_r \rightarrow \beta_r) \geq p_{r,min}) \wedge ((\alpha_r, \beta_r, p_r) \in H)$ **do** add $\widehat{T}_r \leftarrow (\alpha_r, \beta_r, p_r)$ to $\widehat{T}$
        THRES_SEARCH_SORTED_PDDT($n,\ r+1,\ H,\ \widehat{B},\ \bar{B}_n,\ \widehat{T}$, p$_{\text{thres}}$), $p_{r,min} \leftarrow \bar{B}_n / P_{r-1}$
      end for
      if $p_{r,min} <$ p$_{\text{thres}}$ **then** $C \leftarrow \emptyset$
        for all $\beta_r : (p_r(\alpha_r \rightarrow \beta_r) \geq p_{r,min}) \wedge ((\alpha_{r+1} + \beta_r) = \gamma \in H)$ **do** add (α_r, β_r, p_r) to C
        end for
        if $(C = \emptyset) \wedge ((\beta_r, p_r) \leftarrow p_r = \max_\beta p(\alpha_r \rightarrow \beta) \geq p_{r,min})$ **then** add (α_r, β_r, p_r) to C
        end if
        if $(C \neq \emptyset)$ **then**
          for all $(\alpha, \beta, p) \in C \wedge (p_{r,min} <$ p$_{\text{thres}})$ **do** add $\widehat{T}_r \leftarrow (\alpha_r, \beta_r, p_r)$ to $\widehat{T}$
            THRES_SEARCH_SORTED_PDDT($n,\ r+1,\ H,\ \widehat{B},\ \bar{B}_n,\ \widehat{T}$, p$_{\text{thres}}$), $p_{r,min} \leftarrow \bar{B}_n / P_{r-1}$
          end for
        end if
      end if
    end if
  end if
  if $r = n$ **then** $\alpha_r \leftarrow (\alpha_{r-1} + \beta_{r-2})$
    if $(\alpha_r$ in $H)$ **then**
      $(\beta_r, p_r) \leftarrow p_r = \max_{\beta \in H} p(\alpha_r \rightarrow \beta)$
    else $(\beta_r, p_r) \leftarrow p_r = \max_\beta p(\alpha_r \rightarrow \beta)$
    end if
    $p_n \leftarrow p_r, \widehat{B}_n \leftarrow p_1 p_2 \cdots p_n$
    if $\widehat{B}_n \geq \bar{B}_n$ **then** $\alpha_n \leftarrow \alpha_r, \beta_n \leftarrow \beta$
      add $\widehat{T}_n \leftarrow (\alpha_n, \beta_n, p_n)$ to $\widehat{T}$
      $\bar{B}_n \leftarrow \widehat{B}_n, \bar{T} \leftarrow \widehat{T}$
    end if
  end if
  $\widehat{B}_n \leftarrow \bar{B}_n, \widehat{T} \leftarrow \bar{T}$
  return $\widehat{B}_n, \widehat{T}$
end function

4) If $p_{min} < \mathbf{p}_{\text{thres}}$, table C may be needed but we won't compute it immediately. We search for the entries with the fixed input difference in table H and choose the largest one to proceed to the next round first if we sucessfully find them. When the algorithm backtracks gradually to round r, the p_{min} may be updated and we choose the next entry in table H which still satisfies p_{min};

5) After exploring table H and if still $p_{min} < \mathbf{p}_{\text{thres}}$, we begin to compute a pDDT C under the conditions mentioned in Section 3.3;

6) Explore the entries in table C in pre-defined order, update p_{min} dynamically when the recursion backtracks, and terminate if the probability does not satisfy p_{min};

7) After exploring table H and C if needed, recursion returns and backtracks to the previous round i.e. $(r-1)$.

Compared with original algorithm, the sorted pDDT is required to be calculated instead of pDDT. Since it's easy to implement the sorted list with the underlying programming languages like C/C++ and inserting and finding operations in sorted list costs little extra time compared with ordinary list, the proposed idea have less extra computation costs.

In addition, we add P_{r-1} as the multiplication of constructed $(r-1)$-round trail probability and best found trail probability for the first $(n-r)$ rounds. Being similar as Biryukov's Threshold Search, Algorithm 1 operates by recursively extending a trail from i rounds to $(i+1)$ rounds, beginning with $i = 1$ and terminating at $i = n$. The recursion at level i is performed to level $(i+1)$ only if the multiplication of constructed i-round trail probability and best found trail probability for $(n-i)$ rounds is at least $\bar{B}_n$, i.e., $p_1 p_2 \cdots p_i \widehat{B}_{n-i} \geq \bar{B}_n$ or $p_i \geq \bar{B}_n / (p_1 p_2 \cdots p_{i-1} \widehat{B}_{n-i})$. For $i = n$ the last equation is equivalent to: $p_1 p_2 \cdots p_n = \widehat{B}_n \geq \bar{B}_n$. If the latter holds, the initial estimate is updated: $\bar{B}_n \leftarrow \widehat{B}_n$ and the corresponding trail is also updated accordingly: $\bar{T}_n \leftarrow \widehat{T}_n$.

As a result of our investigation, the sorted pDDT proposed above makes more contribution in table C than table H as the entries with certain fixed input difference in H are within a small amount or even none, thus it cuts off rare branches.

4.2 Evaluation of the Proposed Algorithm

Both original algorithm and Algorithm 1 will finish when the initial estimate $\bar{B}_n$ can't be improved any more. We found that the probability order of entries in C also have great influence on time complexity. If the entries with greater probability are more likely to update $\bar{B}_n$ in the last round, the updated p_{min} may reduce the explore of some remaining entries with smaller probability.

Table 1: Search time of the original and the proposed algorithm. Environment: Intel(R) Core(TM) i5-3470 CPU, 3.20GHz, 8GB RAM

Rounds	Time per round (original)	Time accumulation (original)	Time per round (Algorithm 1)	Time accumulation (Algorithm 1)
1	0.001 s	0.001 s	0.002 s	0.002 s
2	0.006 s	0.007 s	0.004 s	0.006 s
3	1.901 s	1.908 s	1.860 s	1.866 s
4	1 m 2 s	1 m 3 s	48.010 s	49.876 s
5	3 m 37 s	4 m 40 s	25.553 s	1 m 15 s
6	10 m 30 s	15 m 10 s	6 m 38 s	7 m 53 s
7	13 m 26 s	28 m 35 s	8 m 22 s	16 m 16 s
8	23 m 12 s	51 m 47 s	13 m 0 s	29 m 16 s
9	25 m 23 s	1 h 17 m 10 s	12 m 46 s	42 m 2 s
10	19 m 8 s	1 h 36 m 18 s	6 m 38 s	48 m 40 s
11	8 m 17 s	1 h 44 m 35 s	2 m 35 s	51 m 15 s
12	19 m 11 s	2 h 3 m 45 s	6 m 47 s	58 m 2 s
13	19 m 23 s	2 h 23 m 8 s	6 m 59 s	1 h 5 m 0 s
14	22 m 1 s	2 h 45 m 10 s	4 m 3 s	1 h 9 m 4 s
15	10 m 29 s	2 h 55 m 38 s	1 m 48 s	1 h 10 m 52 s
16	33 m 0 s	3 h 28 m 38 s	5 m 27 s	1 h 16 m 19 s

The experiment result of the proposed algorithm is presented in the next section.

5 Experiments of the Improved Threshold Search

We applied Algorithm 1 to TEA with additive difference. In our experiment, we ignore the influence of the round constants, the round keys dependence just for a comparison with the original algorithm.

The comparison results are presented in Table 1. Column (Time per round) lists the search time for the best found trail of n rounds, given the probabilities $\widehat{B}_1$, $\widehat{B}_2$, $\cdots$, $\widehat{B}_{n-1}$ of best found trails for the first 1, 2, $\cdots$, $n-1$ rounds. Column (Time accumulation) is the time summation for n rounds, if $\widehat{B}_1$, $\widehat{B}_1$, $\cdots$, $\widehat{B}_{n-1}$ not known. From the table it shows that the proposed algorithm improves the search performance effectively and speed up in an approximate range from 1 to 8 times without changing the best found trails. It is difficult to estimate and quantize the elimination rates of unnecessary branches during the search phase, however, we state that the improvement will be more effective for the ARX block cipher with more rounds.

6 Conclusions

In this paper, we proposed a improved version of automatic search algorithm with a sorted pDDT concept to ARX block cipher. By using sorted pDDT concept, which has input differences in ascending order, probabilities in descending order and output differences in ascending order in sequence, we can reduce the exploring amount of temporary table C to eliminate most of search branches. We verify the improvement experimentally on the block cipher TEA, and give the search results and timing costs compared with the original Biryukov's search algorithm. The result shows, using the our improved algorithm with sorted pDDT concept, search performance has remarkably improvement. The further improvement and analysis on the more types of ARX block cipher will be our further research direction.

Acknowledgments

The research work was supported by New Century Excellent Talents in University of Ministry of Education under Grant NCET-12-0358, Technology Innovation Research Program of Shanghai Municipal Education Commission under Grant 12ZZ019 and Supporting Program of the "Twelfth Five-year Plan" for Sci and Tech Research of China under Grant 2014BAK06B02. Zheng Gong is also supported by the National Natural Sciences Foundation of China under Grant No. 61572028, the Natural Science Foundation of Guangdong (No.2014A030313439), the Foundation for Distinguished Young Teachers in Higher Education of Guangdong under Grant No. Yq2013051, and the Project of Science and Technology New Star of Guangzhou Pearl River (2014J2200006).

References

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The simon and speck families of lightweight block ciphers," *IACR Cryptology ePrint Archive*, vol. 2013, pp. 404, 2013.

[2] A. Biryukov and V. Velichkov, "Automatic search for differential trails in arx ciphers," in *Topics in Cryptology (CT-RSA'14)*, pp. 227–250, Springer, 2014.

[3] D. Khovratovich, I. Nikolic, J. Pieprzyk, P. Sokolowski, and R. Steinfeld, "Rotational cryptanalysis of arx revisited," *IACR Cryptology ePrint Archive*, vol. 2015, pp. 95, 2015.

[4] H. Lipmaa and S. Moriai, "Efficient algorithms for computing differential properties of addition," in *Fast Software Encryption*, pp. 336–350, Springer, 2002.

[5] H. Lipmaa, J. Wallén, and P. Dumas, "On the additive differential probability of exclusive-or," in *Fast Software Encryption*, pp. 317–331, Springer, 2004.

[6] M. Matsui, "On correlation between the order of S-boxes and the strength of DES," in *Advances in Cryptology (EUROCRYPT'94)*, pp. 366–375, Springer, 1995.

[7] N. Mouha, V. Velichkov, C. De Cannière, and B. Preneel, "The differential analysis of s-functions," in *Selected Areas in Cryptography*, pp. 36–56, Springer, 2011.

[8] R. M. Needham and D. J. Wheeler, *TEA Extensions*, Oct. 1997. (`http://www.cix.co.uk/~klockstone/xtea.pdf`)

[9] J. Polimón, J. C. Hernández-Castro, J. M. Estévez-Tapiador, and A. Ribagorda, "Automated design of a lightweight block cipher with genetic programming," *KES Journal*, vol. 12, no. 1, pp. 3–14, 2008.

[10] V. Velichkov, N. Mouha, C. De Canniere, and B. Preneel, "The additive differential probability of arx," in *Fast Software Encryption*, pp. 342–358, Springer, 2011.

[11] L. Wen and M. Wang, "Integral zero-correlation distinguisher for ARX block cipher, with application to shacal-2," in *Information Security and Privacy*, pp. 454–461, Springer, 2014.

[12] D. J. Wheeler and R. M. Needham, "TEA, a tiny encryption algorithm," in *Fast Software Encryption*, pp. 363–366, Springer, 1995.

Kaihao Chen M.E., works in Lab of Cryptography and Computer Forensics, School of Information Security Engineering, Shanghai Jiao Tong University. He received B.E. in 2013 from Shanghai Jiao Tong University. His recent research directions are high performance parallel computing on GPU and analysis of block ciphers.

Xiaoming Tang Ph.D. candidate, School of Information Security Engineering Shanghai Jiao Tong University. His recent research directions are cryptography, including analysis of block ciphers and hash functions.

Peng Xu received the M.E. degree from the School of Information Science and Engineering, Shandong University, in 2008. His main research areas include prison informatization, information security, Internet of things and he has published more than 15 papers. Currently, he is the project leader of the Research and Demonstration of the Key Technology in Prison Intelligent Security System Construction of 2014 National Science and Technology Supporting Program, and is responsible for the study of the Research and Demonstration of the Key Technology in the Intelligent Analysis and Recognition System of Criminal Behavior. At the same time, he is appointed as the expert of the information construction of justice department and the member of the expert group of the Ministry of Science and Technology.

Man Guo got Master degree on Management Science and Engineering from Chinese Academy of Agricultural Science. Now she works as the Program Officer on Science & Technology Management at Torch High Technology Industry Development Center, Ministry of Science and Technology for more than 6 years. She also has 2-year work experiences as Program Officer in State Nuclear Power Technology Corporation. She has published more than ten academic papers on Mass entrepreneurship and innovation and S&T talent team construction.

Weidong Qiu received the M.S. degree in cryptography from Xidian University, Xi'an, China, in 1998, and Ph.D. degree in computer software theory from Shanghai Jiao Tong University, Shanghai, China, in 2001. Before he joined Shanghai Jiao Tong University in 2004, he was a Postdoctoral Fellow at Hagen FernUniversity, Hagen, Germany, from 2001 to 2003. He is currently a Professor in the School of Information Security and Engineering, Shanghai Jiao Tong University. He has published more than twenty academic papers on cryptology. His main research areas include cryptographic theory, technology of network security, and computer forensics.

Zheng Gong received Ph.D. in 2008 from Shanghai Jiao Tong University, China. From 2008 December to 2012 January, he was a postdoc in the DIES group of Twente University. Currently he is an associate professor of Computer Science at South China Normal University. His recent research directions are cryptography and provable security, including the design and analysis of block ciphers, hash functions and message authentication codes.

A Survey of Public Auditing for Shared Data Storage with User Revocation in Cloud Computing

Chi-Wei Liu[1], Wei-Fu Hsien[2], Chou-Chen Yang[2], and Min-Shiang Hwang[1,3]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan (R.O.C.)
(Email: mshwang@asia.edu.tw)
Department of Management Information System, National Chung Hsing University[2]
Department of Medical Research, China Medical University Hospital, China Medical University[3]
No. 91, Hsueh-Shih Road, Taichung 40402, Taiwan (R.O.C.)
(Received May 25, 2015; revised and accepted July 13 & Aug. 4, 2015)

Abstract

Cloud computing technology has matured, so cloud computing produces a wide range of cloud service. Cloud storage services are one of cloud services where cloud service provider can provide storage space to customers. Because cloud storage services bring a lot of convenience, many enterprises and users store the data to the cloud storage. However, the user will outsource data to the cloud storage service, but the user is difficult to manage remote data in the cloud. Therefore, how users verify data integrity is a major challenge. In recent years, public audit is used to verify data integrity by which the user allows other to verify the user's data. Because the feature of cloud service allows users to communicate with each other on the cloud platform, the cloud storage service allows the data owner to share their data to other users. Therefore, public auditing extends to the share data, so the original operation becomes not the same including signature, public audits, dynamic data and user revocation which generates on the situation of shared data. In the paper, we define the requirements of public auditing with shared data and explain four representative approaches which include analysis function, security, and performance requirements. Finally, we provide some topics for future research.

Keywords: Cloud computing, public auditing, share data, user revocation

1 Introduction

Cloud computing is a computing technology, and the internet has grown in recent years. It can share the software and hardware resource, and provide resources to a user's computer or mobile device. The user can obtain a more efficient service because cloud computing can integrate resources. Therefore, in order to achieve cloud computing technology, it must satisfy five basic features: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity and Measured service [40]. However, it is very difficult for general users or small and medium enterprises to construct could environment because they cannot afford the huge costs. Therefore, many information technology companies are finding business opportunities in cloud services. Thus, cloud service providers have joined to build could environments to provide services to the user. Cloud service providers offer three services including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The cost for users to rent cloud service is cheaper than the cost for users to build cloud environment [1].

Cloud storage service is the most common and popular service among many cloud services (e.g. Google Drive, Dropbox, Amazon S3 and Microsoft OneDrive) for general users. However, users have a bottleneck on the local side storage space because a user needs a large storage space to store a huge amount of data on the situation. Cloud storage service has high capacity and high computation that solve users' difficult problems. Moreover, a user builds a larger storage device which is more expensive than rented cloud storage service. Besides, the user can pay the cloud server provider based on the amount of usage. Then, because cloud storage service provides to access cloud services from web service or applications that utilize the application programming interface (API) by mobile devices (e.g. laptop, table computer, and smart phones), it is convenient to use by users, and it achieves

an ubiquitous service.

Although a cloud storage services has many advantages, it brings a lot of challenging issues which include efficacy and security [26, 34, 38, 46, 47, 48, 63]. One of the big challenges is verifying the integrity of the data because users cannot know how the cloud storage service handles their data. These cloud storage services are provided by commercial enterprises, so it cannot be fully trusted by users. Therefore, the cloud service provider may hide data loss and data errors in the service because of their benefits. However, it is very serious that a user stores data in an untrusted cloud storage. For example, the traditional approach is to download the entire data from the cloud, and then verify data integrity by checking the correctness of digital signatures or hash values of the entire data. Surely, this simple approach is able to check users' data integrity in cloud. However, this is not efficient in the conventional approach because the user spends a lot of resources of communication, computation and storage. Besides, due to a large size of outsourced data and a user's limited resource capability, a user has to find an efficient way to achieve integrity verifications without the local copy of data files.

In order to solve the problem of data integrity verification in the cloud storage service, many studies present different methods and security models [2, 3, 4, 16, 19, 24, 32, 61, 62]. Sookhak et al. [47] surveyed remote data auditing in cloud computing and classified three methods in the following.

First method is named probable data possession (PDP) by Ateniese et al. [2]. They utilized the RSA-based Homomorphic verifiable tag (HVT) to verify the integrity of data storage in the cloud without retrieving the entire data. However, the PDP cannot support to change these stored data which is named static PDP model included [2, 20, 25, 27]. To support dynamic data update in the cloud, Ateniese et al [4] applied symmetric-key cryptography to scalable PDP which is named dynamic PDP included [4, 23, 53]. Wang et al. [50] considered data privacy when TPA verified user's data. TPA can piece together authentication of users' data because TPA can verify users' data on process of public auditing. Thus, it creates data privacy issues. Wang et al. [50] utilized a random mask technology to design an improved approach which can avoid TPA learning users' data which is named privacy-preserving PDP included [62, 33, 50, 54]. Robust PDP including Ateniese et al. [3] utilized a spot-checking mechanism to detect a part of the data corruption, Ateniese et al. [3] utilized forward error checking (FRC) to enhance the arbitrary amount of data corruption and B. Chen and Curtmola [19] utilized a robust dynamic PDP to support error detection of dynamic data update. Second method is named proof of retrievability (POR) by Juels and Kaliski [32]. They embedded the special blocks (named sentinels) to the data and checked the correctness of the sentinels to achieve POR. However, the POR only suits static data storage because dynamic data effects the position of the sentinels. Static POR includes [32, 43, 58]. Cash et al. overcame the difficult problem and improve a dynamic POR [16]. Zheng and Xu proposed a fair and dynamic POR on the 2-3 range tree structure [61]. Third method is named proof of ownership (POW) which considers data deduplication to improve efficient data storage and include [24, 29, 45, 60].

In these studies, the role of the verifier can fall into two categories: privacy verification and public verification. Private verification implies the data owner directly verifying data in the cloud storage service is an efficient way. Public verification implies the data owner allowing other to verify the data owner's data is inefficient because it needs to delegate other verifier by the data owner. In general, a user may have a lot of data files which are stored in cloud storage service. However, a user cannot frequently verify he/she data because it will consume his/her resources so not to process other action. In order to achieve an efficient verification of data integrity, Wang et al. [53] proposed a public auditing scheme where a user can delegate a third party auditor (TPA) to assist the validation reduction to consume his/her computing resources. Then, there are related research bases on Wang et al.'s scheme [53]. Zhu et al. [56] designed another public auditing scheme which can support dynamic data update. With more and more data, it brings new challenges in data integrity. Public auditing for big data storage in the cloud will bring new challenges [18, 38]. Liu et al [36] proposed an efficient verification of fine-grained data update scheme which can support public auditing of big data storage. However, to enhance user's data reliability and availability in the cloud, the cloud server will backup copy user's data. When the user updates data, there backup copy also needs to update. Liu et al. [37] considered cloud server efficiently updates multiple replicas and enhances data availability in the cloud.

Cloud storage service can not only store data but also share information with other users in a group. However, these studies [21, 22, 31, 35, 36, 37, 50, 51, 52, 53, 56] do not consider another advantage of cloud where a user can share data with another user on cloud storage service. Users can share data in the cloud because the cloud platform provides communication between users and others. Therefore, it is very convenient a user wants to share data with another user because this need not be transferred to another user data after downloading. However, users share data in the cloud storage service which still has a problem on the data integrity. Therefore, many recent studies extend public auditing for shared data in the cloud [8, 9, 10, 11, 12, 13, 15, 28, 30, 49, 57, 59]. Because the data is shared with multiple users, it needs to consider dynamic data update of multiple users. When the shared user modifies the shared data block, the shared user need to sign the data block. For example, the user A shares own data with other users (like the user B) in the cloud storage service, and the data is divided into several parts of data blocks which are signed by the user A. The user A allows the user B modifying the user A's data block but the user B has to sign the modified data block. When the

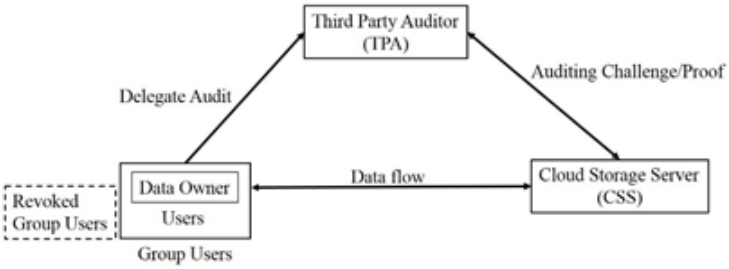


Figure 1: Public auditing with shared data in cloud data storage architecture

user B modifies the shared data block, the user B needs to use his/her private key to sign the modified block. In order to correct the integrity of audit data, the TPA needs to select the corresponding public key to verify the data block (e.g., a data block was signed by user A and it is only correctly verified by user A's public key). Therefore, in the public auditing phase, it is still a problem of identity privacy. However, when a user is revoked from the group because of his/her malicious behavior. The shared data block is signed by the revoked user which needs to be re-signed by the exist user of the group. Therefore, public auditing for shared data has a lot of studies and the system architecture is shown in Figure 1. In the Section 3, we will detail representative approaches [8, 11, 28, 59].

1.1 Requirements

According to [8, 11, 28, 50, 53, 59] studies, they provide the basic requirements of function, security and performance. In our paper, we classify and describe these requirements. Then we use these requirements to analyze the existing scheme in Section 4.

Functional evaluation.

1) Blockless Verification: the auditor can verify data blocks, and needs not to retrieve all audited data blocks in the cloud storage service.
2) Stateless Verification: the auditor need not maintain and update data situation because data situation is maintained by the client and cloud storage service together.
3) Batch Auditing: the auditor can verify the data of different clients at the same time because the auditor can be delegated by a lot of clients.
4) Dynamic Data: the data owner can insert, modify and delete data blocks in the cloud storage service because their data can be continuously updated at any time.
5) Anonymity: the auditor cannot distinguish the identity of the signer on each block during the process of public auditing.
6) Privacy Presenting: the auditor cannot get knowledge to delegate data from the response of the cloud storage service.
7) User Revocation: a user is revoked from the group before an existing user can generate a valid signature on shared data of the blocks signed by the revoked user. The revoked user cannot re-compute valid signatures on shared data.

Security attack evaluation. We list some common attack model and they can analyze whether public auditing scheme can resist the malicious attacker [28, 39].

1) Inside attack: the insiders of the cloud service provider have permission to obtain the client's data in the cloud storage, and take these data to exchange benefits.
2) Forge attack: the cloud server can forge the data tag of data block and deceive the third party auditor.
3) Replace attack: the server can choose another valid pair of data block and data tag (m_i, σ_i) to replace the challenged request (m_j, σ_j), when it already discarded data block or data tag m_i or σ_i.
4) Impersonation attack: an adversary obtains authenticated information of the data owner and cloud storage service and forges another message to pass the verification. Then, the adversary fakes a legal client or cloud storage service and cheats other side.
5) Collusion attack: a revoked user can collude with the malicious cloud server to change the group's shared data.

Performance evaluation.

1) Computing cost: In order to achieve an efficient public auditing, we will analyze the client, TPA and cloud storage service cost on the computing resources.
2) Storage cost: Because the client will upload data to the cloud storage service without the local copy of data files, we will analyze the client, TPA and cloud storage service cost on the storage spaces.

1.2 Contribution

Our contribution can be summarized as the following three aspects: First, we survey the previous researches of public auditing for shared data in the cloud. Then, our paper collect and explain basic requirements in the mechanism. Second, we propose four representative approaches and analyze these approaches by our collected requirements. Third, we summarize the conclusion from the analysis and propose research direction in future work.

1.3 Organization

The rest of paper is organized as follows: In Section 2, we review the related work of public auditability. We discuss the representative approaches of public auditability in detail in Section 3. In Section 4, we analyze the basic requirement in the representative approaches. Finally, we summarize and discuss the future work in Section 5.

2 Related Work

Public integrity auditing with dynamic data for outsourced data storage has caused related research [21, 22, 31, 36, 37, 52, 56]. Wang et al. [52, 53] first proposed an enabling public auditability and data dynamics in the cloud scheme. Their scheme improves data block inserted operation of dynamic data because the inserted operation affects the entire data block which has been sorted. Therefore, they utilized the Merkle Hash Tree (MHT) [41] data structure and bilinear aggregate signature [6] to address dynamic data which can support dynamic index of data block. They extended their scheme to support batch auditing which can improve efficiency. Wang et al. [21, 51] proposed a challenge-response protocol which can determine the data correctness and locate possible errors. However, their scheme only supports partially dynamic data operation. Wang et al. [21] extended [51] to support privacy-preserving third part auditing and correctness analysis of proposed storage verification design. Wang et al. [22, 50] pointed out that Wang et al.'s scheme [53] has data privacy issues which imply the TPA can get the client's data information. Therefore, they use a random mask technology to avoid TPA learning knowledge on every verification process. Wang et al. [22] extended [50] to support dynamic data and prove a secure zero-knowledge leakage public auditing scheme.

Zhu et al. [56] proposed a dynamic audit services for outsourced storage in clouds. They utilized the fragment structure to reduce the storage of signatures, utilized index hash tables to provide the service of dynamic data operation and utilized periodic sampling audit to enhance data integrity. Li et al. [31, 35] considered that the client's resource-constrained device is simple and lightweight. Therefore, they proposed a scheme which a client can delegate TPA to execute high computing process and solve the client's bottleneck before the client uploads data to cloud server. Li et al. [35] extended [31] to improve the users will need to compute the tags for the outsourced data. Liu et al. [36] thought that previous studies are not efficient in dynamic data update because it is a fixed-size block update. Therefore, they proposed a scheme which can support variable-size blocks in dynamic data update and enhance verification efficiency. Liu et al. [37] considered data reliability and availability in the cloud. Consequently, the cloud server will store multiple replicas to enhance data reliability. However, when the stored data is frequently updated, each dynamic update will affect every replica. Therefore, they proposed a multi-replica Merkle hash tree (MR-MHT) to construct replica sub-tree which can enhance data availability in the dynamic data phase. Then, their scheme can support public auditing.

To enhance the previous works [35, 36, 37, 50, 51, 53, 56], there are studies [9, 10, 12, 13, 14, 28, 30, 49, 57] focused on public auditing with shared data in the cloud. Wang et al. [49] proposed a named Knox scheme which is able to audit the integrity of shared data in the cloud for a large group. Unfortunately, their scheme cannot support public auditing. Wang et al. [8, 9] improved drawback of the Knox scheme which implies public auditing so they designed a named Oruta scheme to support public auditing for shared data integrity. Because their scheme utilized ring signature to protect the privacy of users, it did not support a dynamic group. To achieve user revocation, Wang et al. [10, 11] designed a named Panda scheme which is able to audit the integrity of shared data with user revocation in the cloud. They utilized proxy resignature to update the signed data by the revoked user. To preserve the identity of the signer on each block during public auditing, Wang et al. [13, 15] proposed the user of the group to share a global private key. Then, each user can sign blocks by this global private key. However, when a user of the group is compromised or revoked, a global private key has to be re-generated and shared with the existence of the group which will need huge overheard on key management and key distribution. Wang et al. [12] utilized a certificateless scheme to design the first certificateless public auditing mechanism. Their scheme can reduce security risk in certificate management. Wang et al. [14] utilized a multi-signature scheme to design the first multi-owner public auditing mechanism. For example, the correctness of an official document stored in the cloud is confirmed by all the related members before the official document can be announced. Therefore, their scheme can have efficient multi-signature and verify multi-owner data.

Yuan and Yu [58] designed a polynomial commitment scheme which is able to reduce the communication overhead of verification. Yuan and Yu [30, 59] utilized [58] to design a public integrity auditing scheme with multi-user modification. Their scheme uses polynomial authentication tags and proxy tag update techniques, which support public verification and user revocation. Yuan and Yu [59] extended [30] to prevent a compromise attack where single cloud is internal errors or outside attack when cloud server update the authentication tag from the revoked users. Jiang et al. [28] considered the ciphertext store and efficient user revocation where the data owner cannot take part in a user revocation phase. They prevent malicious operation when the cloud server colludes with the revoked user. In Section 3, we will describe these representative approaches in detail.

Table 1: Notations

Notation	Significance
G_1, G_2, G_T	A multiplicative cyclic group
e	A bilinear map $e : G_1 \times G_2 \to G_T$
g	A generator of group G_1
p	The prime order of group G_1
q	A much smaller prime than p
H_1	A hash function $H_1 : \{0,1\}^* \to G_1$
H_2	A hash function $H_2 : \{0,1\}^* \to Z_p$
H_3	A hash function $H_3 : G_1 \to Z_p$
Ψ	A computable isomorphism $\Psi : G_2 \to G_1$ (e.g. $\Psi(g_2) = g_1$
M	The shared data that will be split into n blocks
m_i	A data block of the shared data and will be split into k elements
k	A block element of the shared data block m_i
d	The total number of users in the group
u_i	ith user of the group
sk_i	The user u_i's private key
pk_i	The user u_i's public key
σ_i	Authentication tag generated for shared data block m_i

3 Representative Approaches

Before introducing representative approaches, we list all notation (as shown in Table 1) using in this paper.

3.1 Wang et al.'s Scheme

Wang et al. [8] was the first to propose the scheme which can support shared data on public auditing at the same time because previous studies only considered a data is used by a single user. Therefore, they proposed a privacy-preserving public auditing mechanism for shared data in cloud by the mechanism of one ring to rule them all (Oruta).

They utilized the concept of ring signature [42] to construct homomorphic authenticators, so TPA is able to verify the integrity of shared data. It can achieve efficient verification without retrieving the entire data. They utilized randomly masking technology from C. Wang et al.'s scheme [50] to protect data privacy from public auditing. Meanwhile, they also utilize index hash tables (IHT) from Zhu et al.'s scheme [56] to support dynamic data. Finally, they extend their mechanism to support batch auditing which can allow public auditing on different users simultaneously and improve the efficiency of verification for multiple auditing tasks.

Next we will describe their schemes including setup, public auditing, dynamic data and user revocation phase. Before executing each phase, the CSS need to generate the global parameters: (e, Ψ, p, q, G_1, G_2, G_T, g_1, g_2, H_1, H_2, H_3, d, n, k). Their scheme is as follows:

Setup phase. In the phase, we will describe key generation and signature.

Step 1: A user u_i randomly chooses $x_i \in Z_p$ and computes $w_i = g_2^{x_i}$. Then the user's public key is $pk_i = w_i$ and private key is $sk_i = x_i$. If the user is original, he/she will randomly generate a public aggregate key $pak = (\eta_1, \cdots, \eta_k)$ where η_l are random elements of G_1.

Step 2: The user u_s chooses a block $m_j = (m_{j,1}, \cdots, m_{j,k})$ and the block identifier id_j. The user uses pak to computes $\beta_j = H_1(id_j)\prod_{l=1}^{k}\eta_l^{m_{j.l}} \in G_1$. Then, the user randomly chooses $a_{i,j} \in Z_p$ and gives all the d group members' public keys $(pk_1, \cdots, pk_d) = (w_1, \cdots, w_d)$, and uses a private key sk_s computes a ring signature of this block $\sigma_{j,s} = (\frac{\beta_j}{\Psi(\prod_{i\neq s} w_i^{a_{j,i}})})^{1/x^s} \in G_1$. Therefore, the ring signature of block m_j is $\sigma_j = (\sigma_{j,1}, \cdots, \sigma_{j,d})$.

Public auditing phase. In the phase, we will describe challenge request, proof generation and proof verification.

Step 1: The TPA selects c elements as a subset J of set $[1, n]$ chooses a random value $y_j \in Z_q$, for $j \in J$. Then, the TPA sends the challenged message $\{j, y_j\}_{j\in J}$ to the CSS.

Step 2: The CSS chooses a random value $\tau_i \in Z_q$ and computes $\lambda_l = \eta_l^{\tau_l} \in G_1$, for $l \in [1, k]$. Then, the CSS computes $\mu_l = \sum_{j\in J} y_j m_{j,l} + \tau_l H_3(\lambda_l) in Z_p$, for $l \in [1, k]$. Finally, the CSS aggregates signature as $\phi_i = \prod_{j\in J}\sigma_{j,i}^{y_j}$, for $iin[1, d]$ before the CSS return an auditing proof $\{\{\lambda_1, \cdots, \lambda_k\}, \{\mu_1, \cdots, \mu_k\}, \{\phi_1, \cdots, \phi_d\}, \{id_j\}_{j\in J}\}$.

Index	Block	Virtual index	Random value
$id_j = \{v_j, r_j\}$	m_j	$v_j = j \cdot \delta$	$r_j = H_2(m_j \| v_j)$

Figure 2: Wang et al.'s index hash table (IHT) on Oruta's mechanism

Step 3: The TPA uses public aggregate key $pak = (\eta_1, \cdots, \eta_k)$ and all the group members' public keys $(pk_1, \cdots, pk_d) = (w_1, \cdots, w_d)$ to check the correctness of the auditing proof by computing

$$e(\prod_{j \in J} H_1(id_j)^{y_j} \prod_{l=1}^{k} \eta_l^{\mu_l}, g_2) \stackrel{?}{=} (\prod_{i=1}^{d} e(\phi_i, w_i)) e(\prod_{l=1}^{k} \lambda_l^{H_3(\lambda_l)}, g_2).$$

If the result is true, the TPA can make sure the user's data is correct in CSS. Otherwise, the shared data is incorrect.

Dynamic data phase. In the phase, we will only describe inserted operation because it is more difficult than update and deletion. Then, we also describe their defined form of index hash tables (IHT) (as shown in Figure 2). The IHT has four columns which are described by indexes $id_j = \{v_j, r_j\}$, blocks m_j, virtual index $v_j = j\delta$ (where $\delta \in N^*$ is a system parameter by the original user) and random value $r_j = H_2(m_j || v_j)$, for $j \in [1, n]$ is the number of block.

Step 1: The user wants to insert a new block m'_j into shared data. The user computes the new identifier of the block $id'_j = \{v'_j, r'_j\}$, where $v'_j = \lfloor (v_{j-1} + v_j)/2 \rfloor$ and $r'_j = H_2(m'_j || v'_j)$. The user computes $\beta'_j = H_1(id'_j) \prod_{l=1}^{k} \eta_l^{m_{j,l}}$, computes $\sigma'_{j,s} = (\frac{\beta'_j}{\Psi(\prod_{i \neq s} w_i^{a_{j,i}})})^{1/x^s}$ and generates a new ring signature. Finally, the user uploads $\{m'_j, id'_j, v'_j, r'_j, \sigma'_{j,s}\}$ to the CSS.

Step 2: The CSS updates index hash table (IHT) where the new block m'_j is inserted in the virtual index v'_j and the total number of blocks increase $n + 1$ in shared blocks (as shown in Figure 3).

User revocation phase. Because Wang et al.'s originally intended to solve the privacy-preserving public auditing mechanism for shared data, their scheme needs to decide in advance the number of group members and computes the number of keys. Therefore, their scheme is a static group model which does not consider the situation of a new user to be added in the group or an existing user to be revoked from the group. In order to support a dynamic group, they propose an improved solution where the ring signature on shared data need to re-compute the signer's private key and all the current users' public key when the membership of the group is changed.

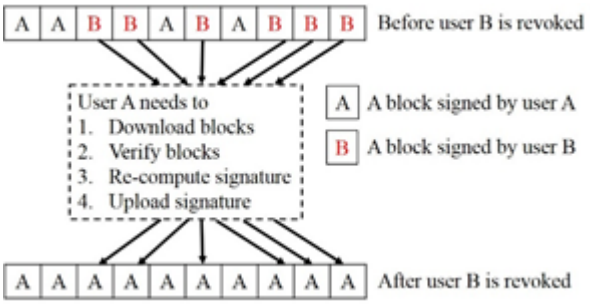


Figure 4: The traditional approach of user A and user B share data in the cloud

For instance, the number of group member is d. When a new user u_{d+1} is added into the group, the signer needs to re-compute his/her private key and others need to re-compute their public keys $(pk_1, \cdots, pk_{d+1})$ on the ring signature. When an existing user u_d is revoked from the group, the signer needs to re-compute his/her private key and others need to re-compute their public keys $(pk_1, \cdots, pk_{d-1})$ on the ring signature.

However, to satisfy the requirement of dynamic group, users need to pay a large amount of computation in the re-computation (as Setup phase). If the group has a lot of users and the user are frequently added or revoked in the group, users need to re-execute the setup phase. Therefore, how to effectively solve the re-computation of dynamic group will be a serious issue.

3.2 Wang et al.'s Scheme

Wang et al. [11] proposed a novel public auditing for shared data with efficient user revocation in the cloud (as Panda). They consider a situation that a user is revoked in the group because of the user's malicious behavior. However, the user is revoked before his/her signature blocks cannot find corresponding blocks of the signer. Therefore, these signed blocks of signature needed to be re-signing. The traditional approach explained that these blocks of the revoked user B gives existing user A to download, verify, re-sign and upload the re-signed blocks (as shown in Figure 4). However, it is not an efficient approach which will increase the exiting users' burden on communication and computation of resources.

Therefore, they utilized the concept of proxy re-signature [5] to solve public auditing for shared data with user revocation. This is not needed to spend a lot of resources on the existing users because the existing users can delegate a cloud server to re-sign blocks by generating re-signed key on the proxy re-signature model (as shown in Figure 5). Their scheme is efficient on user revocation

Index	Block	Virtual index	Random value
1	m_1	1δ	r_1
2	m_2	2δ	r_2
3	m_3	3δ	r_3
...	...	...	...
n	m_n	$n\delta$	r_n

insert

Index	Block	Virtual index	Random value
1	m_1	1δ	r_1
2	m_2'	$\lfloor 3\delta/2 \rfloor$	r_2'
3	m_2	2δ	r_2
4	m_3	3δ	r_3
...	...	...	...
$n+1$	m_n	$n\delta$	r_n

Figure 3: Insert block m_2' into shared data by using the index hash table (IHT) as identifiers on Oruta

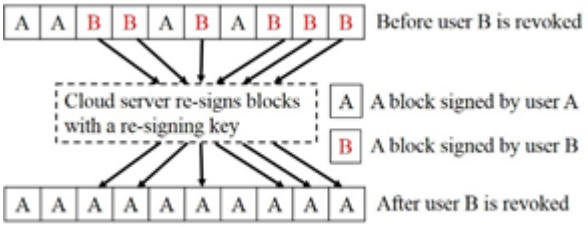


Figure 5: Wang et al.'s approach of user A and user B sharing data in the cloud

because it can reduce the computation and communication resources of existing users.

However, this solution extends an important issue for the semi-trusted cloud server to manage the re-signing key of the group. In order to avoid the single re-signing proxy on the semi-trusted cloud server, they proposed a solution which utilized a new multi-proxy model by improved Shamir Secret Sharing proxy model [44]. Because this multi-proxy model is not included in this paper, this issues more detail reference [11]. They utilized index hash tables (IHT) from Zhu et al.'s scheme [56] to support dynamic data. Finally, they extend their mechanism to support batch auditing which can allow public auditing on different users simultaneously and improve the efficiency of verification for multiple auditing tasks.

Next we will describe their scheme including setup, public auditing, dynamic data and user revocation phase. Before executing each phase, the CSS need to generate the global parameters: $(e, p, q, G_1, G_T, g_1, w, H_1, H_2, d, n)$. Their scheme is as follows:

Setup phase. In the phase, we will describe key generation and signature.

Step 1: A user u_i randomly chooses $x_i \in Z_p$ and computes the user's public key $pk_i = g^{x_i}$, and private key is $sk_i = x_i$. If the user is original, he/she will create a user list which includes the identity of all users in the group and the user list is public and signed by the original user.

Step 2: The user u_i uses private key $sk_i = x_i$ to sign the shared data block $m_j \in Z_p$ and its block identifier id_j, and w be another generator of G_1, where $j \in [1, n]$. Finally, the signature block is $\sigma_j = (H_1(id_j)w^{m_j})^{x_i} \in G_1$.

Public auditing phase. In the phase, we will describe challenge request, proof generation and proof verification.

Step 1: The TPA selects c elements as a subset L of set $[1, n]$ chooses a random value $y_l \in Z_q$, for $l \in L$ and q is a much smaller prime than p. Then, the TPA sends the challenged message $\{(l, y_l)_{l \in L}$ to the CSS.

Step 2: The CSS divides set L into d subset $(L_1, \cdots, L_d)$, where L_i is the subset of selected blocks signed by user u_i. Then the CSS computes $\mu_i = \sum_{l \in L_i} y_l m_l \in Z_p$. Finally, the CSS computes $\phi_i = \prod_{l \in L_i} \sigma_l^{y_l} \in G_1$, for $i \in [1, d]$ before the CSS returns an auditing proof $\{\{\mu_1, \cdots, \mu_d\}, \{\phi_1, \cdots, \phi_d\}, \{id_l, s_l\}_{l \in L}\}$.

Step 3: The TPA uses an auditing challenge $\{(l, y_l)\}_{l \in L}$, an auditing proof $\{\{\mu_1, \cdots, \mu_d\}, \{\phi_1, \cdots, \phi_d\}, \{id_l, s_l\}_{l \in L}\}$ and all the group members' public keys $(pk_1, \cdots, pk_d)$ to check the correctness of the auditing proof by computing the equation $e(\prod_{i=1}^{d} \phi_i, g) \stackrel{?}{=} \prod_{i=1}^{d} e(\prod_{l \in L_i} H_1(id_l)^{y_l} w^{\mu_i}, pk_i)$. If the result is true, the TPA can make sure the user's data is correct in CSS. Otherwise, the shared data is incorrect.

Dynamic data phase. In the phase, we will only describe inserted operation because it is more difficult than update and deletion. Then, we also describe their defined form of index hash tables (IHT) (as shown in Figure 6). The IHT has four columns which are described by indexes $id_j = \{v_j || r_j || s_j\}$, blocks m_j, virtual index $v_j = \text{j} \cdot \delta$ (where $\delta \in N^*$ is a system parameter by the original user), random value $r_j = H_2(m_j || v_j)$ and s_j is the signer identity of block m_j, for $j \in [1, n]$ is the number of block.

Step 1: The user s_i' wants to insert a new block m_j' into shared data. The user s_i' computes the new identifier of the block $id_j' = \{v_j' || r_j' || s_i'\}$, where

Index	Block	Virtual index	Random value	Signer id
$id_j = \{v_j \| r_j \| s_j\}$	m_j	$v_j = j \cdot \delta$	$r_j = H_2(m_j \| v_j)$	s_j

Figure 6: Wang et al.'s index hash table (IHT) on Panda's mechanism

$v'_j = \lfloor (v_{j-1} + v_j)/2 \rfloor$ and $r'_j = H_2(m'_j \| v'_j)$. The user uses his/her private key $sk_i = x_i$ to sign the block $\sigma'_j = (H_1(id_j)w^{m_j})^{x_i} \in G_1$. Finally, the user uploads $\{m'_j, id'_j, v'_j, r'_j, \sigma'_j, s_i\}$ to the CSS.

Step 2: The CSS updates index hash table (IHT) where uses $\{id'_j, m'_j, v'_j, r'_j, s'_i\}$ instead of $\{id_j, m_j, v_j, r_j, s_i\}$, stores the signature σ'_j instead of σ_j and the total number of blocks increases $n+1$ in shared blocks (as shown in Figure 7).

User revocation phase. In the phase, we will describe rekey generation and re-signature. For example, the user u_i is revoked with the signature of the user u_j instead of the signature of the user u_i.

Step 1: The CSS chooses a random value $r \in Z_p$ and sends to the user u_i.

Step 2: The user u_i computes r/x_i and sends to the user u_j.

Step 3: The user u_j computes $(rx_j)/x_i$ and sends to the CSS.

Step 4: The CSS generates a re-signing key $?rk_{i\to j} = x_j/x_i \in Z_p^*$. The CSS use the user u_i's public key, the signature σ_k, the block m_k and the block identifier id_k to compute $e(\sigma_k, g) \stackrel{?}{=} e(H_1(id_k)w^{m_k}, pk_i)$ and check the signature σ_k whether the block m_k was signed by the user u_i. If the result is true, the CSS computes $\sigma'_k = \sigma_k^{rk_{i\to j}} = (H_1(id_k)w^{m_k})^{x_i x_j/x_i} = (H_1(id_k)w^{m_k})^{x_j}$, otherwise the CSS aborts the re-signed request.

Step 5: The original user updates the user u_j's id instead of the user u_i's id on the singer identifier from a user list and signs the new user list.

3.3 Yuan and Yu's Scheme

Yuan and Yu [59] proposed a novel public integrity auditing for dynamic data sharing scheme which supports multiple users to modify shared data in the cloud storage service. They considered a problem where the cloud server aggregates authenticated tags from multiple users in public auditing phase. Because the data blocks can be modified and signed by different users' secret keys which are different each other, the cloud server has to one by one verify different users' signature in public auditing phase.

For example, a simple method can solve the problem where all users of the group share the same secret key, so it can be easily aggregated. However, when a user is revoked, he/she still can generate authenticated tags. Therefore, they utilized polynomial commitment scheme [58] to design a polynomial-based authentication tags from multiple users into one which can send the integrity proof information to the public verifier. Therefore, the public verifier only needs a constant size of integrity proof information and a constant number of computational operations. Finally, they extend their mechanism to support batch auditing which can allow public auditing on different users simultaneously and improve the efficiency of verification for multiple auditing tasks. Next we will describe their scheme including setup, public auditing, dynamic data and user revocation phase. Before executing each phase, the CSS need to generate the global parameters: $(e, p, q, G_1, G_T, g_1, u, H_2, d, n)$. Their scheme is as follows:

Setup phase. In the phase, we will describe key generation and signature.

Step 1: The master user u_0 responsibly manages the membership of the group and generates public keys (PK), users' secret keys (SK) and the system's master key (MK). The master user randomly chooses $\{x_i\}_{1\le i\le d-1} \in Z_q^*$, $\alpha \in Z_q^*$ and computes $v = g^{\alpha x_0}$, $k_0 = g^{x_0}$, $\{k_i = g^{x_i}, g^{x_0/x_i}\}_{1\le i\le d-1}$. The public keys are $PK = \{g, u, q, v, \{g^{\alpha^j}\}_{0\le j\le k+1}, k_0, \{k_i, g^{x_0/x_i}\}_{1\le i\le d-1}\}$, the master key is $MK = \{x_0, \alpha\}$ and the secret keys are $SK_i = \{x_i\}_{1\le i\le d-1}$.

Step 2: The master user u_0 computes the signature block $\sigma_i = (u^{B_i} \prod_{j=0}^{k} g^{m_{ij}\alpha^{j+2}})^{x_0} = (u^{B_i} g^{f_{\rightharpoonup \beta_i}(\alpha)})^{x_0}$ where $\rightharpoonup \beta_i = \{0, 0, \beta_{i,0}, \beta_{i,1}, \cdots, \beta_{i,k-1}\}$ and $\beta_{i,j} = m_{i,j}$. Then, $B_i = H_2(\{fname \| i \| t_i \| d\})$, $fname$ is the file name, i is the index of data block m_i, t_i is the time stamp and d is the index of user in the group. Finally, the master user sends $\{m_i, \sigma_i]\}_{1\le i\le n}$ to the CSS and sends $\{B_i\}_{1\le i\le n}$ to the TPA.

Public auditing phase. In the phase, we will describe challenge request, proof generation and proof verification.

Step 1: The TPA selects c data blocks as a subset L and chooses two random values $R \in Z_q^*$ and $\mu \in Z_q^*$. Then, the TPA computes $X = \{(g^{x_0/x_i})^R\}_{0\le i\le d-1}$ and g^R. The TPA sends the challenge message $CM = \{L, X, g^R, \mu\}$ to the CSS.

Step 2: The CSS generates $\{p_i = \mu^i \bmod q\}_{i\in L}$ and computes $y = f_{\rightharpoonup A}(\mu) \bmod q$, where $\rightharpoonup A = \{0, 0, \sum_{i\in L} p_i m_{i,0}, \cdots, \sum_{i\in L} p_i m_{i,k-1}\}$. The CSS divides the polynomial $f_{\rightharpoonup A}(x) - f_{\rightharpoonup A}(\mu)$ with $(x-\mu)$ using polynomial long division, and indicates the coefficients vector of the resulting quotient polynomial as

Index	Block	Virtual index	Random value	Signer id
1	m_1	1δ	r_1	s_1
2	m_2	2δ	r_2	s_2
3	m_3	3δ	r_3	s_3
...	...	...	...	...
n	m_n	$n\delta$	r_n	s_n

insert

Index	Block	Virtual index	Random value	Signer id
1	m_1	1δ	r_1	s_1
2	m_2'	$\lfloor 3\delta/2 \rfloor$	r_2'	s_2'
3	m_2	2δ	r_2	s_2
4	m_3	3δ	r_3	s_3
...	...	...	...	...
$n+1$	m_n	$n\delta$	r_n	s_n

Figure 7: Insert block m_2' into shared data by using the index hash table (IHT) as identifiers on Panda

$\rightharpoonup w = (w_0, w_1, \cdots, w_k)$, that is $f_{\rightharpoonup w} \equiv \frac{f_{\rightharpoonup A}(x) - f_{\rightharpoonup A}(\mu))}{(x-\mu)}$. The CSS computes $\Psi = \prod_{(} j = 0)^k (g^{\alpha^j})^{w_j} = g^{f_{\rightharpoonup w}(\alpha)}$. Then, the data blocks of a challenged subset L are modified by the user $\{u_s\}_{s \in d}$, the CSS computes $\pi_i = (\sigma_i, g^{x_0 R/x_s}) = e((u^{B_i} g^{f_{\rightharpoonup \beta_i}(\alpha)}), g)^{x_0 R}$ or modified by the master user u_0, the CSS computes $\pi_i = e(\sigma_i, g^R) = e((u^{B_i} g^{f_{\rightharpoonup \beta_i}(\alpha)}), g)^{x_0 R}$. These π_i will be aggregated as $\pi = \prod_{i \in L} \pi_i^{p_i}$. Finally, the CSS returns the proof message $\{\pi, \Psi, y\}$ to the TPA.

Step 3: The TPA computes $\eta = u^{\omega}$, where $\omega = \sum_{i \in L} B_i p_i$ and verifies the integrity of file as $e(\eta, k_0^R) e(\Psi^R, v \cdot k_0^{-\mu}) \stackrel{?}{=} \pi \cdot e(k_0^{-y}, g^R)$. If the result is true, the TPA can make sure the user's data is correct in CSS. Otherwise, the shared data is incorrect.

Dynamic data phase. In the phase, we will only describe update operation because they have not considered fully dynamic operation such as the data block insert and delete operation.

Step 1: A user u_s of group wants to modify a block m_i to m_i'. Therefore, u_s needs to use own secret key x_s to compute the re-signed block $\sigma_i' = (u^{B_i'} \prod_{j=0}^{k-1} g^{m_{i,j}' \alpha^{j+2}})^{x_s} = (u^{B_i'} g^{f_{\rightharpoonup \beta_i'}(\alpha)})^{x_s}$, where $\rightharpoonup \beta_i' = \{0, 0, \beta_{i,0}', \beta_{i,1}', \cdots, \beta_{i,k-1}'\}$ and $\beta_{i,j}' = m_{i,j}'$. Then $B_i' = H(fname||i||t_i'||d)$. Finally the user u_k uploads $\{m_i', \sigma_i'\}$ to the CSS and uploads B_i' to the TPA.

Step 2: The CSS receives the modified message and uses $\{m_i', \sigma_i'\}$ instead of $\{m_i, \sigma_i\}$.

Step 3: The TPA receives the modified message and uses B_i' instead of B_i.

User revocation phase. In the phase, we will describe rekey generation, reject generation and re-signature.

Step 1: When a user u_s of group is revoked, the master user u_0 computes rekey generation $\chi = \frac{x_0 + \rho}{x_s} \bmod q$, where $\rho \in Z_q^*$ is a random value and computes reject generation $g^{\frac{x_0}{(x_0+\rho)}}$. Finally, the master user u_0 sends χ to the CSS and sends $g^{\frac{x_0}{(x_0+\rho)}}$ to the TPA and group users.

Step 2: The CSS receives χ and updates the signature $\sigma_i' = \sigma_i^{\chi} = (u^{B_i} g^{f_{\rightharpoonup \beta_i}(\alpha)})^{x_0 + \rho}$

Step 3: The TPA and group users reject the user u_s's public parameter g^{x_0/x_s}.

3.4 Jiang et al.'s Scheme

Jiang et al. [28] proposed a public integrity auditing for shared dynamic cloud data with group user revocation. They considered a problem of collusion attack where a revoked user can collude with the malicious cloud server to change the group existed user's data. Because a group user may have malicious behavior, the data owner (or the group manager) will revoke the group of malicious user. However, if a semi-trusted cloud server cooperates with the revoked user each other, the group users' data will have a secure problem.

Therefore, how to design an efficient and reliable scheme, while achieving secure group user revocation. They propose a mechanism which not only supports the group data encryption and decryption during the data modification processing, but also achieves efficient and secure user revocation. They utilized a vector commitment scheme [17], utilized an asymmetric group key agreement (AGKA) scheme [55] and a verifier-local revocation group signature scheme [7] to construct their mechanism. A vector commitment scheme is used over the database, and AGKA scheme is used to encrypt/decrypt the share database, and a verifier-local revocation group signature scheme will avoid the collusion of cloud and revoked group users.

Next we will describe their scheme including setup, public auditing, dynamic data and user revocation phase. Before executing each phase, the CSS need to generate the public parameters: $PP = (p, q, G, G_T, H, g, \{h_i\}_{i \in n}, \{h_{i,j}\}_{i,j \in n, i \neq j})$. For all $i = (1, 2, \cdots, n)$, set $h_i = g^{z_i}$. For all i,j= $(1, 2, \cdots, n)$, set $h_{i,j} = g^{z_i z_j}$ where random values $z_i = (z_1, z_2, \cdots, z_n) \in Z_p$. Their scheme is as follows:

Setup phase. In the phase, we will describe key generation, commitment and signature.

Step 1:

1) The data owner chooses a random value $\gamma \in Z_p^*$, computes $w = g_2^{\gamma}$ and generates the

group public key $gpk = (g_1, g_2, w)$. Then the value γ is only known and protected by the data owner.

2) The data owner generates an SDH (Strong Diffie-Hellman) tuple (A_i, x_i) by choosing random values $x_i \in Z_p^*$ for each user, such that $\gamma + x_i \neq 0$ and computing $A_i = g_1^{1/(\gamma+x_i)}$. Then, the users of group generate the group secret key $gsk = (gsk[1], gsk[2], \cdots, gsk[d])$ where $gsk[i] = (A_i, x_i)$, and the revocation token RL corresponding to a user's secret key is $grt[i] = A_i$.

3) Finally, the user of group create (gpk, gsk, grt).

Step 2: The data owner computes commitment $C = (h_1^{m_1} \cdot h_2^{m_2} \cdots h_n^{m_n}) = \prod_{i=1}^{n} h_i^{m_i}$ and auxiliary information $aux = (m_1, m_2, \cdots, m_n)$.

Step 3:

1) For t^{th} time, the data owner updates data after the data blocks is signed. The data owner chooses a random value $r \in Z_p$ and obtain generators $(\hat{u}, \hat{v})$ in G_2 from H_0 as $(\hat{u}, \hat{v}) = H_0(gpk, \{C(t-1), C^t, t\}, r) \in G_2^2$ and computes $(\hat{u}, \hat{v})$ images in G_1 as $u = \Psi(\hat{u})$, $v = \Psi(\hat{v})$.

2) The data owner chooses an exponent $\alpha \in Z_p$ and compute $T_1 = u^{\alpha}$ and $T_2 = A_i v^{\alpha}$, sets $\delta = x_i \alpha \in Z_p$ and pick blinding values r_α, r_x and $r_\delta \in Z_p$, computes helper values $R_1 = u^{r_\alpha}$, $R_2 = e(T_2, g_2)^{r_x} \cdot e(v, w)^{-r_\alpha} \cdot e(v, g_2)^{-r_\delta}$ and $R_3 = T_1^{r_x} u^{-r_\delta}$, computes a challenge value c from H_2 as $c = H_2(gpk, (C(t-1), C^t, t), r, T_1, T_2, R_1, R_2, R_3) \in Z_p$, computes $s_\alpha = r_\alpha + c\delta$, $s_x = r_x + cx_i$ and $s_\delta = r_\delta + c\delta \in Z_p$. Finally, the data owner sends the signature $\sigma^t = (r, T_1, T_2, c, s_\alpha, s_x, s_\delta)$ to the CSS.

3) If σ^t is vaild, then the CSS computes $C(t) = \sigma^t C^t$ and adds the information of $\sum(t) = (C(t-1), C^t, t, \sigma^t)$ to aux.

4) Set public key parameter $PK = (PP, gpk, C(t-1), C(t))$.

Public auditing phase. In the phase, we will describe TPA to verify the validity of the signature.

Step 1: The CSS sends $(gpk, \sigma^t, C(t-1), C^t, t)$ to the TPA.

Step 2: Because the signature is $\sigma^t = (r, T_1, T_2, c, s_\alpha, s_x, s_\delta)$ and group public key is $gpk = (g_1, g_2, w)$, the TPA can computes $\hat{u}$, $\hat{v}$ and their image $u = \Psi(\hat{u}$, $v = \Psi(\hat{v}$ where $(\hat{u}, \hat{v}) = H_0(gpk, \{C(t-1), C^t, t\}, r) \in G_2^2$ and compute helper values $R_1' = u^{s_\alpha}/(T_1^c)$, $R_2' = e(T_2, g_2)^{s_x} \cdot e(v, w)^{-s_\alpha} \cdot e(v, g_2)^{-s_\delta} \cdot (e(T_2 \cdot w)/e(g_1/g_2))^c$ and $R_3' = T_1^{s_x} \cdot u^{-s_\delta}$. Then, the TPA computes a challenge value $c' \in Z_p$ using H_2 as $c' = H_2(gpk, (C(t-1), C^t, t), r, T_1, T_2, R_1', R_2', R_3')$ and checks the challenge $c \stackrel{?}{=} c'$.

Dynamic data phase. In the phase, we will describe update operation because they have not considered fully dynamic operation such as the data block insert and delete operation.

Step 1: Jiang et al. assumed that the current public key is $PK = (PP, gpk, C(t-1), C(t))$. A group user uses the public key PK to compute a proof $\Lambda_i^t = \prod_{j=1, j\neq i}^{n} h_{i,j}^{m_j^t} = (\prod_{j=1, j\neq i}^{n} h_j^{m_j^t})^{z_i}$ of the i^{th} committed message and sends $\tau = (m_i^t, \Lambda_i^t, \sum(t))$ to the CSS.

Step 2: The CSS will verify whether the user is revoked in the group.

1) The CSS receives the i^{th} committed message $\tau = (m_i^t, \Lambda_i^t, \sum(t))$. Then, the CSS sends $(gpk, \sigma^t, \sum(t))$ to the TPA.

2) Because the signature is $\sigma^t = (r, T_1, T_2, c, s_\alpha, s_x, s_\delta)$ and group public key is $gpk = (g_1, g_2, w)$, the TPA can computes $\hat{u}$, $\hat{v}$ and their image $u = \Psi(\hat{u})$, $v = \Psi(\hat{v})$ where $(\hat{u}, \hat{v}) = H_0(gpk, \{C(t-1), C^t, t\}, r) \in G_2^2$ and compute helper values $R_1' = u^{s_\alpha}/(T_1^c)$, $R_2' = e(T_2, g_2)^{s_x} \cdot e(v, w)^{-s_\alpha} \cdot e(v, g_2)^{-s_\delta} \cdot (e(T_2 \cdot w)/e(g_1/g_2))^c$ and $R_3' = T_1^{s_x} \cdot u^{-s_\delta}$. Then, the TPA computes a challenge value $c' \in Z_p$ using H_2 as $c' = H_2(gpk, (C(t-1), C^t, t), r, T_1, T_2, R_1', R_2', R_3')$ and checks the challenge $c \stackrel{?}{=} c'$. The TPA ensures that σ^t was not generated by each revoked user $A \in RL$.

3) If the result is true, the CSS need to verify the correctness of the group user. The CSS checks the equation $e(C^t/(h_i^{m_i^t}), h_i) \stackrel{?}{=} e(\Lambda_i^t, g)$. If the result is true, which means Λ_i^t is a valid proof that C^t was created to a sequence $(m_1, m_2, \cdots, m_n)$, such that $m = m_i$.

Step 3: A group user wants to update message m_i' instead of m_i, computes the updated commitment $C' = C \cdot h_i^{m'-m}$ and the updated information $U = (m, m', i)$.

Step 4: The TPA can computes an update proof $\Lambda_j = \prod_{i=1, i\neq j}^{n} h_{i,j}^{m_i} = (\prod_{i=1, i\neq j}^{n} h_i^{m_i})^{z_j}$ and j is the position of message. The proof Λ_j is valid with respect to C' which contains m' as the new message at position j. The TPA uses the update information $U = (m, m', i)$ to generate the proof of update. If the position of message $i \neq j$, compute the updated commitment $C' = C \cdot h_i^{m'-m}$ and the updated proof is

$\Lambda'_j = \Lambda_j \cdot (h_i^{m'-m})^{z_j} = \Lambda_j \cdot h_{j,i}^{m'-m}$. If the position of message $i = j$, compute the updated commitment $C' = C \cdot h_i^{m'-m}$ while not changing the proof Λ_i. Finally, the TPA verifies the commitment C' and corresponding proof Λ_i is also valid over message m'_i.

User revocation phase. In the phase, we will describe TPA to verify the validity of the signature and check the revocation list.

Step 1: The CSS sends $(gpk, \sigma^t, C(t-1), C^t, t)$ to the TPA.

Step 2: Because the signature is $\sigma^t = (r, T_1, T_2, c, s_\alpha, s_x, s_\delta)$ and group public key is $gpk = (g_1, g_2, w)$, the TPA can computes $\hat{u}$, $\hat{v}$ and their image $u = \Psi(\hat{u})$, $v = \Psi(\hat{v})$ where $(\hat{u}, \hat{v}) = H_0(gpk, \{C(t-1), C^t, t\}, r) \in G_2^2$ and compute helper values $R'_1 = u^{s_\alpha}/T_1^c)$, $R'_2 = e(T_2, g_2)^{s_x} \cdot e(v, w)^{-s_\alpha} \cdot e(v, g_2)^{-s_\delta} \cdot (e(T_2 \cdot w)/e(g_1/g_2))^c$ and $R'_3 = T_1^{s_x} \cdot u^{-s_\delta}$. Then, the TPA computes a challenge value $c' \in Z_p$ using H_2 as $c' = H_2(gpk, (C(t-1), C^t, t), r, T_1, T_2, R'_1, R'_2, R'_3)$ and checks the challenge $c \stackrel{?}{=} c'$.

Step 3: The TPA ensures that σ^t was not generated by each revoked user $A \in RL$. Therefoere, the TPA checks whether A is encoded in (T_1, T_2) by checking if $e(T_2/A, \hat{u}) \stackrel{?}{=} e(T_1, \hat{v})$. If no element of RL is written in (T_1, T_2), the signer of σ^t has not been revoked.

4 Analysis

In the section, we will analyze these schemes [8, 11, 28, 59] which contain functional requirement, security and performance. And we also use the tables to present a corresponding requirement in each scheme.

4.1 Functional Evaluation

In Table 2, we will analyze seven functional requirements: blockless verification, stateless verification, bath auditing, dynamic data, anonymity, privacy presenting and user revocation in the representative approaches. Yuan, Yu's scheme [28] and Jiang et al.'s scheme [59] decided which TPA needed to maintain the data situation of the user in the dynamic data phase. Because Jiang et al.'s scheme has not consider blockless verification, their scheme extends to support batch auditing which is difficult in the public auditing phase. In the dynamic data phase, Yuan, Yu's scheme and Jiang et al.'s scheme only considered data update, so their scheme can support data insert operation. Because Wang et al.' scheme [8] utilized ring signature, their scheme can influence the TPA to get the user identity. These scheme can satisfy privacy presenting, when the TPA can get the data of the group in the public auditing phase. Because Wang et al. [8] first proposed the scheme which can support shared data on public auditing, they have not considered to user revocation in the group. However, they make up the problem, but the improved scheme needs to re-generate the key of each user. These approach can satisfy the requirement of user revocation.

4.2 Security Evaluation

In Table 3, we will analyze the five attack models: inside attack, forge attack, replace attack, impersonation attack and collusion attack in the representative approaches. In the inside attack, because these schemes are used by the user to upload plaintext in the cloud storage server, the cloud storage server can know the user's data. Therefore, the cloud storage server can use unauthorized data. In the forge attack, these scheme can resist the cloud server to forge the data tag of data block because the data owner upload the signed the data tag of data block. Therefore, the cloud server is hard to forge a legitimate data tag. In the replace attack, Wang et al. [8] and Wang et al. [11] do not consider the cloud server does not update the user's data, so they cannot support the replace attack. Yuan et al.'s scheme uses the time stamp to record updated time, so it can check the time stamp of the data. Jiang et al.'s scheme considered which TPA verifies the update proof, so it can check whether the cloud server update the user's data. In the impersonation attack, because they focused on data integrity, their scheme do not consider authentication. Jiang et al.'s scheme was only a simple authentication where the TPA verified the user on the revocation list. However, when the user does not exist on the revocation list, the TPA cannot verify the impersonation attack. In the collusion attack, because Wang et al.'s scheme [8] has not supported user revocation, the revoked user and the semi-trusted server can collude to attack the shared data. Because Wang et al. [11], Yuan et al. and Jiang et al. have support user revocation, they can avoid a collusion attack.

4.3 Performance Evaluation

We will analyze four phases: setup phase, public auditing phase, dynamic data phase and user revocation phase in the four entities which include data owner, user (the group user), cloud storage server (CSS) and third party auditor (TPA). Before we analyze the performance evaluation, first we introduce the notations in Table 4.

In Table 5, we analyze four schemes how to execute a setup phase. Wang et al.'s scheme [11] explained that the data owner needs lower computing resource in the setup phase. The group user does not need to generate a secret key because the data owner supports key generation as shown in the Jiang et al.'s scheme.

In Table 6, we analyze four scheme how to execute a public auditing phase. Because in a public auditing phase the data owner and the group user have not to execute,

Table 2: Comparison of functional requirements

	Wang et al. [8]	Wang et al. [11]	Yuan, Yu [59]	Jiang et al. [28]
Blockless verification	Yes	Yes	Yes	No
Stateless verification	Yes	Yes	No	No
Batch auditing	Yes	Yes	Yes	No
Dynamic data	Yes	Yes	Partial	Partial
Anonymity	Yes	No	No	No
Privacy Presenting	Yes	Yes	Yes	Yes
User Revocation	No	Yes	Yes	Yes

Table 3: Comparison of security attack

	Wang et al. [8]	Wang et al. [11]	Yuan, Yu [59]	Jiang et al. [28]
Inside attack	No	No	No	No
Forge attack	Yes	Yes	Yes	Yes
Replace attack	No	No	Yes	Yes
Impersonation attack	No	No	No	No
Collusion attack	No	Yes	Yes	Yes

Table 4: Notations

Notation	Significance
T_E/T_D	The computing time of asymmetric encryptions
T_{Ge}	The computing time of exponentiation in group operation
T_{BLS}	The computing time of BLS signature
T_B	The computing time of bilinear pairing
T_M	The computing time of multiplication
T_A	The computing time of addition
T_{GM}	The computing time of multiplication in group operation
T_h	The computing time of hash function
n	The number of block in a file
i	The number of verified block
d	The total number of users in the group
k	A block element of the shared data block m_i

Table 5: Comparison of computation in setup phase

	Wang et al. [8]	Wang et al. [11]	Yuan, Yu [59]	Jiang et al. [28]
Data owner	$n(T_{Ge}^{d-1}+T_{Ge}^{k}+T_{BLS}$ $+2T_{GM}+T_h)+T_{Ge}$ $+2T_{GM}+T_h)+T_{Ge}$	$(n+1)T_{Ge}$ $+n(T_{BLS}+T_{GM}+T_h)$ $+n(T_{BLS}+T_{GM}+T_h)$	$n(T_{Ge}^{k}+T_{Ge}+T_{BLS}$ $+T_{GM}+T_h)$ $+2T_{Ge}+T_M$	$(d+6)T_{Ge}+T_{Ge}^{n}$ $+(d+3)T_A+4T_M$ $+4T_{GM}+2T_h$
User	T_{Ge}	T_{Ge}	$2T_{Ge}$	-
CSS	-	-	-	T_{GM}
TPA	-	-	-	-

they do not consume any computing resources. In the Jiang et al.'s scheme, the CSS does not consume computing resource because the CSS will response the entire data to the TPA. Then, the TPA needs to verify the entire data, so the TPA requires more computing resources. The CSS is an affected factor including a block element of the shared data block, the total number of users in the group and the number of verified block. Wang et al. [8] considered two factors include the number of verified block and a block element of the shared data block, Wang et al. [11] considered one factor which is the total number of users in the group and Yuan et al. considered all factors. However, Yuan et al.'s scheme is more flexible in different situations.

In Table 7, we analyze four schemes how to execute a dynamic data phase. Jiang et al.'s scheme obviously requires more computing resources because their scheme has three entities needed to execute. These schemes [8, 11, 59] only consider that the group user transfers the updated data to the CSS, and the CSS directly update the data. Therefore, when the semi-trusted CSS has not updated the data, the group user cannot get related message. Jiang et al.'s scheme considered that the CSS can verify whether the user is in this group and the TPA can verify whether the stored data of the CSS has been updated. Therefore, Jiang et al.'s scheme spent a lot of computing resources in the verification.

In Table 8, we analyze four schemes how to execute a user revocation phase. Wang et al.'s scheme [11] and Yuan et al.'s scheme are similar because they scheme which data owner delegates the CSS to re-sign the signed data block of the revoked user. However, Yuan et al.'s scheme decided which data owner needs more computing resources. Jiang et al.'s scheme needed to verify the signature and check whether the revoked user has been revoked in the revocation list RL.

In Table 9, we analyze four schemes how to distribute storage. The TPA cannot require storage space in Wang et al.'s scheme [8] and Wang et al.'s scheme [11]. Yuan et al.'s scheme decided which TPA requires to store file information, and Jiang et al.'s scheme decided which TPA requires to store revocation list. Because Wang et al.'s scheme [8] considered anonymity, the CSS could not store the signer's information. However, Wang et al.'s scheme [11] considered user revocation, so the CSS requires to update the signed data block of the revoked user. Because Yuan et al.'s scheme only consider modification operation, the CSS only store m and σ. However, Jiang et al.'s scheme is $aux = (m_1, m_2, \cdots, m_n)$, $(C(t-1), C^t, t, \sigma^t)$, so their scheme requires more storage space.

5 Conclusion and Future Work

In the cloud storage service, the data integrity of remote verification is already a critical issue. The concept of public audit can solve to remotely verify data integrity and extend to verify the shared data. We organize public auditing requirements containing function, security and performance from the many relevant literatures. We also list the four representative approaches and analyze these approaches. These comparison tables can clearly understand the advantages and disadvantages of each approach. Finally, in this paper, we provide the future development of public audit and shared data.

For future developments, we will focus on the following areas of particular interest. Efficiency: because users demand high performance, the scheme satisfies an effective scheme to reduce the computing resources which include public audit, dynamic data and user revocation of the operation. Therefore, how to design an efficient public audits with shared data that is an important issue.

Security: in addition to data integrity, the public auditing need to consider the data confidentiality. Because the user will store data in the cloud storage service, the cloud service provider can access the user's data. Therefore, the user need to encrypt data before the user uploads data to the cloud storage service. How to design a public audit with shared data in the situation of encrypted data which will be able to satisfy integrity and confidentiality simultaneously.

Data recovery: the user upload data to the cloud storage service before the user deletes data which will reduce the user's storage space. When the cloud server is lost the user data, third party auditor verifies the user's data is in complete. However, the user do not back up data on the local storage space. Therefore, the user need to save his/her data. How to design a scheme which can support public audit and data recovery.

References

[1] M. Armbrust, et al., "A view of cloud computing", *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 598–609, Virginia, USA, 2007.

[3] G. Ateniese, et al., "Remote data checking using provable data possession", *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–34, 2011.

[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks*, pp. 9:1–9:10, Istanbul, Turkey, 2008.

[5] M. Blaze, G. Bleumer, M. Strauss, "Divertible protocols and atomic proxy cryptography", in *Advances in Cryptology (EUROCRYPT'98)*, LNCS 1403, pp. 127–144, Springer, 2006.

[6] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proceedings of the 7th*

Table 6: Comparison of computation in Public auditing phase

	Wang et al. [8]	Wang et al. [11]	Yuan, Yu [59]	Jiang et al. [28]
CSS	$1T_{Ge}$ $+k((i+1)T_M+T_A+T_h)$	$(T^d_{Ge}+dT_M$ $(T^d_{Ge}+dT_M$	$iT_{Ge}+2T^k_{Ge}+T^i_{Ge}$ $+k(iT_M)+T_B$	-
TPA	T_B	T_B	$(d+1)T_{Ge}+iT_M+T_B$	$4T_{Ge}+2T_h+5T_{GM}$

Table 7: Comparison of computation in Dynamic data phase

	Wang et al. [8]	Wang et al. [11]	Yuan, Yu [59]	Jiang et al. [28]
User	$2T_h+T_{GM}+2T_{GM}$ $+T^{d-1}_{Ge}+T_{BLS}$	$2T_h+T_{GM}$ $+T_{Ge}+T_{BLS}$	T_h+T_{GM} $+2T^k_{Ge}+T_{BLS}$	$T^{n-1}_{Ge}+T_{Ge}$ $+T_{GM}$
CSS	-	-	-	T_B
TPA	-	-	-	$T^{n-1}_{Ge}+6T_{Ge}+7T_{GM}+2T_h$

Table 8: Comparison of computation in user revocation phase

	Wang et al. [8]	Wang et al. [11]	Yuan, Yu [59]	Jiang et al. [28]
Data owner	No support	T_M	$3T_M+T_{Ge}$	-
User	No support	T_M	-	-
CSS	No support	$T_M+T_B+T_{BLS}$	T_{BLS}	-
TPA	No support	-	T_{GM}	$4T_{Ge}+2T_h+5T_{GM}+T_B$

Table 9: Comparison of storage

	Wang et al. [8]	Wang et al. [11]	Yuan, Yu [59]	Jiang et al. [28]
CSS	$IHT\{id,m,v,r\}$, σ	$IHT\{id,m,v,r,s\}$, σ	m, σ	aux, σ^t
TPA	No	No	B	RL

International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 514–532, Gold Coast, Australia, 2001.

[7] D. Boneh, H. Shacham, "Group signatures with verifier-local revocation", in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pp. 168–177, Washington DC, USA, Oct. 25-29, 2004.

[8] W. Boyang, L. Baochun, "Oruta: Privacy-preserving public auditing for shared data in the cloud", *IEEE Transactions on Cloud Computing*, vol. 2, no. 1, pp. 43–56, 2014.

[9] W. Boyang, L. Baochun, and L. Baochun, "Oruta: Privacy-preserving public auditing for shared data in the cloud", in *Proceedings of the 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS'13)*, pp. 93–98, Xian, China, Sept. 9-11, 2012.

[10] W. Boyang, L. Baochun, and L. Baochun, "Public auditing for shared data with efficient user revocation in the cloud", in *Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM'13)*, pp. 2904–2912, Turin, Italy, Apr. 14-19, 2013.

[11] W. Boyang, L. Baochun, and L. Baochun, "Panda: Public auditing for shared data with efficient user revocation in the cloud", *IEEE Transactions on Services Computing*, vol. 8, no. 1, pp. 92-106, 2015.

[12] W. Boyang, L. Baochun, L. Baochun, and L. Fenghua, "Certificateless public auditing for data integrity in the cloud", in *Proceedings of the First IEEE Conference on Communications and Network Security (CNS'13)*, pp. 136–144, Maryland, USA, Oct. 14-16, 2013.

[13] W. Boyang, L. Baochun, and L. Ming, "Privacy-preserving public auditing for shared cloud data supporting group dynamics", in *Proceedings of IEEE International Conference on Communications (ICC'13)*, pp. 1946–1950, Budapest, Hungary, June 9-13, 2013.

[14] W. Boyang, L. Baochun, L. Xuefeng, L. Fenghua, L. Xiaoqing, "Efficient public verification on the integrity of multi-owner data in the cloud", *Journal of Communications and Networks*, vol. 16, no. 6, pp. 592–599, 2014.

[15] W. Boyang, S. S. M. Chow, L. Ming, L. Baochun, "Storing shared data on the cloud via security-mediator", in *Proceedings of the 33rd IEEE International Conference on Distributed Computing Systems (ICDCS'13)*, pp. 124–133, Pennsylvania, USA, July 8-11, 2013.

[16] D. Cash, A. Küpcü, D. Wichs, "Dynamic proofs of retrievability via oblivious RAM", in *Advances in Cryptology (EUROCRYPT'13)*, LNCS 7881, pp. 279–295, Springer, 2013.

[17] D. Catalano, D. Fiore, "Vector commitments and their applications", in *Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC'13)*, pp. 55–72, Nara, Japan, Feb. 26 - Mar. 1, 2013.

[18] L. Chang, et al., "Public auditing for big data storage in cloud computing – A survey", in *Proceedings of the 16th IEEE International Conference on Computational Science and Engineering (CSE'13)*, pp. 1128–1135, Sydney, Australia, Dec. 3-5, 2013.

[19] B. Chen, R. Curtmola, "Robust dynamic provable data possession", in *Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'12)*, pp. 515–525, Macau, China, 2012.

[20] L. Chen, "Using algebraic signatures to check data possession in cloud storage", *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1709–1715, 2013.

[21] W. Cong, W. Qian, R. Kui, C. Ning, L. Wenjing, "Toward secure and dependable storage services in cloud computing", *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.

[22] W. Cong, W. Qian, R. Kui, L. Wenjing, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", in *Proceedings of the 29th IEEE Conference on Information Communications (INFOCOM'10)*, pp. 1–9, San Diego, California, USA, Mar. 14-19, 2010.

[23] C. Erway, A. K, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pp. 213–222, Illinois, USA, 2009.

[24] S. Halevi, D. Harnik, B. Pinkas, A. Shulman-Peleg, "Proofs of ownership in remote storage systems", in *Proceedings of the Proceedings of the 18th ACM conference on Computer and Communications Security*, pp. 491–500, Chicago, Illinois, USA, 2011.

[25] C. Hanser, D. Slamanig, "Efficient simultaneous privately and publicly verifiable robust provable data possession from elliptic curves", *IACR Cryptology ePrint Archive*, pp. 392–406, 2013.

[26] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, "The rise of big data on cloud computing: Review and open research issues," *Information Systems*, vol. 47, no. 6, pp. 98–115, 2015.

[27] W. Huaqun, "Proxy provable data possession in public clouds", *IEEE Transactions on Services Computing*, vol. 6, no. 4, pp. 551–559, 2013.

[28] T. Jiang, X. Chen, J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation", *IEEE Transactions on Computers*, to be published.

[29] Y. Jiawei, Y. Shucheng, "Secure and constant cost public cloud storage auditing with deduplication", in *Proceedings of the First IEEE Conference on Communications and Network Security (CNS'13)*, pp. 145–153, Maryland, USA, Oct. 14-16, 2013.

[30] Y. Jiawei, Y. Shucheng, "Efficient public integrity checking for cloud data sharing with multi-user mod-

ification", in *Proceedings of the 33rd IEEE International Conference on Computer Communications (INFOCOM'14)*, pp. 2121–2129, Toronto, Canada, Apr. 27 - May 2, 2014.

[31] L. Jin, T. Xiao, C. Xiaofeng, D. S. Wong, "An Efficient Proof of Retrievability with Public Auditing in Cloud Computing", in *5th International Conference on Intelligent Networking and Collaborative Systems (INCoS'13)*, pp. 93–98, 2013.

[32] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 584–597, Virginia, USA, 2007.

[33] Y. Kan, J. Xiaohua, "An efficient and secure dynamic auditing protocol for data storage in cloud computing", *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 9, pp. 1717–1726, 2013.

[34] R. Kui, W. Cong, W. Qian, "Security challenges for the public cloud", *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[35] J. Li, X. Tan, X. Chen, D. Wong, and F. Xhafa, "OPoR: Enabling proof of retrievability in cloud computing with resource-constrained devices," accepted and to be publish in *IEEE Transactions on Cloud Computing*, Oct. 2014.

[36] C. Liu, J. L. Chen, T. Yang, X. Zhang, C. Yang, R. Ranjan, and K. Ramamohanarao, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2234–2244, 2014.

[37] C. Liu, R. Ranjan, C. Yang, L. Wang, and J. Chen, "MuR-DPA: Top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud", *IEEE Transactions on Computers*, to be published.

[38] C. C. Liu, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and iot: A big picture," *Future Generation Computer Systems*, vol. 49, no. 6, pp. 58–67, 2015.

[39] S. Meena, E. Daniel, N. A. Vasanthi, "Survey on various data integrity attacks in cloud environment and the solutions", in *Proceedings of the 2013 IEEE International Conference on Circuits, Power and Computing Technologies (ICCPCT'13)*, pp. 1076–1081, Nagercoil, India, Mar. 20-21, 2013.

[40] P. M. Mell and T. Grance, *The NIST Definition of Cloud Computing*, Technical Report: SP 800-145, National Institute of Standards and Technology, 2011.

[41] R. C. Merkle, "Protocols for public key cryptosystems," in *IEEE Symposium on Security and Privacy*, pp. 122–134, California, USA, 1980.

[42] R. L. Rivest, A. Shamir, Y. Tauman, "How to leak a secret", in *Proceedings of the Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 612–613, Gold Coast, Australia, Dec. 9-13, 2001.

[43] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'08)*, pp 90–107, Melbourne, Australia, 2008.

[44] A. Shamir, "How to share a secret", *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[45] Y. J. Shin, J. Hur, K. Kim, "Security weakness in the proof of storage with deduplication", *IACR Cryptology ePrint Archive*, pp. 554, 2012.

[46] M. Sookhak, et al., "Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues", *ACM Computing Surverys*, vol. 47, no. 4, pp. 1–34, 2015.

[47] M. Sookhak, H. Talebian, K. Ahmed, A. Gani, M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues", *Journal of Network and Computer Applications*, vol. 43, pp. 121–141, 2014.

[48] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[49] B. Wang, B. Li, and H. Li, "Knox: Privacy-preserving auditing for shared data with large groups in the cloud", in *Proceedings of the Proceedings of the 10th International Conference on Applied Cryptography and Network Security (ACNS'12)*, pp. 507–525, Singapore, June 26-29, 2012.

[50] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.

[51] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in *Proceedings of the 17th International Workshop on Quality of Service (IWQoS'09)*, pp. 1–9, South Carolina, USA, 2009.

[52] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing", in *Proceedings of the Proceedings of the 14th European Conference on Research in Computer Security*, pp. 355–370, Saint-Malo, France, Sept. 21-25, 2009.

[53] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, 2011.

[54] L. Wei, et al., "Security and privacy for storage and computation in cloud computing", *Information Sciences*, vol. 258, pp. 371–386, 2014.

[55] Q. Wu, Y. Mu, W. Susilo, B. Qin, J. Domingo-Ferrer, "Asymmetric group key agreement", in *Advances in Cryptology (EUROCRYPT'09)*, LNCS 5479, pp. 153–170, Springer, 2009.

[56] Z. Yan, et al., "Dynamic audit services for outsourced storages in clouds", *IEEE Transactions on Services Computing*, vol. 6, no. 2, pp. 227–238, 2013.

[57] Y. Yu, J. Ni, M. H. Au, Y. Mu, B. Wang, and H. Li, "On the security of a public auditing mechanism for shared cloud data service", *IEEE Transactions on Services Computing*, to be published.

[58] J. Yuan, and S. Yu, "Proofs of retrievability with public verifiability and constant communication cost in cloud", in *Proceedings of the Proceedings of the ACM International Workshop on Security in Cloud Computing (ASIACCS-SCC'13)*, pp. 19–26, Hangzhou, China, 2013.

[59] J. Yuan, and S. Yu, "Public integrity auditing for dynamic data sharing with multi-user modification", *IEEE Transactions on Information Forensics and Security*, to be published.

[60] Q. Zheng, S. Xu, "Secure and efficient proof of storage with deduplication", in *Proceedings of the Proceedings of the second ACM Conference on Data and Application Security and Privacy*, pp. 1–12, San Antonio, Texas, USA, Feb. 07-09, 2012.

[61] Q. Zheng, S. Xu, "Fair and dynamic proofs of retrievability", in *Proceedings of the Proceedings of the First ACM Conference on Data and Application Security and Privacy*, pp. 237–248, San Antonio, USA, 2011.

[62] Y. Zhu, H. Hu, G. J. Ahn, S. S. Yau, "Efficient audit service outsourcing for data integrity in clouds", *Journal of Systems and Software*, vol. 85, no. 5, pp. 1083–1095, 2012.

[63] D. Zissis, D. Lekkas, "Addressing cloud computing security issues", *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

Chih-Wei Liu received his M.S. in Soil And Water Conservation from National Chung Hsiung University, Taichung, Taiwan, ROC, in 2008. He is currently pursuing the Ph.D. degree from Computer Science and Information Engineering Department of Asia University, Taichung, Taiwan. His research interests include information security, cloud computing, and information law.

Wei-Fu Hsien received his B. S. in Department of Information Management from National Kaohsiung Marine University, Kaohsiung, Taiwan, ROC, in 2013. He is currently pursuing the M.S. degree with the Department of Management Information Systems from National Chung Hsing University. His research interests include security and privacy of cloud computing, and applied cryptography.

Chou-Chen Yang received his B.S. in Industrial Education from the National Kaohsiung Normal University, in 1980, and his M.S. in Electronic Technology from the Pittsburg State University, in 1986, and his Ph.D. in Computer Science from the University of North Texas, in 1994. From 1994 to 2004, Dr. Yang was an associate professor in the Department of Computer Science and Information Engineering, Chaoyang University of Tech- nology. Currently, he is a professor in the Department of Management Information Systems, National Chung Hshing University. His research interests include network security, mobile computing, and distributed system.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

An Analytical Black Hole Attack Model Using a Stochastic Topology Approximation Technique for Reactive Ad-Hoc Routing Protocols

Christopher W. Badenhop, Benjamin W. Ramsey, and Barry E. Mullins
(Corresponding author: Benjamin W. Ramsey)

Department of Electrical and Computer Engineering, Air Force Institute of Technology
2950 Hobson Way, Wright-Patterson AFB, OH 45433, USA
(Email: benjamin.ramsey@afit.edu)
(Received June 10, 2015; revised and accepted Sept. 6, 2015)

Abstract

This paper presents an analytical Black Hole attack model to predict the mean packet loss of ad-hoc networks using reactive routing protocols without apriori knowledge of the actual topology configuration. Topology information is summarized as a set of prototypical hop-distance profiles that describe likely hop distance perspectives within the topology and are generated using K-means clustering. Experiments are conducted to validate the theoretical attack condition, the hop-distance profiles, and prediction performance. Results show the model prediction falls within the 95% confidence intervals of packet loss through simulation of a variety of fixed and ad-hoc topologies.

Keywords: Ad-hoc networks, black hole attack, network availability modelling

1 Introduction

The computer network is a pervasive and critical asset in our society. It permits the sharing of distributed resources to achieve complex social, economic, and scientific objectives irrespective of locality. However, it is also a vulnerability to its hosts because any disruption, degradation, or denial of access to this network adversely affects the objectives of the distributed organization. Moreover, computer networks are subject to disruptive, degrading, and denial attacks at every layer of the network stack [2, 25, 38]. Ad-hoc networks are especially vulnerable to disruption because they rely on coordination *in-situ* rather than apportioning resources *apriori* as done in infrastructure-based networks. Ad-hoc networks provide data routing services to loosely coordinating groups or to address the need for multi-hop communication in environments without infrastructure. With respect to security analysis of systems, there has been significant research on the development of confidentiality and integrity analytical models. Classic models such as the Bell-LaPadula Confidentiality Model [7], Lipner's Integrity Model [24], and the Chinese Wall Model [10] have existed for decades. The body of this research has provided a foundational approach to proving security properties in systems under study.

Since networks provide a delivery service, the *availability* security property is of great importance to network designers. Unfortunately, the historical depth of research on analytical availability models is lagging behind that of *confidentiality* and *integrity* research. While there is some availability modeling research in [1, 14, 16, 23, 31, 39], the *de facto* approach to assessing the effects of availability attacks on networks is measured through simulation. Examples of this approach include work performed in [11, 19, 26, 32]. While the simulation approach has a clear utility, there are several drawbacks. First, the approach is exhaustive and scales poorly. High dimensional experiments may take orders of weeks or months to provide conclusions. Second, the simulation models require initial validation when used and revalidation upon any modification to the simulation model-base [4]. Third, complex interactions, such as causality, between simulation objects are abstracted and must be statistically estimated through repetition. Effective experiment design can certainly ascertain causality between simulated factors and response variables to generate regression models; however, their mathematical relationship remains hidden.

At the cost of fidelity, these challenges may be avoided by the use of analytical models for security analysis. The contribution of this research is the development of an analytical model for reactive ad-hoc protocols that measures availability degradation of networks subjected to Black Hole attacks. A Black Hole attack is a well-known denial of service attack for ad-hoc networks that deceptively attracts data to flow through nodes under control of an attacker. As packets arrive, they are silently dropped. Such a model can be used in conjunction with other availability models to influence design decisions of distributed system or ad-hoc network developers when limited imple-

mentation details exist. Moreover, the model explains the relationship between contributing factors for Black Hole attacks that are hidden when using simulated experimentation. While there has been extensive work in detecting, avoiding, and isolating Black Hole attacks, the relationship between the topology parameters and the attack effectiveness has not been extensively studied. Limited attack effectiveness has been measured using simulation in [17, 28, 34]; however, the scope of each study is limited to only a few topology types (e.g., protocol, number of Black Holes, number of nodes, and operating area). The results of these observational studies make it difficult to extrapolate performance for other types of ad-hoc topologies.

In [5], a theorem is developed for reactive ad-hoc routing protocols with hop-distance as a primary route metric selection criteria. During route discovery, if a Black Hole node is closer in hop distance than the destination to the source, then the Black Hole node may present a fake route to the downstream nodes with a metric that exceeds the metric of any legitimately proposed route. An analytical Black Hole attack model is developed that calculates the probability of this theorem being true for arbitrary source-destination pairs of a given ad-hoc network. Since the attack probability applies to any route in the network, it is a holistic measure of the susceptibility of a given network to Black Hole attack and may be useful for providing upper or lower bounds of network throughput degradation while under attack.

The analytical model in [5] is a function of the number of nodes in the network, the number of nodes conducting Black Hole attacks in the network, and the average node degree of the network. It assumes that the Black Hole nodes are uniform-randomly dispersed within the operating area of the ad-hoc network, and that all nodes within the network have equal probability of being a source or destination of new route. To avoid requiring absolute knowledge of the topology of the ad-hoc network under study, a topology approximation technique is used, seeded by one or more statistically estimated parameters of the topology under study. These parameters include the mean node degree of the network and the number of nodes. They are simpler to estimate prior to the instantiation of an ad-hoc topology than attempting to estimate the graph of the topology instance. The parameters are used to generate a n-ary 2-cube topology, which has average degree n and 2^n nodes [30]. The model uses this topology to calculate the probability of attack for all source and destination pairs of the ad-hoc network under study.

The motivation for the utilization of n-ary 2-cubes to approximate ad-hoc topologies is based on the intuition that high-dimensional topologies of an arbitrary orientation, when projected onto a 2-dimensional plane, *appear* as an ad-hoc topology. Moreover, the projection of a single n-ary 2-cube onto a plane may represent a set of flat topologies by rotating the n-ary 2-cube in the higher dimensional space. Unfortunately, the similarities are deceiving, and several issues make it challenging to use this as an approximation method. First, ad-hoc topologies have nodes with varying node degree, whereas the node degree for all nodes in a n-ary 2-cube have a constant degree. This means that as the variance of the node degree of an ad-hoc network increases, the approximation will not be able to represent portions of the network with extreme connectivity. Second, given an ad-hoc topology with a known node degree and number of nodes, it is likely that, due to the ridged definition of the n-ary 2-cube, a corresponding n-ary 2-cube approximation having the same values for both parameters does not exist. Any application using this approximation, including the Black Hole attack model, must perform a trade-off study to determine which n-ary 2-cube approximation minimizes calculation error, degrading the utility of the approximation. Third, ad-hoc topologies may become partitioned over their lifetime due to mobility or node failure. A n-ary 2-cube is unable to model network partitions because the node degree of the approximation is homogeneous within the topology. Fourth, two nodes may be within transmission distance within the projection of an arbitrarily rotated n-ary 2-cube onto a 2-dimensional plane; however, their Euclidean distance in the high dimensional space may beyond transmission range. This means that the projection will contain edges that do not exist in the n-ary 2-cube.

The work presented in this paper extends the work accomplished in [5] while addressing the disadvantages of using an n-ary 2-cube as an approximation technique. First, a simple simulated experiment is conducted to enhance the credibility of the theorems derived in [5]. Second, the Black Hole attack model is generalized for arbitrary network topologies. In this generalization, the topology state is known and a simulated experiment is conducted to show that the analytical model is able to predict the network level effects of Black Hole attack. Third, the generalized model is extended to incorporate unique aspects of ad-hoc networks; namely, that nodes may become partitioned and that the true topology state is difficult to realize prior to its instantiation. The n-ary 2-cube topology approximation is replaced by a set of prototype *neighborhoods*, derived statistically via k-means clustering. A third simulated experiment is conducted to validate the extended analytical Black Hole attack model. To illustrate the improvement of the analytical model derived in this work, it is compared with performance predictions using the original model defined in [5].

1.1 Ad-Hoc Network Routing Background

An ad-hoc routing service is comprised of four core components: 1) determining topology state, 2) calculating routes, 3) selecting a route, and 4) forwarding packets according to the selected route [35]. The predominant challenge for the routing service is to efficiently realize and maintain the state of network topology while contending

with confounding dynamics in the physical, RF, and logical domains. Examples of dynamic events include node power failures, RF interference, and topology discovery on initial deployment. Global awareness of these events is achieved through protocol coordination, through which participants discover and exchange local topology state information with peers to identify potential routes. The fittest route is selected from this state update per destination or as needed.

One major aspect of routing protocols is when routes are calculated. A *proactive* protocol will enforce a periodic synchronization between all nodes to achieve topology state coherency. A node with fresh topology information can immediately calculate the next hop in the forwarding path or, depending on the protocol, determine the complete route. To minimize coordination overhead, *reactive* routing protocols only coordinate when necessary. The trade-off between reactive and proactive strategies is route setup time and effective bandwidth. Proactive protocols have more deterministic route setup times at a cost of utilizing higher bandwidth [29]. Reactive protocols utilize less bandwidth for control packets, but have higher variance in the route setup period [22].

This research generally applies to reactive ad-hoc protocols; however, the specific work focuses exclusively on Ad-Hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR). Both of these have matured to be de facto reactive protocols and constitute a base design class from which other reactive protocols have been derived. In essence, to attempt a unified analysis, this work applies to the common aspects of all reactive protocols (i.e., the route discovery process) and, more specifically, to AODV and DSR.

1.2 Ad-Hoc On-demand Distance Vector Routing

AODV routing is a reactive routing, forward updating, hop-by-hop, flat, and single-path routing protocol [27]. The protocol is broken into three services: 1) Route Discovery, 2) Route Repair, and 3) Packet Forwarding. The Route Discovery process occurs when a source node desires to route to a destination. The source node sends a route request (RREQ) packet that is flooded throughout the network via broadcast. As the RREQ is propagating the network, intermediate nodes append their ID to the RREQ and store a forwarding rule towards the source in preparation of a reply message. When the destination (or an intermediate node that knows the forwarding path to the destination) receives a RREQ it responds with a route reply (RREP) message. The responding node places the path information collected during the RREQ into the RREP and sends it along the reverse path previously established during the RREQ flood to the source node. Each node that receives the RREP adds the forwarding rule to their route table and forwards the RREP toward the source. Because of the flooding nature of a RREQ, the destination generates a RREP for each discovered path.

Intermediate and source nodes, receiving a RREQ, RREP, or a route error (RERR) message, update their forwarding table if 1) the destination sequence number in the coordination message is higher than the one stored in their table, or 2) the destination sequence number is the same as the entry in its routing table, but the hop-count in the message is shorter. Coordination messages containing higher destination sequence numbers imply fresher routing information.

Packet forwarding is achieved via a distance vector table stored at each node in the network containing entries for each known destination. For each destination, the node stores the next hop, distance in hops to the destination, and the sequence number of the latest update to the route. When application packets arrive to be forwarded, the node examines the destination in the packet and determines the next hop using the appropriate entry in the routing table.

1.3 Dynamic Source Routing

DSR is a reactive, forward updating, source-based, and flat routing protocol [21]. Its route discovery and maintenance behavior is very similar to AODV; however, the major differences between the protocols are the manner of packet routing and how the routes are stored. Unlike AODV, the route is maintained completely by the source node in DSR. The source node is responsible for generating the route request and has complete freedom to select any route reply to use when routing packets. Instead of storing the route hop-by-hop, DSR uses source routing where the source node places complete routing information in each application packet. Each intermediate node along a route uses this information to determine the next hop. The intent of the designers is to follow the analog of the TCP/IP *fate sharing* [13] by placing the majority of the complexity burden at the end nodes.

The route selection method is not specified in [21], but rather, is left up to the implementation of the protocol. Many DSR implementations use hop count as the route selection metric, such as Network Simulator 2, PicoNet, and the Rice Monarch Project.

1.4 Related Work

A significant number of published research papers measure simulated Black Hole attacks on ad-hoc networks. Performance degradation from Black Hole attack is measured on AODV networks in [6, 11, 26, 28, 32]. For DSR, performance results can be found in [3, 9, 20, 33]. Performance measurements of Black Hole attacks in other networks types include [15, 17, 19]. Due to the large parameter space of ad-hoc networks, there is little overlap between each study; however, they all indicate that Black Hole attack decreases network throughput.

Several recent works develop analytical models to characterize the performance of Black Hole attacks. In [39],

a probabilistic model is developed to quantify the effects of a Black Hole attack in a smart grid network. In [12], an Adaptive Neural-Fuzzy Inference System (ANFIS) is created to detect Black Hole node behaviors. A Colored Petri-Net model is developed in [17]; however, the model must be simulated to derive results. The foundations of a formal Black Hole attack model for wireless sensor network routing protocols is proposed in [31].

In [1] an analytical model is presented to calculate network throughput under denial of service attacks; specifically, these attacks are Jellyfish and Black Hole. Their model estimates the availability of a network flow (i.e., a group of packets traversing a route) based the proportion of lifetime that a network flow incurs zero throughput. The expected time a route has zero throughput is calculated as the product of the probability that at least one malicious node is in an arbitrary route of a certain length and the expected correction time to expunge all malicious nodes from that route. The correction time is based on the number of attempts to detect the attack, rediscover an alternative route, and repair for each malicious node in the route. Given the expected interval of zero throughput, one can calculate availability as one minus the ratio of the time of zero throughput over the expected duration of the flow.

A completely different Black Hole model is proposed in [23] to model packet loss instead of throughput of an AODV Mobile Ad-hoc Network (MANET) during a Black Hole attack. Konig assumes uniform node density to simplify the topology so that the number of nodes included in a given topology search area may be determined. By letting the radius of this search area be a multiple of the transmission distance, one can geometrically determine the number of nodes reachable at each hop. The author of this method also makes an attempt to address the border effect errors with the uniform density assumption; however, the authors acknowledge that their method is imperfect. Given the set of nodes included in the i^{th} RREQ of the expanding ring search, Konig can find 1) the probability that at least one Black Hole is in the search area and 2) the probability that the destination is within the search area. By taking the product of these two probabilities for each phase of the ring search, the sum of products is the probability an arbitrary route in a network with a given network density is subject to Black Hole attack.

2 Revisiting the Hypercube Black Hole Attack Model

From [5], Black Hole node b in network topology G is able to provide a false route with a winning metric to drop application packets on a route from source node s to destination node d if:

$$\exists b \in B \quad s.t. \{h(s,d) > h(s,b)\}, \tag{1}$$

where $h(x,y)$ is the minimum hop distance between x and y in network topology G and B is the set of Black Hole nodes present in G. While a proof is provided in [5], the prior work did not provide experimental validation.

2.1 Validation of the Attack Condition

A series of simulated experiments are conducted to test the validity of Equation (1) by observing the effects of packet loss while varying the hop distances between the source, destination, and a Black Hole node over a linear topology. The use of a linear topology allows explicit control of the hop distances of each player in the experiment series. The linear topology consists of 21 nodes, where a single source node is placed in the center of the network and is flanked by 10 nodes on each side. For a given simulation experiment, the destination node is designated as one of the 10 nodes on the right of the source node and a Black Hole node is designated as one of the 10 nodes on the left. During the simulation, the source node attempts to establish a route to the destination. The Black Hole node participates during the route setup and attempts to move the route through itself. Once the route is selected, the source sends constant bit rate (CBR) traffic to the destination. If the Black Hole attack is successful, none of the packets reach the destination because they are being forwarded to the opposite side of the network to the Black Hole node, which drops all of them. Packet loss is recorded from 100 scenarios generated by testing all combinations of $h(s,b)$ and $h(s,d)$, where each hop distance takes on a value from 1 to 10. Each scenario is replicated 100 times to generate a mean normalized packet loss statistic, where normalized packet loss is the proportion of packets lost over the total number of sent packets. The entire sequence of experiments are conducted using both AODV and DSR protocols.

Each wireless ad-hoc node in the network is a simulation model, which is comprised of an antenna, radio, propagation model, and a protocol stack in Network Simulator 2.34 (ns-2.34). Specifically, the stack is comprised of an omni-directional antenna with unity gain, a 914MHz Lucent WaveLAN Direct Sequence Spread Spectrum (DSSS) radio, an implementation of IEEE 802.11 Medium Access Control (MAC) layer, and a reactive MANET routing protocol. The stack enables each node to provide packet routing for the wireless ad-hoc network. Besides basic routing services, some nodes are designated as application end-points, which send or receive CBR traffic. The linear topology is enforced by placing nodes in a line, where the transmission coverage area of each node contains a either two neighbors, or for the end nodes, a single neighbor. A Black Hole is a node with a modified MANET routing protocol designed to conduct Black Hole attacks and is identical to the simulation model used in [5]. The simulation transmission range of each radio is 250 meters.

The observed normalized packet loss for AODV and DSR as a function of destination and Black Hole hop distances are shown as a surface plot in Figure 1. A given point in the z axis is the normalized average packet loss observed when $h(s,b) = x$ and $h(s,d) = y$. The figure

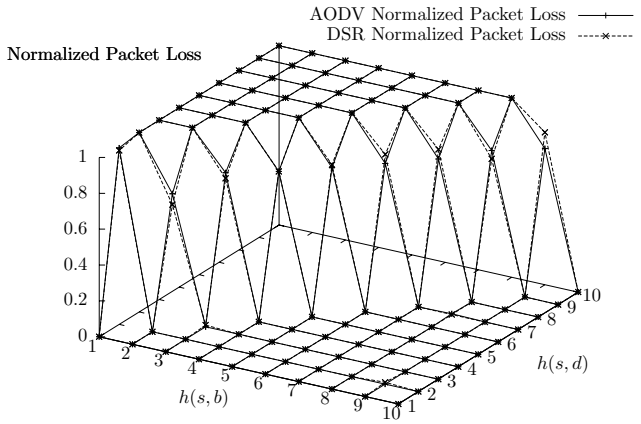


Figure 1: Normalized packet loss as a function of hop-distance

shows that in all cases where $h(s,b) \geq h(s,d)$, the packet loss is zero. Conversely, packet loss is incurred for each case where $h(s,b) < h(s,d)$. Packet loss is at 100% when $h(s,d) - h(s,b) > 1$. The reason that packet loss is only at 80% when $h(s,d) - h(s,b) = 1$ (i.e., the Black Hole node is one hop closer than the destination node to the source) is an artifact of the simulation models for AODV and DSR in ns-2.34. Recall that from [5], the shortest path a Black Hole can advertise to the source node without masquerading as the source has length $h(s,b)+1$. When $h(s,d) - h(s,b) = 1$ both the Black Hole and destination node will respond with routes having the same hop count metric. As a tiebreaker, the RREP arriving first is selected. Since $h(s,d) - h(s,b) = 1$, the RREP from the Black Hole node has fewer hops to traverse than the RREP created from the destination node. However, the simulation avoids RREQ broadcast collisions at each hop by waiting a uniformly random time period before rebroadcasting. When the destination and Black Hole hop distances to the source node are close, there are occurrences where the Black Hole node receives the RREQ at a later time than the destination because the predecessors of the Black Hole node encounter a larger cumulative random delay.

2.2 Decoupling the Hypercube Topology from the Model

The Analytical Black Hole model is the probability Equation (1) is true for all source destination pairs. This is calculated by considering all possible relative distances of $h(s,b)$ and $h(s,d)$ in a given network. From [5], the discrete probability of this event is

$$P(A) = \sum_{h=1}^{n} P(A|H=h)P(H=h), \tag{2}$$

where $P(A)$ is the probability of a Black Hole attack and $P(H)$ is the probability that $h(s,d) = h$. Given $h(s,d)$, the probability of a Black Hole attack is simply the probability that at least one of the B Black Hole nodes are closer than h hops to the source. This requires knowing the number of possible neighbors that are closer than h and finding the probability that at least one of the neighbors is a Black Hole node. The n-ary 2-cube topology is useful here because this quantity can be derived analytically given parameter n, which is the longest expected route length. Moreover, the symmetric properties of a n-ary 2-cube topology result in every node having the same quantity of unlabelled neighbors at each hop distance. This allows $P(A)$ to be calculated without considering the relative location of each source node within the topology. Let $q(x)$ be the quantity of neighbors including Black Hole nodes at hop distance x. The number of nodes that are closer than h hops is the sum of $q(x)$ for all $x = 1, 2, \ldots, h-1$. Given $q(x)$ is known for all values of x, N is the number of nodes in the topology, B is the number of Black Hole nodes in the network, then $P(A)$ is a hyper-geometric discrete random variable shown in Equation (3).

$$P(A) = \sum_{h=1}^{n} \left\{ \left(1 - \frac{\binom{(N-2)-\sum_{i=1}^{h-1} q(i)}{B}}{\binom{N-2}{B}} \right) \frac{q(h)}{N-1} \right\}. \tag{3}$$

Because this analytical model is derived for n-ary 2-cubes, the model assumes that all source nodes have the same $q(x)$ function. Decoupling the analytical model from the n-ary 2-cube topology requires that $q(x)$ is context dependent on the position of the source node within the network being analyzed. If the topology is known, then the number of $q(x)$ functions has an upper bound of N, implying that each node has a unique $q(x)$ function. Moreover, the conjecture is that the set of these $q(x)$ functions is sufficient to describe the network topology under study. If a topology exhibits symmetry, then there will consequently be duplicate $q(x)$ functions describing the network. Ignoring duplicate functions, fewer $q(x)$ functions are required to describe the symmetric topology. Let a *source node class* be a set of one or more nodes that share the same $q(x)$ function. More specifically, source node class C_k has $q_i(x) = q_j(x) \forall i, j \in C_k; x = 1, 2, \ldots, n$. When a route discovery is initiated, there is an associative probability that the source node originating the discovery belongs to a particular source node class. The source node class membership probability equation is simply the proportion of nodes in a class over the number of nodes in the network, where $|C_k|$ is the cardinality of class C_k. This is

$$P(s \in C_k) = \frac{|C_k|}{N} \forall C_k, k = 1, 2, \ldots, K. \tag{4}$$

Incorporating Equation (4) into the model results in

$$P(A) = \sum_{k=1}^{K} \sum_{h=1}^{n} P(A|H=h)P(H=h|s \in C_k)P(s \in C_k). \tag{5}$$

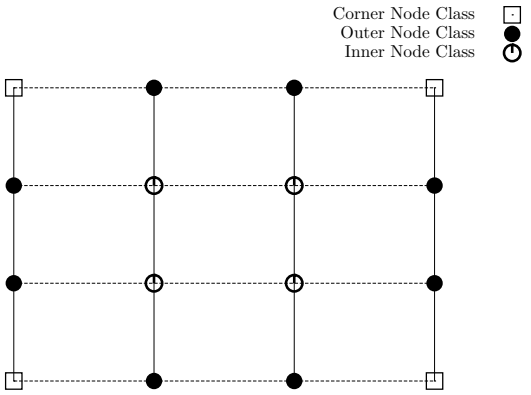


Figure 2: 4x4 Wireless grid topology with labeled source node classes

Note that K is the number of source node classes for the network and its value is a function of the topology under study. Expanding Equation (5) is

$$P(A) = \sum_{k=1}^{K} \sum_{h=1}^{n} \left\{ \left(1 - \frac{\binom{(N-2)-\sum_{i=1}^{h-1} q_k(i)}{B}}{\binom{N-2}{B}} \right) \frac{q_k(h)|C_k|}{N(N-1)} \right\}. \quad (6)$$

2.3 Validation of the Generalized Attack Model

Equation (6) is validated through a series of simulated experiments. To illustrate the concept of source node classes and $q(x)$ functions, these experiments use a simple fixed 4x4 grid network. To keep the topology fixed at 16 nodes and in a 4x4 grid structure, non-Black Hole nodes are removed from the network as Black Hole nodes are added. This keeps the number of source node classes and $q(x)$ functions constant. The distances between nodes force communication between only cardinally adjacent nodes in the grid. A 4x4 grid topology has three source node classes, labeled C_1: *Corner Nodes*, C_2: *Outer Edge Nodes*, and C_3: *Inner Nodes*. Figure 2 shows the topology with each node assigned to one of the three source node classes. From the figure there are four corner nodes in C_1, eight outer nodes in C_2, and four inner nodes in C_3 respectively. The $q_k(x)$ function (i.e., the quantity of neighbors x hops from a source node in class k) for each source node class is shown in Table 1.

Table 1: Values for $q_k(x)$ for each source node class in the 4x4 grid

Hop Distance	$x =$	1	2	3	4	5	6
Corner Nodes	$q_1(x) =$	2	3	4	3	2	1
Outer Edge Nodes	$q_2(x) =$	3	4	4	3	1	0
Inner Nodes	$q_3(x) =$	4	6	4	1	0	0

The normalized packet loss is observed as the number of Black Hole nodes are increased in the topology from one to eight. For each scenario, 50 4x4 grid topologies are generated. For each topology a subset of the 16 nodes are randomly designated as Black Hole nodes and 100 source-destination pairs are also randomly designated. Each connection pair is independently simulated, where the source attempts to establish a route with the destination in the presence of Black Hole nodes. Once the route exists, the source sends CBR traffic to the destination. Each simulation is repeated 10 times to account for the random packet delay incurred during the simulation and to avoid confounding effects of congestion and route caching, which are not currently accounted for in the analytical model. Statistics on the number of dropped, sent, and received packets are collected and used to estimate the mean normalized packet loss for each factor level combination.

The probability of attack is calculated using Equation (6) and is overlaid with the simulation results in Figure 3. Clearly the analytical model's predications are within the 95% confidence intervals (CIs) for all Black Hole levels for both protocols. The figure also shows that the attacker experiences diminishing returns as the number of Black Hole nodes grows, with an upper-bound at approximately 78% normalized packet loss. An attacker may use this curve to optimize cost of placement versus payoff. Using this network as a example, approximately three quarters of the maximum performance is achieved by deploying at least three Black Hole nodes. In terms of security defense analysis, the expected packet loss does not exceed 80%. System designers may use this upper-limit to implement distributed applications that tolerate operating conditions, such as through caching, redundancy, or multipath.

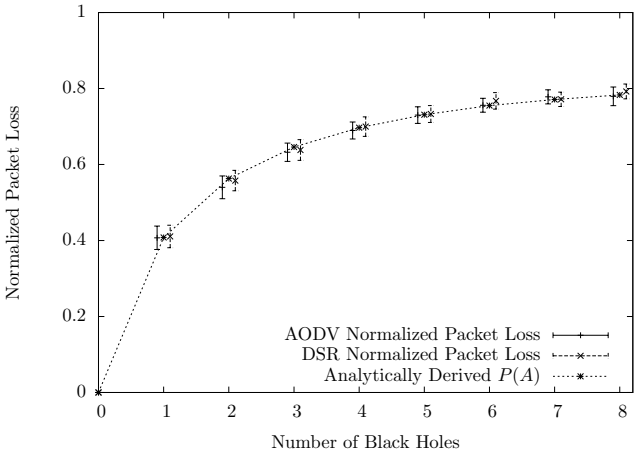


Figure 3: Normalized packet loss due to Black Hole attack for the 4x4 grid network

3 The Attack Model Adapted for Ad-hoc Networks

The analytical model presented in the previous section is generalized to account for any topology that may be described as a set of source node classes, each with a particular $q(x)$ function. However, there are several challenges to overcome so that this analytical model may be useful for ad-hoc networks while avoiding the n-ary 2-cube approximation technique. First, the topology is not known *apriori*, making it difficult to assess the susceptibility of a network is instantiated. Second, ad-hoc networks may be partitioned, which violates the assumptions of the original model. In this section, the analytical model is enhanced to address these two challenges.

3.1 Describing Ad-hoc Topologies Stochastically

In [8], the authors stochastically generate random topologies using a small set of parameters to empirically derive neighbor hop distance probability density functions for a variety of ad-hoc network types. This work expands on [8] by using K-means clustering on stochastically generated topologies to identify K distinct source node classes and the associative $q_k(x)$ functions (i.e., neighbor hop distance probability density functions) to represent an expected configuration of the ad-hoc network prior to its existence. Using this approach, only the deployment strategy, number of nodes, and operating area are required *apriori*. Unlike the case for known topologies, the number of classes is not bounded by the number of nodes N. Because the network may take on a variety of topology configurations, K may be orders of magnitude larger than N, which implies that a larger set of $q(x)$ functions are required to adequately describe an ad-hoc network than a particular topology instantiation such as the 4x4 grid topology, described in a previous section.

The strategy of this approach is to generate a set of source node classes that adequately describe the distribution of possible topology instantiations. This is accomplished stochastically by generating M random topology instances according to the expected number of nodes, area of deployment, and deployment strategy. For each of the M topology instances, the $q(x)$ function of every node is empirically derived, resulting in a collection of $M \times N$ distinct $q(x)$ samples. The $q(x)$ function samples are associated using K-means clustering [36]. This results in the identification of K source node classes, where the center of each class C_k is an n-dimensional vector of hop-distance quantities (i.e., $q_k(x)$). For stochastic topologies, the probability that source node s belongs to a particular source node class C_k is estimated as the proportion of the generated $q(x)$ samples in cluster k over the total number of generated $q(x)$ samples. The update to Equation (4) is shown in Equation (7).

$$P\left(s \in C_k\right) = \frac{|C_k|}{MN}, \tag{7}$$

where N is the number of nodes and M is the number of instantiated topologies.

3.2 Network Partitioning

Given the area, number of nodes, and deployment strategy, there is some probability that ρ nodes will be partitioned due to spatial separation. To account for partitioned nodes, let ρ_k be the average number of partitioned nodes for source node class C_k. This statistic can be derived using $q_k(x)$, where

$$\rho_k = N - \sum_{h=1}^{n} q_k(h).$$

When a destination node is partitioned from a source node, the existence of any Black Hole in the same network partition as the source node results in a Black Hole attack. Moreover, a route is established and additional network traffic is generated that would otherwise have not existed. The effect is that on a pair-wise comparison, partitioned networks with Black Hole nodes will not only have increased packet loss; they will also have an increase in the number of sent packets. Let ψ be a random event where the source attempts to connect with a destination that is one of the ρ nodes partitioned from the source node. With respect to a given source node class C_k, the probability a randomly selected destination is partitioned is

$$P\left(\psi_k\right) = \frac{\rho_k}{N-1}.$$

Given that the destination node is partitioned from the source node $s \in C_k$, the source node will only receive replies from Black Hole nodes during route discovery. Therefore, if there is at least one Black Hole node that is not partitioned from the source, then a Black Hole attack occurs. The equation for this is

$$P(A|\psi_k) = \begin{cases} B < \rho_k, & \left(1 - \frac{\binom{\rho_k - 1}{B}}{\binom{N-2}{B}}\right) \\ B \geq \rho_k, & 1 \end{cases} \tag{8}$$

Note that when there are greater or equal number of Black Holes nodes than the expected number of partition nodes, then at least one Black Hole node must exists in the same partition as the source node.

3.3 Stochastic Analytical Black Hole Attack Model for Ad-Hoc Networks

Considering the stochastic representation of the ad-hoc topology and accounting for partitioning, the revised form of the analytical model for Black Hole attack on ad-hoc networks is

$$P(A) = \sum_{k=1}^{K} \left\{ \left[P(A|\psi_k) P(\psi_k) + P(A|\psi_k^{'}) \left(1 - P(\psi_k)\right) \right] P(s \in C_k) \right\}. \tag{9}$$

Table 2: Four simulated ad-hoc network types under test

Type	Nodes	Area (m^2)	Density (m^{-2})
1	10	500	0.02
2	20	500	0.04
3	20	1000	0.02
4	40	1000	0.04

The probability of attack is the sum of the attack probabilities for all source node classes. For each class C_k, the attack probability accounts for events including partitioned destinations and non-partitions with probabilities $P(\psi_k)$ and $(1 - P(\psi_k))$ respectively. Since $P(A|\psi_k)$ is defined in Equation (8), this leaves $P(A|\psi_k^{'})$ to be defined, which is

$$\begin{aligned} P(A|\psi_k^{'}) &= \sum_{h=1}^{n} P(A|H)P(H=h) \\ &= \sum_{h=1}^{n} \left[\left(1 - \frac{\binom{N-2-\sum_{i=i}^{h-1} q_k(i)}{B}}{\binom{N-2}{B}} \right) \frac{q_k(h)}{N-\rho_k-1} \right]. \end{aligned} \quad (10)$$

Equation (10) is derived from Equation (3) and adjusted to account for partitioned nodes. With Equations (8), (10) and for completeness, the analytical model expression is expanded to

$$P(A) = \sum_{k=1}^{K} \left\{ \left[P(A|\psi_k) \frac{\rho_k}{N-1} + \left(1 - \frac{\rho_k}{N-1} \right) P(A|\psi_k^{'}) \right] \frac{|C_k|}{MN} \right\}. \quad (11)$$

3.4 Validation of Revised Model

An experiment is conducted via simulation to validate the revised analytical Black Hole attack model for ad-hoc networks. Four distinct topology types are chosen to represent a sample space of ad-hoc topologies that vary in operating area, number of nodes, and the resulting density. The properties of each topology type are described in Table 2.

Each topology type has its own set of source node classes, which are found using the population sampling and K-means clustering method described earlier in this paper. One thousand random topologies are generated to create large sample sizes for each topology type. K-means clustering is applied to each sample set, where $K = 200$ is found by analyzing the change in variance as K increases [37]. The experiment is a full factorial design with factors of topology type, number of Black Hole nodes (1 to 10), and ad-hoc network protocol (AODV and DSR), resulting in 80 distinct factor-level combinations. For each factor-level combination, 100 topology instances are generated and simulated independently. For each topology instance, 100 randomly selected source-destination pairs attempt to establish routes and transmit CBR traffic in the presence of Black Hole nodes. The quantity of replications is selected to minimize sampling bias in the results. The packet loss for each connection is recorded and used to derive an estimate of the expected packet loss for the factor-level combination. Because the analytical model does not account for congestion or mobility dynamics, they are not simulated in this experiment to avoid measuring confounding factors.

3.5 Results and Analysis

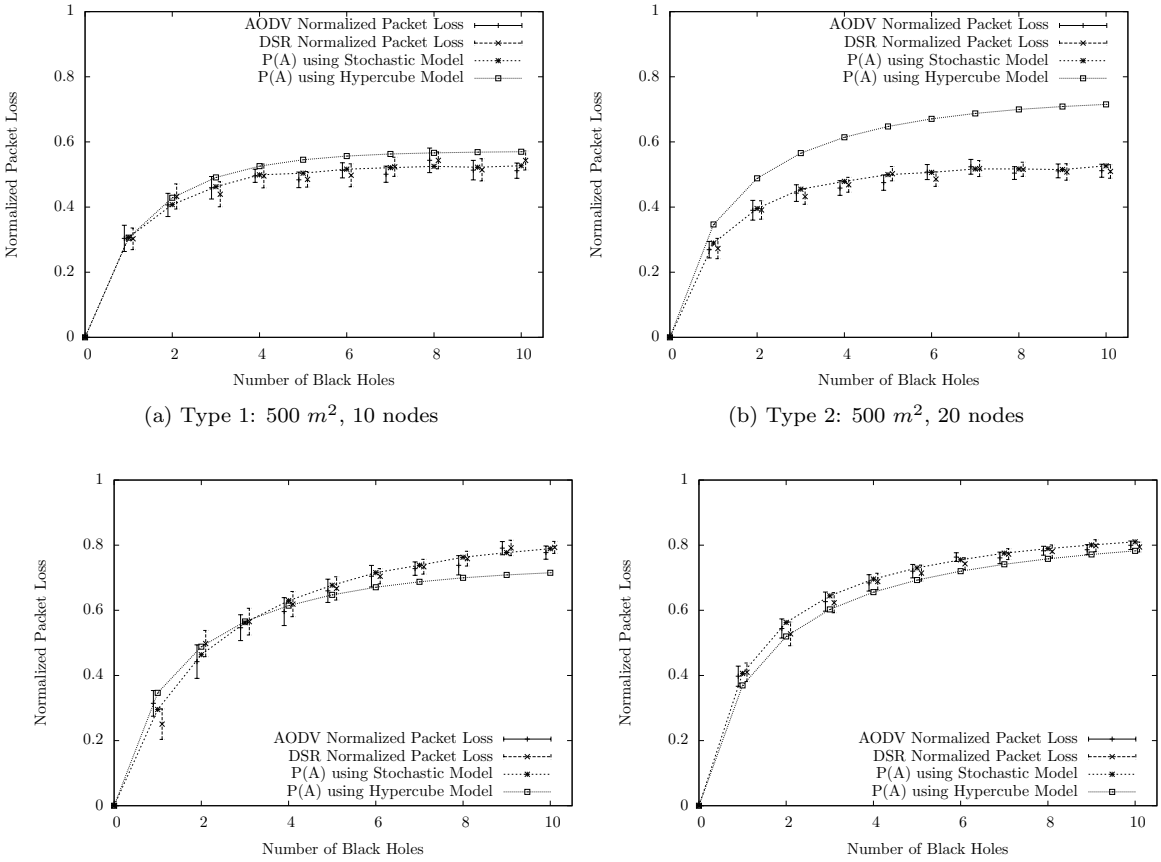
The results of the experiment are shown in Figure 4. For each topology type, the measured 95% CI of the normalized packet loss for AODV and DSR is plotted against analytical results calculated using Equation (11). The analytical model derived in [5] is also plotted to evaluate the benefits of the enhancements to this model. For this case, the hypercube with the closest number of neighbors is used as the topology approximation model. With respect to the figure, the x axis indicates the number of Black Hole nodes deployed into the network for a given normalized packet loss response.

The results show that the stochastic analytical model's prediction of packet loss falls within the 95% CI for all scenarios for each topology type. This is strong evidence in support of the claim that $P(A)$, as calculated by the revised analytical model, can be used to predict normalized packet loss of a network under Black Hole attack. Moreover, the original hypercube analytical model performs poorer than the stochastic model for the ad-hoc topology scenarios under study. In Figures 4a and 4d, the hypercube topology estimates are tolerable, but in several cases the analytically derived performance values are under or over estimating the simulation results. The hypercube topology approximation does not predict normalized packet loss for ad-hoc topology types 2 and 3. In Figure 4b the hypercube model significantly overestimates Black Hole attack. The hypercube performance curve in Figure 4c both under-estimates and over-estimates performance. Excluding the cases where there are zero Black Holes, the hypercube model prediction falls within the 95% CI packet loss in only nine of the 40 remaining data points presented in Figure 4.

Another noticeable difference between the performance predictions of the two models is that the stochastic curve has some slight variation between data-points while the hypercube performance curves do not. This is because the source node classes are derived statistically and consequently incur a degree of sample variation in the K class $q(x)$ functions. On the other hand, the hypercube analytical model uses the n-ary 2-cube topology, so it has no amount of variation in its single source node class $q(x)$ function.

4 Conclusion

This work provides a network availability model to be used to assess the impact of network disruption due to Black Hole attacks for insecure reactive ad-hoc protocols in ad-hoc topologies. Given the downsides to using a hypercube topology, the model is revised and a series of experiments are performed to validate these revisions.



(a) Type 1: 500 m^2, 10 nodes

(b) Type 2: 500 m^2, 20 nodes

(c) Type 3: 1000 m^2, 20 nodes

(d) Type 4: 1000 m^2, 40 nodes

Figure 4: Simulated packet loss of ad-hoc networks vs. hypercube and stochastic analytical model predictions

First, the attack condition is validated using an experiment where a linear topology is used to enforce a variety of hop distances between a source, destination, and Black Hole node. The results confirm the effectiveness of a Black Hole attack is based on the relative hop distances.

Second, rather than utilize the hypercube approximation technique, the analytical model is generalized to use arbitrary topologies for calculating the attack probability, where a topology is represented as a set of source node classes, each with a unique $q(x)$ function. A given $q(x)$ function represents an existential pattern within the topology that describes the number of neighbors at a given hop distance x. A second experiment is conducted using simulation for a grid network to validate the generalization of the analytical model. A 4x4 grid topology is used because the topology is deterministic and requires only three source node classes to represent the entire topology of 16 nodes. The experimental results show that the analytical model is able to utilize the $q(x)$ functions of the three source node classes to predict the mean normalized packet loss of the topology as a function of the number of Black Hole nodes in the topology.

Third, the analytical model is extended to account for specific aspects of ad-hoc topologies. Because the topology is not known until it is instantiated, the source node classes cannot be explicitly realized. Instead, they are statistically derived using K-means clustering on a large sample of instantiated topologies having the same number of nodes, operating area, and deployment strategy. The ad-hoc topology may contain zero or more network partitions. In this work, the model is extended to account for cases where the source node is partitioned from a destination node. A third experiment is conducted through simulation to validate the ad-hoc network adaptations to the model. Four different types of networks are studied by varying the number of nodes and operating area. The results show that the additions to the analytical model aid it in predicting the impact of Black Hole attacks on ad-hoc networks. Moreover, the experiment shows that the revised model provides better prediction of mean normalized packet loss than using the original hypercube model. For this experiment, the hypercube model correctly predicts 9 out of 40 scenarios, whereas the stochastic analytical model correctly predicts measured normalized packet loss for all 40 scenarios, suggesting a significant improvement in the model.

Given these accomplishments, there are several areas identified as future work. First, to minimize confounding effects and measure fundamental Black Hole attack response, the significant aspects of congestion and mobil-

ity have been avoided. With the foundational results of this research, future work should examine these aspects; the analytical work in [18] may provide a starting point. Second, there are several varieties of Black Hole attacks and many other types of network disruption attacks. The theory and model presented in this paper address a single type of Black Hole attack. This work can be readily extended to address other variants of the attack such as commandeering, masquerading, and wormholes.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

References

[1] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Impact of denial of service attacks on ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 16, no. 4, pp. 791–802, 2008.

[2] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks," in *The 15th International Conference on Computer Modelling and Simulation (UKSim'13)*, pp. 693–698, 2013.

[3] A. S. Al Shahrani, "Rushing attack in mobile ad hoc networks," in *The Third International Conference on Intelligent Networking and Collaborative Systems (INCoS'11)*, pp. 752–758, 2011.

[4] T. R. Andel and A. Yasinsac, "On the credibility of manet simulations," *IEEE Computer*, vol. 39, no. 7, pp. 48–54, 2006.

[5] C. W. Badenhop and B. E. Mullins, "A black hole attack model using topology approximation for reactive ad-hoc routing protocols," *International Journal of Security and Networks*, vol. 9, no. 2, pp. 63–77, 2014.

[6] A. Bala, M. Bansal, and J. Singh, "Performance analysis of manet under blackhole attack," in *The First International Conference on Networks and Communications*, pp. 141–145, 2009.

[7] D. Bell and L. LaPadula, *Secure Computer Systems: Mathematical Foundations*, Technical Report MTR-2547, MITRE Corporation, 1973.

[8] C. Bettstetter and J. Eberspacher, "Hop distances in homogeneous ad hoc networks," in *The 57th IEEE Semiannual Vehicular Technology Conference*, vol. 4, pp. 2286–2290, 2003.

[9] N. Bhalaji and A. Shanmugam, "Association between nodes to combat blackhole attack in dsr based manet," in *The International Conference on Wireless and Optical Communications Networks*, pp. 1–5, 2009.

[10] D. F. C. Brewer and M. J. Nash, "The chinese wall security policy," in *IEEE Symposium on Security and Privacy*, pp. 206–214, 1989.

[11] K. Chadha and S. Jain, "Impact of black hole and gray hole attack in aodv protocol," in *Recent Advances and Innovations in Engineering (ICRAIE'14)*, pp. 1–7, 2014.

[12] A. Chaudhary, V. N. Tiwari, and A. Kumar, "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in manets," *International Journal of Network Security*, vol. 18, no. 3, pp. 514–522, 2016.

[13] D. Clark, "The design philosophy of the darpa internet protocols," *ACM SIGCOMM*, vol. 18, no. 4, pp. 106–114, 1988.

[14] X. Fei and W. Wenye, "On the survivability of wireless ad hoc networks with node misbehaviors and failures," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 3, pp. 284–299, 2010.

[15] D. M. Gregg, W. J. Blackert, D. V. Heinbuch, and D. Furnanage, "Assessing and quantifying denial of service attacks," in *Military Communications Conference*, vol. 1, pp. 76–80, 2001.

[16] O.-E. Hedenstad, "Security model for resource availability - subject and object type enforcement," in *Military Communications Conference*, pp. 1–7, 2009.

[17] H. Hejiao and Z. Qiang, "Petri-net-based modeling and resolving of black hole attack in wmn," in *The 36th Annual Computer Software and Applications Conference Workshops (COMPSACW'12)*, pp. 409–414, 2012.

[18] X. Hui, W. Xianren, H. R. Sadjadpour, and J. J. Garcia-Luna-Aceves, "A unified analysis of routing protocols in manets," *IEEE Transactions on Communications*, vol. 58, no. 3, pp. 911–922, 2010.

[19] R. K. Jha, U. D. Dalal, and I. Z. Bholebawa, "Performance analysis of black hole attack on wimax-wlan interface network," in *The Third International Conference on Computer and Communication Technology (ICCCT'12)*, pp. 303–308, 2012.

[20] C. Jiwen, Y. Ping, T. Ye, Z. Yongkai, and L. Ning, "The simulation and comparison of routing attacks on dsr protocol," in *The 5th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4, 2009.

[21] D. Johnson, Y. Hu, and D. Maltz, *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks*, Technical Report RFC-4728, IETF, 2007.

[22] D. Kiwior and L. Lam, "Routing protocol performance over intermittent links," in *Military Communications Conference*, pp. 1–8, 2007.

[23] A. Konig, D. Seither, R. Steinmetz, and M. Hollick, "An analytical model of routing, misbehavior, and countermeasures in mobile ad hoc networks," in *Global Telecommunications Conference*, pp. 1–6, 2009.

[24] S. Lipner, "Non-discretionary controls for commercial applications," in *Symposium on Privacy and Security*, pp. 2–10, 1982.

[25] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in rpl-based internet of things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459–473, 2016.

[26] K. Pavani and D. Avula, "Performance evaluation of mobile adhoc network under black hole attack," in *The International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA'12)*, pp. 1–6, 2012.

[27] C. Perkins, E. Belding-Royer, and S. Das, *Ad Hoc on-demand Distance Vector (AODV) Routing*, Technical Report RFC-3561, IETF, 2003.

[28] N. Purohit, R. Sinha, and K. Maurya, "Simulation study of black hole and jellyfish attack on manet using ns3," in *The Nirma University International Conference on Engineering (NUiCONE'11)*, pp. 1–5, 2011.

[29] F. Qian, C. Zhongmin, Y. Jin, and H. Xunchao, "A performance comparison of the ad hoc network protocols," in *The Second International Workshop on Computer Science and Engineering*, vol. 2, pp. 293–297, 2009.

[30] Y. Saad and M. H. Schultz, "Topological properties of hypercubes," *IEEE Transactions on Computers*, pp. 867–872, 1988.

[31] K. Saghar, D. Kendall, and A. Bouridane, "Application of formal modeling to detect black hole attacks in wireless sensor network routing protocols," in *The 11th International Bhurban Conference on Applied Sciences and Technology (IBCAST'14)*, pp. 191–194, 2014.

[32] R. K. Sahu and N. S. Chaudhari, "Performance evaluation of ad hoc network under black hole attack," in *World Congress on Information and Communication Technologies (WICT'12)*, pp. 780–784, 2012.

[33] M. Salehi, H. Samavati, and M. Dehghan, "Evaluation of dsr protocol under a new black hole attack," in *The 20th Iranian Conference on Electrical Engineering (ICEE'12)*, pp. 640–644, 2012.

[34] K. J. Sarma, R. Sharma, and R. Das, "A survey of black hole attack detection in manet," in *The International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT'14)*, pp. 202–205, 2014.

[35] Z. Siyu, P. Yongxiang, Y. Yang, and L. Jianping, "An open architecture for the routing protocols design in ad hoc networks," in *The 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT'10)*, vol. 7, pp. 18–22, 2010.

[36] H. Suoto and S. B. Sen, "Cluster-based region formation for modeling manet," in *Military Communications Conference*, pp. 1–7, 2007.

[37] R. L. Thorndike, "Who belongs in the family?," *Psychometrika*, vol. 18, no. 4, pp. 267–276, 1953.

[38] P. Yau and C. Mitchell, "Security vulnerabilities in ad hoc networks," in *The 7th International Symposium on Communication Theory and Applications*, pp. 148–153, 2003.

[39] S. A. R. Zaidi and M. Ghogho, "Stochastic geometric analysis of black hole attack on smart grid communication networks," in *The Third International Conference on Smart Grid Communications (SmartGridComm'12)*, pp. 716–721, 2012.

Christopher Badenhop is a PhD student in the Department of Electrical and Computer Engineering, Air Force Institute of Technology. He received a Masters in Cyberspace Operations from Air Force Institute of Technology in 2012 and a Masters in Computer Engineering from Wright State University in 2006. His research interests include computer network security, embedded system security, and RF communications.

Benjamin Ramsey is an Assistant Professor of Computer Science at the Air Force Institute of Technology. He received the PhD degree in computer science from the Air Force Institute of Technology in 2014. His research interests include wireless network security and critical infrastructure protection.

Barry Mullins is a Professor of Computer Engineering at the Air Force Institute of Technology. He received the PhD degree in electrical engineering from Virginia Polytechnic Institute and State University in 1997. His research interests include cyber operations, software reverse engineering, computer and network security, critical infrastructure protection, and reconfigurable computing systems.

Stride Towards Proposing Multi-Modal Biometric Authentication for Online Exam

A. Prakash[1,2], R. Dhanalakshmi[3]
(Corresponding author: A. Prakash)
Department of Computer Science and Engineering, Hindustan University[1]
Rajiv Gandhi Salai (OMR), Padur, Kelambakam, Chennai 603103, India
Information Technology, Jerusalem College of Engineering[2]
Velacherry Tambaram Main Road, Pallikkaranai, Chennai 600100, India
(Email: prakash1712@yahoo.com)
Department of Computer Science and Engineering, KCG College of Technology[3]
KCG Nagar, Rajiv Gandhi Salai, Karapakkam, Chennai 600097, India
(Received June. 7, 2015; revised and accepted Aug. 11 & Sep 5, 2015)

Abstract

Biometric authentication has been getting widespread attention over the past decade with growing demands in automated secured personal identification and has been employed in diverse fields. It ensures actual presence of biometric entity of a person in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem. Also in the previous work they use face and dress color as hard and soft biometric traits. The major drawback of the existing continuous authentication system is, it is able to successfully authenticate the user continuously with high tolerance to the user posture. So, to overcome this drawback and improve the systems robustness against illumination changes and cluttered background, in this paper we use additional biometric traits which are mole, ornament details and face dimensions in addition to the dress color and face color. Also, we extend it to the online exam application. That is, continuously monitoring of a person in an online exam is proposed employing hard biometric like facial recognition and soft biometrics. Modified PCA (Principal Component Analysis) is employed here for the facial recognition part. Both the hard biometric (face) and soft biometrics is fused with the help of optimization algorithm based similarity technique. Finally the authentication is performed and evaluated using standard evaluation metrics. The technique is implemented in MATLAB and will be compared to prominent existing techniques.

Keywords: Biometric traits, continuous biometric authentication, face recognition, MPCA, multimodal biometric systems

1 Introduction

The excellence of a biometric technique is assessed by means of its inherent competence in recognition, which is estimated using the bogus refutation and fake acceptance paces. The birth of the multimodal biometrics is brought about by the synthesis of the diverse biometric mode data at the trait mining, match score, or decision level [17]. One of the generally used biological features is the face recognition [18]. Face recognition has the aim of identifying individuals in photographs or videos from their facial appearance. When comparing is done with other biometrics, face recognition is found passive and does not necessitate supportive persons who are close to sensor or in contact with it. Human faces, automatic recognition are an aggressively investigated part, which discovers many applications such as surveillance, authentication or human-computer interaction. In universal and non-intrusive biometric, face is an effortlessly obtainable [17], which makes it perfect for applications where other biometrics such as fingerprints or iris scanning are not possible [13]. In pattern recognition system, the most focused area is face recognition. The face recognition rate will get affected due to variation of human face like different pose, illumination and different expression. Real-world automatic face recognition tackled these variations [14]. Under different illumination environment it is not simple to attain for robust face recognition. The variation of illumination causes changes in face appearance considerably, it discriminate that the difference between the changes in same face image due to illumination is higher than the variation due to change in face identity [10]. It is accepted by numerous that feature based face recognition systems hold guarantee in specific applications where movement can be utilized as a sign for face segmentation and tracking, and the vicinity of more information can

expand recognition execution. On the other hand, these systems have their own difficulties. They oblige tracking the video sequence, and recognition algorithms that have the capacity to incorporate data over the whole video. The capacity of diverse approaches to adapt to face posture and misalignment can be generally controlled by the measure of express geometric data they use in the face representations [10].

The fundamental objective of face recognition system is to divide the qualities of a face that are controlled by the intrinsic shape and color of the facial surface from the arbitrary states of image generation. Different methods were utilized for the face recognition methodology like Diffusion-Based Face Selective Smoothing in DCT Domain where impact of illumination changes on distinctive frequency subbands and propose a dissemination based image selective smoothing algorithm to eliminate the undesired impacts of illumination varieties [9]. Soft biometrics additionally has increased considerable significance. Soft biometric attributes are characterized as "those qualities that give some information about the individual, however fail to possess the peculiarity and perpetual quality to sufficiently separate any two individuals [11]. These characteristics incorporate sexual orientation, ethnicity, colour of eye/skin/hair, tallness, weight, and SMT (scars, marks, and tattoos). While soft biometric attributes do not have sufficient oppressive information to completely verify the client, it has been demonstrated that they can enhance system login security when consolidated with hard biometric characteristics [4].

2 Literature Review

Recently, a number of researches are being carried out in multi-biometric authentication area. A brief review of some of these researches is given in this section, especially related to facial recognition based authentication.

Galbally et al. [5] proposed security of biometric recognition frameworks by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The technique consisted of two phases namely, feature extraction phase and classification phase. In feature extraction phase, the features amounting to 25 of them were extracted. It included full reference based features and no reference based features. Subsequently, classification based on these features was carried out by the trained QDA classifier. The proposed technique was applied to Iris, Fingerprint and Face Recognition.

Chen et al. [3] had proposed a method for face recognition or authentication against pose, illumination, and expression (PIE) variation using modular face features. A sub-image in low-frequency sub-band was extracted by a wavelet transform (WT) to reduce the image dimensionality. It was partitioned into four sections for indicating to the local features and diminishing the PIE impacts, and the small image in a coarse scale was produced by means of the WT without losing the worldwide face features. Five measured feature spaces were developed. The most discriminative common vectors in each one feature space were found, and a nearest feature space-based (NFS-based) distance was ascertained for characterization. The weighted summation was performed to combine the five distances. Examinations were directed to demonstrate that the proposed method was better than traditional techniques.

Shermina and Vasudevan [1] had proposed a face recognition method that was robust to pose and illumination variations. For processing the pose invariant image, the Locally Linear Regression (LLR) method was used to create the virtual frontal view face image from the non frontal view face image. The low frequency components of Discrete Cosine Transform (DCT) were utilized to regularize the illuminated image during processing the illumination invariant image. The Fisher Linear Discriminant Analysis (FLDA) method and Principal Component Analysis (PCA) methods were implemented to identify the facial images with both pose variant and illumination variant. To be a last element the scores regarding FLDA and also PCA were being combined utilizing a hybrid approach based on the Feed Forward Neural Network (FFN). Scores obtained from the initial recognition method, the weight was allocated to the image. The authentication process of image was form on the weight assigned and the mixture of the scores. The experimental results determined that their proposed method based on hybridization technique recognizes the face image was efficiently than traditional method.

Ajay et al. [19] had compared the performance of various combinations of edge operators and linear subspace methods to determine the best combination for pose classification. To estimate the behavior, they had accomplished analysis on CMU-PIE database which had images with wide variation in illumination and pose. They established that the behavior of pose classification mainly dependent on the selection of edge operator and linear subspace method. From Prewitt edge operator and Eigen feature regularization approach the most excellent classification precision was attained. Adaptive histogram equalization was utilized as a preprocessing step to adapt illumination variation, which resulting into considerable improvement in performance.

Muruganantham [6] had proposed a method that offers an up-to-date evaluation of major human face recognition research. They presented a summary of face recognition and its applications. The face databases, explanation and restrictions which were used to evaluate the performance of these face recognition algorithms were given. The face recognition system was mostly affected by four significant factors; they were pose illumination, uniqueness, occlusion and facial expression. Here they anticipated a vital evaluation of the current researches related with the face recognition process. They proposed a wide review of most important researches on face recognition process accomplished on various scenarios. Additionally, abbreviation

portrayal of face recognition process in conjunction with the methods linked with the different factors that affected the face recognition process

Arindam et al. [12] had proposed a method for automatic face recognition by means of integrated peaks of the Hough transformed significant blocks of the binary gradient image. In this technique initially the gradient of an image was computed and a threshold was get on with it to obtain a binary gradient image, which was less responsive to noise and illumination changes. Secondly, major blocks were taken out from the absolute gradient image, to obtained pertinent information with the idea of dimension reduction. Lastly the most excellent fitted Hough peaks were taken out from the Hough transformed significant blocks for competent face recognition. These Hough peaks were joined together, which were utilized as feature in classification process.

Choudhary et al. [7] had proposed a method to label a Self-Organizing Map (SOM) to measure image similarity. In their work, into the neural network the facial images along with the regions of interest were introduced. After completion of training process, each neural block was tuned to a particular facial image prototype. Then, the probabilistic decision rule performed facial recognition. Their method provided very accurate results for face identification along with illumination variation and facial poses and facial expressions. From a single database onwards the SOM method was trained. A facial recognition system automatically recognized a person, which obtained from a digital image or video frame from a video source. It was applied in security systems and the analysis could be compared with other biometric recognition system like fingerprint or eye iris recognition systems.

Khourya et al. [16] were presented bi-modal biometric authentication on mobile phones in challenging conditions. They looked at the issue of face, speaker and bi-modal verification in mobile situations when there was critical condition disparity. They presented this disparity by selecting customer models on high quality biometric samples acquired on a laptop computer validating them on lower quality biometric examples gained with a mobile phone. To perform these tests they build up three novel authentication protocols for the expansive publicly available MOBIO database. They assessed state-of-the-art face, speaker and bi-modal validation methods and demonstrated that between session variability modelling utilizing Gaussian mixture models gave a reliably powerful system to face, speaker and bi-modal verification. It was likewise demonstrated that multi- algorithm combination gave a steady execution change to face, speaker and bi-modal authentication. Utilized the bi-modal multi- algorithm system they infer a state-of-the-art authentication framework that acquired a half total error rate of 6.3 % and 1.9 % for Female and Male trials, separately.

3 Problem Identification

There are several issues that threaten the security in biometric authentication systems. User authentication merely at the very first login session is one among these severe issues, which is normally found in majority of the currently available computer and network systems. This issue is a massively serious security issue, particularly in systems with high security requirement, since an imposter is permitted to access the resources in the system in the period between user log in and user log out.

Together with this, only using the face and dress color as biometric traits in continuous authentication system reduces the accuracy of the system under pose variations. Also, the previous continuous biometric system uses PCA for face recognition. But the PCA has various drawbacks such as, recognition rate is not high in case of images having different poses, facial expressions and change in illumination and also the accuracy rate is not high.

4 Proposed Continuous Biometric Authentication System

There are several issues that threaten the security in biometric authentication systems. User authentication merely at the very first login session is one among these severe issues, which is normally found in majority of the currently available computer and network systems. This issue is a massively serious security issue, particularly in systems with high security requirement, since an imposter is permitted to access the resources in the system in the period between user log in and user log out. Therefore, this paper introduces a continuous biometric authentication system, wherein, the system is observed incessantly from the time the user logs in. This system makes use of diverse user authentication modalities like face, ornaments, dress colour, beard, scars and mustache for monitoring the logged in user in a continuous manner. Moreover, the login security of this system is augmented through the union of hard as well as soft biometric traits. Figure 1 portrays the entire block representation of the proposed continuous multimodal biometric authentication system.

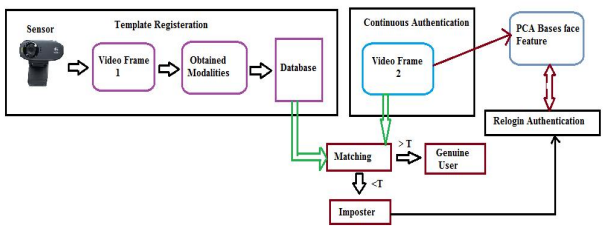


Figure 1: Block diagram of the proposed method

From the above figure, it is clear that the user's image is captured via a sensor in the beginning. Next, the de-

sired user authentication modalities are chosen from the sensor image and registered in the database. Face, ornaments, dress colour, beard, scars and mustache serve as the necessary modalities for authentication. This is then followed by the continuous authentication process, which is performed through the matching of the registered template and the subsequent video frame. Normalized cross correlation process is being utilized for carrying out the matching procedure. At the end of matching, the similarity score is produced from each and every modality. Later on, the Group Search Algorithm (GSO) with optimized weights aids in fusing these scores. Then, a threshold is preset to allow the authentication of the user as the genuine user or the imposter. A genuine user will be the authentication result, if the fused score exceeds the predetermined threshold. Otherwise, the presence of imposter is evident. In the proposed system, a remedy is provided for the situation with an imposter. Re-login authentication mode is that remedy, wherein, matching is accomplished with the application of the Modified principle component analysis (MPCA) on the face image. The following sections give a concise explanation of the proposed continuous biometric authentication system. There are totally three authentication subsystems available in the proposed system, namely, Initial login authentication, Continuous authentication and Re-login authentication.

All the subsystems in the continuous biometric authentication system have three modules each and they are the acquisition module, the feature extraction module and the matching module. An interface exists between the matching module and the database enclosing the templates. In this approach, whenever a user logs in, an enrollment template is freshly registered. So, temporal details such as color in the user's wear can also be used as the enrollment template. Two main processes are carried out here, namely, the training and the testing. The modalities of the user are gained by means of the sensor and the database stores them during the training phase. On the other hand, the stored template is utilized to perform the matching procedure at the time of testing. The vital processes involved during the period of initial login authentication and continuous login authentication are depicted in Figure 2.

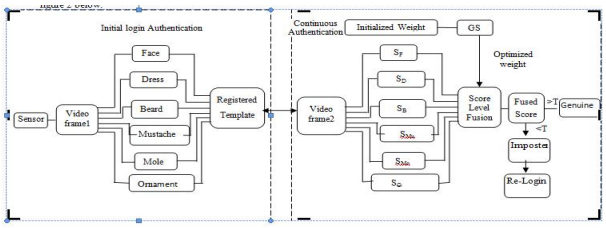


Figure 2: Initial and continuous authentication

4.1 Initial Login Authentication

The user employs the conventional authentication system for entering the system. Then, the sensor focuses the user's body for making the registration of the modalities like face, ornaments, color of clothing, mole, beard and mustache. During the period of training, the various poses of the user like turn head down, turn head to right, turn head to left, stretching the arms, quitting and leaning back in chair are caught due to the fact that the user may make movements or leave the spot. Training with these poses of the user can largely enhance the authentication system's accuracy.

4.2 Continuous Authentication

Mostly, the user templates are registered in a system only for particular time duration. In continuous authentication process, the template that is registered in the beginning and the second frame of the video are subjected to the matching process. Normalized cross correlation is utilized for deciding the likeness between the image and each one of the modalities.

4.3 Feature Matching Using Normalized Cross Correlation

The inspiration for employing cross correlation to handle template matching comes from the square Euclidean distance, which is given by,

$$D^2_{f,t}(u,v) = \sum_{x,y}[f(x,y) - t(x-u, y-v)]^2.$$

Where represents the image and the sum is over , subject to the window consisting of the feature located at. The expansion of is:

$$D^2_{f,t}(u,v) = \sum_{x,y}[f^2(x,y) - 2f(x,y)t(x-u,y-v) + t^2(x-u,y-v)]^2.$$

The expression $t^2(x-u, y-v)$ specifies a constant. If $f^2(x,y)$ is more or less constant, the rest of the cross-correlation terms will be:

$$c(u,v) = \sum_{x,y}[f(x,y)t(x-u,y-v)].$$

The above-mentioned equation offers the measure of how closely the image as well as the feature resemble. Few shortcomings are produced, when the above equation is employed for handling template matching. The first shortcoming is that the template matching with the above equation will not succeed, if the image energy $\sum f^2(x,y)$ alters with position. An example for this case is that the correlation existing among the feature and a precisely matching image area may be found to be smaller, when compared to the correlation between the feature and a bright region. In addition, the range of $c(u,v)$ relies on

the feature size. Further, the equation undergoes modifications with the variations in image amplitude, which are created due to the changes in illumination all throughout the image sequence. The aforementioned drawbacks can be tackled with the normalization of the image and feature vectors to unit length through the correlation coefficient, which in turn generates a correlation coefficient in the form of cosine.

$$\gamma(u,v) = \frac{\sum_{x,y}[f(x,y) - \bar{f}(u,v)t(x-u,y-v) - \bar{t}]}{\{\sum_{x,y}[f(x,y) - \bar{f}(u,v)]^2 \sum_{x,y}[t(x-u,y-v) - t]^2\}^{0.5}}.$$

Where, $\bar{t}$ indicates the mean of the feature and $\bar{f}(u,v)$ points to the mean of $f(x,y)$ that lie in the region below the feature. The equation stated above is termed as the normalized cross-correlation. At last, a similarity score for the image and every single modality is computed depending on the normalized cross correlation procedure. Assume that the continuous biometric authentication system makes use of NN modalities, $M_1, M_2, \cdots, M_N$ for authenticating a person. Further, let the similarity score yielded for each one of the modality be $S = S_1, S_2, \cdots, S_N$. Now, the weighted sum rule of the fused matching score F_S can be given as:

$$F_S = \sum_{i=1}^{n} W_i S_i.$$

Where W_i specify the weight allotted to M_i in the interval $[0, 1]$.

A weighting strategy that relies on Group Search Algorithm is being proposed here for accomplishing an enhancement in the performance of the score level fusion. The score weights of each and every feature are chosen in a random fashion and then, the GSO algorithm is exploited for optimizing the score weights with n number of iterations.

4.4 Group Search Optimization Algorithm

GSO is normally a population-dependent optimization algorithm with three constituent members, namely, the producer, the scrounger and the ranger. In this algorithm, a population containing arbitrary weights that lie in the interval between 0 and 1 is created at first. Each one of the individual residing in this population is known as the group. All these random weights will not be the best one. Hence, a fitness function that is applied on all the random weights is used to spot the best weight from the population. The member of the population holding the best fitness value will be the producer. The other members holding the best fitness values, but excluding the producer will be the scroungers. Finally, the rest of the members that are neither the producer nor the scrounger will be the rangers. The current position of every single member in the group of best weights is given by, $X_i^K \in R^n$ .The computation of the head angle, $\phi_i^K = (\phi_{i1}^K .....\phi_{in}^K) \in R^{n-1}$, and the head direction, $D_i^k \phi_i^K = (d_{i1}^K .....d_{in}^K) \in R^{n-1}$, is done with the help of polar to Cartesian coordinates transformation.

$$d_{i1}^k = \prod_{p-1}^{n-1} cos(\phi_{ip}^k) d_{ij}^k - sin(\phi_{i(j-1)}^k) \prod_{p-i}^{n-1} cos(\phi_{ip}^k) d_{in}^k - sin(\phi_{i(n-1)}^k).$$

As the subsequent action, the producer scans the field and this can be described in terms of the distance and the maximum pursuit angle. Here, θ_{max} stands for the maximum pursuit angle and l_{max} specify the maximum pursuit distance. During the k^{th} iteration, the producer does the scanning process in three directions and those directions are zero degree, left hand side hypercube and right hand side hypercube. In the direction of zero degree,

$$X_Z = X_p^k + r_1 l_{max} D_p^k(\phi_k).$$

During the right hand side hypercube direction,

$$X_r = X_p^k + r_1 l_{max} D_p^k(\phi^k + \frac{r_2 \theta_{max}}{2}).$$

At the time of left hand side hypercube direction,

$$X_1 = X_p^k + r_1 l_{max} D_p^k(\phi^k - \frac{r_2 \theta_{max}}{2}).$$

Where, r_1 denotes the normally distributed number and r_2 refers to the distributed random sequence lying in the interval between 0 and 1. Moreover, the producer makes the choice of the best point through the fitness value computation. The current position is deemed as the best position in situations, where the producer could not discover a best position than the present one. Else, the present point will be modified and the new angle will be formed with the expression stated below.

$$\phi^{k+1} = \phi^k + r_2 \alpha_{max}.$$

Where α_{max} indicates the maximum turning angle The angle will become as $\phi^{K+a} = \phi^k$ in cases where the producer fails to uncover a better resource than the current position, even when a^{th} iteration is completed. Then, the scrounging function takes place and the resultant will be the arbitrary selection of 80 % of the members from the remaining members. Random walk is employed for making a search of the distributed resources from the disperse operator. It forms a random head angle ϕ_i at K^{th} and selects a random distance as specified underneath. $l_i = a.r_1 lmax$ The last strategy in the GS algorithm is ranging, in which a movement to the new point is accomplished as given by the expression,

$$X_i^{K+1} = X_i^k + l_i D_i^K(\phi^{k+1}).$$

At the end, the best updated weights are achieved later to the completion of n number of iterations in the GSO algorithm, which has enabled the score level fusion as explained in Section 5.3.2.

4.5 Matching

Matching is conducted with a threshold, preset as T. An optimized weighting strategy was used in an earlier phase for yielding a fused score of all the features. The fundamental structure of the matching process, which works in accordance to the preset threshold, is shown in Figure 3.

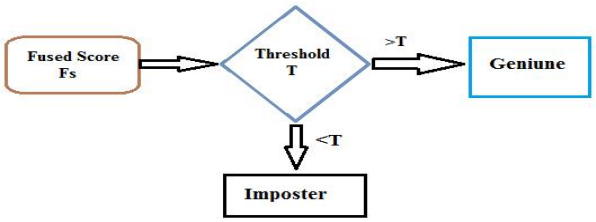


Figure 3: Matching process

The above figure states that a comparison is made between the fused modality score and the preset threshold. If the result of comparison is in such a way that the fused score exceeds the threshold level, the user is deemed as genuine. Else if the threshold is smaller than the fused score, the user is proved to be an imposter or a fake one. If a fake user is identified, our proposed methodology allows another process, known as Re-login authentication, to be carried out.

4.6 Authentication Using Modified PCA (MPCA)

In this phase, the face image in the initial template as well as the failed frame is applied with the modified PCA. Once MPCA is applied over the face image, the cross correlation is replaced by the Euclidean distance. Hence, MPCA only does the face authentication in continuous biometric system. If unsuccessful authentication occurs in any place of the authentication process, Re-login authentication is immediately conducted as the subsequent step in the proposed scheme.

4.7 MPCA Based Face Feature Extraction

The steps involved in MPCA are: (i) divide the face images into N number of sub-block images at an initial period and (ii) apply PCA to every single sub-block image using the local information pertaining to the face. When the process is started, the first sub-image of the image under consideration is compared against the entire number of images residing in the database. The images that satisfy a match with the first sub-image are alone chosen. Then, the second sub-image is compared against the set of images chosen in the previous step and the matched images are discovered. This procedure is repeated for all the sub-images and the recognized image will be the final outcome. If any of the sub-images is found to have got rid at an earlier stage, then the image is unrecognized. MPCA outweighs PCA by taking the changes in illumination, pose and facial expressions into account, in addition to offering improved results with larger accuracy. This recognition phase computes the weights W_k for both the training as well as the test frame. The computation of the difference in weights allows finding the Euclidean distance. To achieve recognition, a threshold has to be predetermined. The expressions in the images would be identical, if the threshold and the Euclidean distance have the same value. The weight W_k is computed in accordance to the following equation.

$$W_k = U_k(A_i - \varphi_i).$$

Where $U_k = \sum_{k=1}^{M} V_k \Phi_k$. Further, U_k denotes the Eigen faces, V_k points to the Eigen vectors and Φ_k represents the mean adjusted value. Re-login step will be performed at the condition, when the authentication ends up in failure in the proposed continuous biometric system.

5 Experimental Results

In this part we have presented the results of our proposed methodology and have scrutinized their appearance. The suggested multi-modal biometric authentication is executed in the MAT LAB program and the multi-modal biometric authentication is tested with the hard biometric (face) and soft biometrics (Ornaments, beard, mustache, dress color, mole) the result is contrasted with FAR and FRR values. The proposed authentication is implemented in a windows machine having configurations Intel (R) Core i5 processor, 1.6 GHz, 4 GB RAM, and the operation system platform is Microsoft Wnidow7 Professional. In Figure 1 the continuous authentication system setup is specified.

Figure 4: Continuous authentication system setup: Laptop with a webcam

5.1 Database Description

In our work, to evaluate the proposed continuous authentication scheme we collected videos of 10 subjects using the system shown in Figure 4. Every one user was asked to carry out the subsequent set of action while seated in front of the webcam. A few example screen shots are illustrated in Table 1.

- Scenario A: turning head to the left;
- Scenario B: turning head to the right;
- Scenario C: turning head down;
- Scenario D: straight to the chair;
- Scenario E: stretch arms;
- Scenario F: walk away.

Table 1: Example video frames used in experimentation

5.2 Evaluation Metrics

The effectiveness of proposed technique is analyzed by invoking some performance measures such as false rejection ratio (FRR), false accept ratio (FAR). The performance measures are explained below;

False rejection ratio: The system identifies imperfectly that a user is not in the cameras field of view although the user is yet in front of the camera. False discards lower the usability of the system.

False accept ratio: The system incorrectly identifies an imposter as the legitimate user. False admits lower the security of the system.

5.3 Performance Evaluation

The basic idea of our research is to continuously authenticate the subject in the online examination by means of soft and hard biometrics. To develop the authentication competence in our work we employ the MPCA (Modified Principal Component Analysis) with GSO. Niinuma et al. [13] have made cleared the incessantly validate the online examination by means of PCA and resemblance measures. We employ the MPCA with GSO algorithm to develop the competence. In Niinuma et al. [13] the facial recognition was performed by means of the PCA and soft biometric used were face colour and dress colour. However in our work the facial recognition is performed by means of MPCA and soft biometrics we are use (Ornaments, beard, mustache, dress color, mole). Both the hard biometric (face) and soft biometrics are fused with the assist of GSO algorithm based resemblance technique. The subsequent graph elucidated the presentation of the suggested approaches.

5.3.1 Performance of Continuous Authentication

In this section, we explain the performance of continuous systems using the Niinuma et al. [13] and proposed MPCA with GSO. The following graph demonstrates how our approach MPCA with GSO is effectively better then the Niinuma et al. [13].

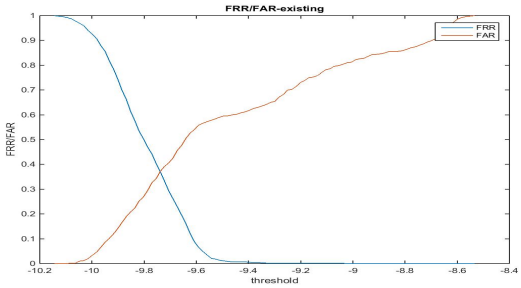


Figure 5: Performance of FAR and FRR for the continuous authentication using Niinuma et al. [13]

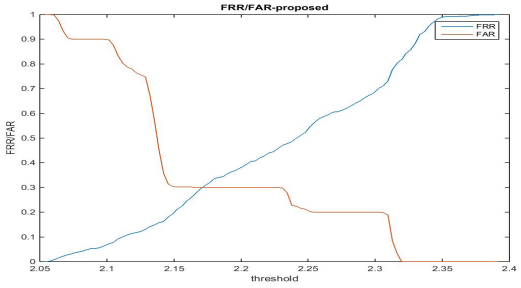


Figure 6: Performance of FAR and FRR for the continuous authentication using MPCA with GSO

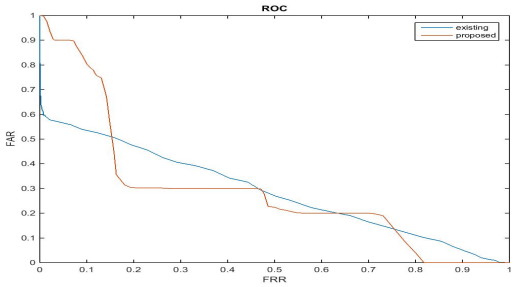


Figure 7: Performance of continuous authentication using ROC curve

Figures 5 and 6 illustrate the performance of the continuous authentication of Niinuma et al. [13] and proposed approach MPCA with GSO. When analyzing Figure 6, the approach achieves the minimum FRR and FAR of 0.3 but in Niinuma et al. [13] obtain the 0.37 which value is very much high compare to the proposed approach which

shows in Figure 5. When the system achieves the minimum FRR and FAR values the system achieve the maximum accuracy. In Figure 7 illustrate the performance of the continuous authentication using ROC curve. The approach Niinuma et al. [13] shows the resulted in an equal error rate (EER) of 0.49% and the proposed method of MPCA with GSO system using resulted in an EER of 0.28%, which is significantly better than the existing system Niinuma et al. [13].

5.3.2 Re-login Authentication

The user approaches to the re-login authentication, every time the system identifies that the user is no longer in front of the console. In this time, the system is bolted and it attempts to identify the user and re-authenticate him routinely. Now, the user is validated by means of both soft (colour histograms) and hard biometrics (face). The suggested re-login authentication method is assessed by means of video clips where an authorized user logs in, the user leaves the work environment (without logging out) and next, another user (an impostor) emerges in the field of view of the webcam. Figure 8 demonstrates this scenario. The system effectively identifies an impostor in Figure 8(c) and allows re-login to the first logged in user in Figure 8(e).

The colored ellipses in Figure 88(a) and (e) point out that the system properly identified the valid user in front of the console. At the same time, black-and-white images in Figure 8(b), (c), and (d) point out that the system properly recognized the absence of the legitimate user in front of the console.

Figure 8: Example results of re-login authentication experiments

Figures 9 and 10 show the re-login authentication of the online examination by means of Niinuma et al. [13] and suggested approach MPCA with GSO. When examining Figure 9, we attain the FAR and FRR rate is 0.65 which value is high. If the FAR and FRR values are high means the system can never get the higher competence. On the other hand, in Figure 10 we get the FRR and FAR value of 0.35 which value is very much low compare to the Niinuma et al. [13]. In our suggested work we employ the modified PCA and GSO algorithm for the system. The modified PCA employed to develop the efficiency of the

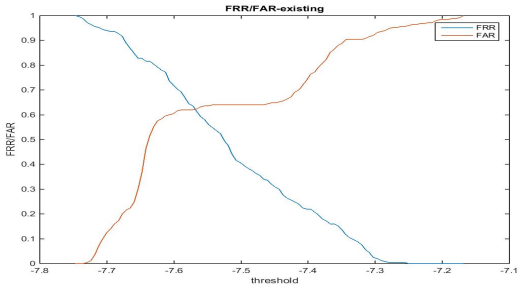


Figure 9: Performance of FAR and FRR for the re-login authentication using Niinuma et al. [13]

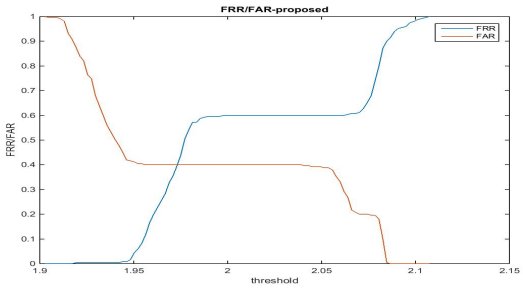


Figure 10: Performance of FAR and FRR for the Re-login authentication using MPCA with GSO

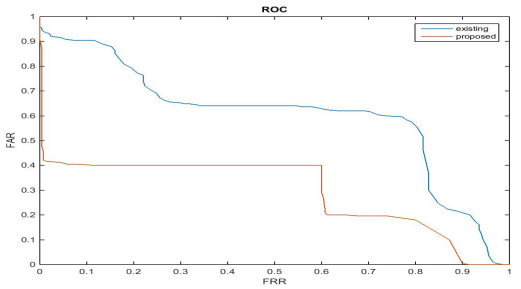


Figure 11: Performance of re-login authentication using ROC curve

hard biometric feature such as face. The presentation of the re-login authentication system is specified by the detection error rate (DET) curve exposed in Figure 11. The approach Niinuma et al. [13] demonstrates the resulted in an equal error rate (EER) of 0.62% and the suggested method of MPCA with GSO system by means of resulted in an EER of 0.40%, which is considerably better than the presented system Niinuma et al. [13].

6 Conclusion

We have proposed a new framework that uses both soft biometric traits and hard biometric traits for continuous user authentication. This framework registers a new en-

rollment template every time the user logs in, which enables the system to effectively use soft biometric traits for continuous authentication. The proposed system uses, face, dress colour, beard, mustache, and mole as biometric traits for continuous authentication. At a specified time interval, the initially registered template was matched with the next frame obtained through a sensor. Finally, for each biometric traits a matching score was generated based on the cross correlation. The generation matching scores were fused with the help of GSO based similarity technique. At any stage of mismatching, it requests to a re-login authentication stage. The experimental results of our proposed continuous biometric authentication system show better and improved authentication accuracy compared with the existing technique.

References

[1] Y. N. Chen, C. C. Han, C. T. Wang, K. C. Fan, "A novel scheme for face recognition and authentication against pose, illumination and expression changes," *Journal of Information Science and Engineering*, vol. 27, pp. 369–380, 2011.

[2] W. Fu Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016

[3] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE Transactions On Image Processing*, vol. 23, no. 2, pp. 710–724, 2014.

[4] A. K. Jain, S. C. Dass, and K. Nandakumar, "Can soft biometric traits assist user recognition?," in *Proceedings of SPIE*, LNCS 5404, pp. 561–572, Springer, 2004.

[5] A. K. Jain, S. C. Dass, and K. Nandakumar, "Soft biometric traits for personal recognition systems," in *Proceedings of the First International Conference on Biometric Authentication (ICBA'04)*, LNCS 3072, pp. 731–738, Springer, 2004.

[6] A. Jaiswal, N. Kumar, R. K. Agrawal, "Illumination invariant facial pose classification," *International Journal of Computer Applications*, vol. 37, no. 1, pp. 0975-8887, 2012.

[7] A. Kar, D. Bhattacharjee, D. K. Basu, M. Nasipuri, M. Kundu, "Face recognition using Hough peaks extracted from the significant blocks of the gradient image," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 1, Jan. 2012.

[8] E. Khourya, L. El Shafeya, C. McCoolb, M. Gnthera, S. Marcela, "Bi-modal biometric authentication on mobile phones in challenging conditions," *Journal of Image and Vision Computing*, vol. 32, no. 12, pp. 1147–1160, Dec. 2014.

[9] M. Leszczynski, "Image preprocessing for illumination invariant face verification," *Journal of Telecommunication and Information Technology*, vol. 4, pp. 19–25, 2010.

[10] C. C. Liu, D. Q. Dai and H. Yan, "Local discriminant wavelet packet coordinates for face recognition," *Journal of Machine Learning Research*, vol. 8, pp. 1165–1195, 2007.

[11] M. C. Mohan, V. V. Kumar and K. V. Subbaiah, "A new method of face recognition based on texture feature extraction on individual components of face," *International Journal of Signal and Image Processing*, vol. 1, no. 2, pp. 69–74, 2010.

[12] S. Muruganantham, "A comprehensive review of significant researches on face recognition based on various conditions," *International Journal of Computer Theory and Engineering*, vol. 4, no. 1, Feb. 2012.

[13] K. Niinuma, U. Park and A. K. Jain, "Soft biometric traits for continuous user authentication," *IEEE Transactions on Information Fo-rensics and Security*, vol. 5, no. 4, pp 771–780, Dec. 2010.

[14] P. Paysan, R. Knothe, B. Amberg, S. Romdhani and T. Vetter, "Face recognition using 3-D models: Pose and illumination," *Proceedings of IEEE*, vol. 94, no. 11, pp. 1977–1999, 2009.

[15] A. Prakash, "A biometric approach for continuous user authentication by fusing hard and soft traits," *International Journal of Network Security*, vol. 16, no. 1, pp. 65–70, 2014.

[16] R. Rathi, M. Choudhary, B. Chandra, "An application of face recognition system using image processing and neural networks," *International Journal of Computer, Technology and Applications*, vol. 3, no. 1, pp. 45–49, 2012.

[17] A. Ross and A. K. Jain, "Multimodal Biometrics: An Overview," in *Proceedings of 12th European Signal Processing Conference (EUSIPCO'04)*, pp. 1221–1224, Sept. 2004.

[18] A. Ross and A. K. Jain, "Information fusion in biometrics," in *Proceedings of AVBPA*, pp. 354–359, Halmstad, Sweden, June 2001.

[19] J. Shermina and V. Vasudevan, "An efficient face recognition system based on the hybridization of invariant pose and illumination process," *European Journal of Scientific Research*, vol. 64, no. 2, pp. 225–243, 2011.

[20] J. R. Sun, M. L. Shih, M. S. Hwang, "A survey of digital evidences forensic and cybercrime investigation procedure," *International Journal of Network Security*, vol. 17, no. 5, pp. 497–509, 2015

A. Prakash is working as Assistant Professor at Jerusalem College of Engineering, Chennai. He has received B.E and M.E degree in Computer Science and Engineering. He is currently pursuing Ph.D at Hindustan Institute of Technology and Science. His areas of research interests include Network Security and Image Processing.

R. Dhanalakshmi a Ph.D holder from College of Engg.,

Guindy Anna University Chennai for the research activities in Information Security and Networking. She holds a B.E in Computer Science from Bharathidasan University and M.Tech in Advanced Computing from SASTRA University. She has vital research experience serving as a research Associate in the NTRO Sponsored Project Collaborated directed basic research on Smart and Secure Environment at Anna University under the consortium of IIT Madras. To her credit, she has nearly 25 research papers in International Conferencess and International Journals including Elsevier, Springer, IFIP and IGI Global. Her fields of interest include Information Security, Data Mining, Knowledge and Semantic Networks, Intelligent Networks and Mobile Computing.

A Provably Password Authenticated Key Exchange Scheme Based on Chaotic Maps in Different Realm

Hongfeng Zhu, Yifeng Zhang, and Yan Zhang
(Corresponding author: Hongfeng Zhu)

Software College, Shenyang Normal University
No. 253, HuangHe Bei Street, HuangGu District, Shenyang 110034, China
(Email:zhuhongfeng1978@163.com, {1548452125, 1505733680}@qq.com)
(Received Dec. 6, 2014; revised and accepted Jan. 16 & Mar. 12, 2015)

Abstract

Until now, the overwhelming majority of password-authenticated key agreement protocols using chaotic maps are based on three architectures (client/server, two clients/server and multi-server) and four security models (heuristic security, random oracle, ideal cipher and standard model). However, with rapid changes in the modern communication environment such as wireless mesh networks and cloud storing, it is necessary to put forward a kind more flexible and general architecture to adapt it. So, in our paper, we firstly propose a provable secure two-party in two-realm key agreement protocol using chaotic maps in the standard model. Our proposed protocol is more general and it is easy to expand to many other forms, such as three-party or N-party in different realms. The new protocol resists dictionary attacks mounted by either passive or active network intruders, allowing, in principle, even weak password phrases to be used safely. It also offers perfect forward secrecy, which protects past sessions and passwords against future compromises. Finally, we give the security proof in the standard model and the efficiency analysis of our proposed scheme.

Keywords: Chaotic maps, different realms, key exchange, mutual authentication

1 Introduction

Nowadays, chaos theory has widely used to cryptography. Chaotic system has numerous advantages, such as extremely sensitive to initial parameters, unpredictability, boundness, etc. Meanwhile, chaotic sequence generated by chaotic system has the properties of non-periodicity and pseudo-randomness. In a word, chaos theory and chaotic system have exploited a new way for cryptography.

In 1998, Baptista [1] firstly connects cryptography with chaos theory. As a fundamental cryptographic primitive, key agreement protocol allows two or more parties to agree on shared keys which will be used to protect their later communication. Then, combining chaos theory and key agreement primitive, many authenticated key exchange (AKE) protocols [7, 8, 12, 16, 21, 23, 24, 25] have been proposed. The literature [25] firstly proposed a new one-way authenticated key agreement scheme (OWAKE) based on chaotic maps with multi-server architecture. The OWAKE scheme is widely used to no need for mutual authentication environment on Internet, such as readers-to-journalists model and patient-to-expert model. Using the chaotic maps, the literature [24] firstly proposed a new multiple servers to server architecture (MSTSA) to solve the problems caused by centralized architecture, such as multi-server architecture with the registration center (RC). The core ideas of the proposed scheme are the symmetry (or called peer to peer) in the servers side and the transparency for the clients side. In brief, based on chaotic maps, there were many AKE protocols from functionality aspect, or from efficiency aspect, or from security aspect, or from architecture aspect to improve the AKE protocols.

However it is quite unrealistic that two clients trying to communicate with each other are registered on the same server. In the real situation with distributed applications, an authentication setting usually occurs such that two clients are registered in different servers. For example, from a user's point of view in a mobile computing environment, a secure end-to-end channel between one mobile user in cell A and another user in cell B may be a primary concern. Additionally, the end-to-end security service minimizes the interferences from the operator controlled network components. Over the past years, many protocols based on the different password authentication (DPWA) model have been presented in the cross-realm setting and some of them have been easily broken and subsequently modified [2, 5, 9, 13, 15]. Byun et al. first pro-

posed a Client-to-Client Password-Authenticated Key Exchange (C2C-PAKE) in the cross-realm setting where two clients are in two different realms and hence two servers involved [2]. Unfortunately, the scheme was found to be flawed. Chen first pointed out that one malicious server in the cross-realm setting could mount a dictionary attack to obtain the password of a client who belongs to the other realm [5]. In [15], Wang et al. showed dictionary attacks by a malicious server on the same protocol. Kim et al. [9] pointed out that the protocol was susceptible to Dening-Sacco attacks [6], and they also proposed an improved C2C-PAKE protocol. However, very recently, Phan and Goi suggested two unknown key share attacks on the improved C2C-PAKE protocol. They presented countermeasures in [13]. Up until now, several countermeasures to protect the attacks on the C2C-PAKE protocol have been presented in [2, 5, 9, 13, 15]. Recently Byun [3] presented an efficient C2C-PAKE protocol and proved it is secure under decisional Diffie-Hellman assumption in the ideal cipher and random oracle models. But most of the presented protocols were susceptible to Off-line Password Guessing Attacks with Server Compromise. The main reason [17, 22] is that there is a need for the password to encrypt or decrypt some information during the protocol process. This implies that the server has to store the plaintext password. So the password verification information in the server obtained by the attacker may mount an Off-line Password Guessing Attacks.

Based on the chaotic maps, we believe the more general architecture should be involved in AKE protocols. So we propose the first two-party in two-realm key exchange protocol using chaotic maps in standard model.

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. Next, a novel chaotic maps problem is described in Section 3. Then, the non-interactive twin chaotic maps-key exchange protocol is given in Section 4. The Security of our proposed protocol is given in Section 5. The efficiency analysis of our proposed protocol and some feasible applications are given in Section 6. This paper is finally concluded in Section 7.

2 Preliminaries

2.1 One-way Hash Function and Pseudo-random Function Ensembles

There are four main properties in a secure cryptographic one-way hash function $h : a \to b$:

1) The function h takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output;

2) The function h is one-way in the sense that given a, it is easy to compute $h(a) = b$. However, given b, it is hard to compute $h^{-1}(b) = a$;

3) Given a, it is computationally infeasible to find a' such that $a' \neq a$, but $h(a') = h(a)$;

4) It is computationally infeasible to find any pair a, a' such that $a' \neq a$, but $h(a') = h(a)$.

Pseudo-random function ensembles:
If a function ensemble $F = \{F_n\}_{n\in N}$ is pseudo-random [14], then for every probabilistic polynomial oracle $\mathcal{A}$ and all large enough n, we have that:

$$\mathcal{A}^{G_n}(1^n) = 1]| < \varepsilon(n)$$

where $G = \{G_n\}_{n\in N}$ is a uniformly distributed function ensemble, $\varepsilon(n)$ is a negligible function, $Adv^F = \max_{\mathcal{A}}\{Adv^F(\mathcal{A})\}$ denotes all oracle $\mathcal{A}$,and $Adv^F(\mathcal{A})$ represents the accessible maximum.

2.2 Symmetric Encryption

A symmetric encryption scheme $E_k(Kgen, E, D)$ consists of three algorithms as follows:

1) Randomized Key Generation Algorithm $Kgen$: it returns a key k drawn from the key space $Keys(E_k)$ at random.

2) Encryption Algorithm E: it takes the key $k \in Keys(E_k)$ and a plaintext $M \in \{0,1\}^*$ as the inputs and outputs a ciphertext $C \in \{0,1\}^*$. So it can be written $C = E_k(M)$.

3) Decryption Algorithm D:it takes the key $k \in Keys(E_k)$ and a ciphertext $C \in \{0,1\}^*$ as the inputs and outputs a plaintext $M \in \{0,1\}^*$. So it can be written $M = D_k(C)$.

2.3 Definition and Hard Problems of Chebyshev Chaotic Maps

Let n be an integer and let x be a variable with the interval $[-1, 1]$. The Chebyshev polynomial $T_n(x)$: $[-1, 1] \to [-1, 1]$ is defined as $T_n(x) = \cos(ncos^{-1}(x))$ [16]. Chebyshev polynomial map T_n: $R \to R$ of degree n is defined using the following recurrent relation:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x),$$

where $n \geq 2, T_0(x) = 1$, and $T_1(x) = x$. The first few Chebyshev polynomials are:

$$\begin{aligned} T_2(x) &= 2x^2 - 1, \\ T_3(x) &= 4x^3 - 3x, \\ T_4(x) &= 8x^4 - 8x^2 + 1, \\ \cdots &\quad \cdots \end{aligned}$$

One of the most important properties is that Chebyshev polynomials are the so-called semi-group property which establishes that

$$T_r(T_s(x)) = T_{rs}(x).$$

An immediate consequence of this property is that Chebyshev polynomials commute under composition

$$T_r(T_s(x)) = T_s(T_r(x)).$$

In order to enhance the security, Zhang [21] proved that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$. The enhanced Chebyshev polynomials are used in the proposed protocol:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) (\mathrm{mod} N)$$

where $n \geq 2$, $x \in (-\infty, +\infty)$, and N is a large prime number. Obviously,

$$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x)).$$

Definition 1. *(Semi-group property) Semi-group property of Chebyshev polynomials:*

$$\begin{aligned} T_{rs}(x) &= T_r(T_s(x)) \\ &= \cos(r\cos^{-1}(s\cos^{-1}(x))) \\ &= \cos(rs\cos^{-1}(x)) \\ &= T_s(T_r(x)) \\ &= T_{sr}(x), \end{aligned}$$

where r and s are positive integer and $x \in [-1, 1]$.

Definition 2. *(Chaotic Maps-Based Discrete Logarithm (CDL) problem) Given x and y, it is intractable to find the integer s, such that $T_s(x) = y$. The probability that a polynomial time-bounded algorithm $\mathcal{A}$ can solve the CDL problem is defined as $Adv_{\mathcal{A}}^{CDL}(p) = \Pr[\mathcal{A}(x, y) = r : r \in Z_p^*, y = T_r(x) \bmod p]$.*

Definition 3. *(CDL assumption) For any probabilistic polynomial time-bounded algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{CDL}$ $(p)$is negligible, that is, $Adv_{\mathcal{A}}^{CDL}(p) \leq \varepsilon$, for some negligible function ε.*

Definition 4. *(Chaotic Maps-Based Diffie-Hellman (CDH) problem) Given x, $T_r(x)$ and $T_s(x)$, it is intractable to find $T_{rs}(x)$. The probability that a polynomial time-bounded algorithm $\mathcal{A}$ can solve the CDH problem is defined as $Adv_{\mathcal{A}}^{CDH}(p) = \Pr[\mathcal{A}(x, T_r(x) \bmod p, T_s(x) \bmod p) = T_{rs}(x) \bmod p : r, s \in Z_p^*]$.*

Definition 5. *(CDH assumption) For any probabilistic polynomial time-bounded algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{CDH}(p)$ is negligible, that is, $Adv_{\mathcal{A}}^{CDH}(p) \leq \varepsilon$, for some negligible function ε.*

2.4 Definition and Properties of Chebyshev Chaotic Maps

Definition 6. *[7, 8] $f : J \to J$ is said to be topologically transitive if for any pair of open sets $U, V \subset J$, there exists $k > 0$ such that $f^k(U) \cap V \neq \phi$.*

Definition 7. *$f : J \to J$ has sensitive dependence on initial conditions if there exists $\delta > 0$ such that for any $x \in J$ and any neighborhood N of x, there exist $y \in N$ and $n \geq 0$ such that $|f^n(x) - f^n(y)| > \delta$.*

Definition 8. *Let V be a set, then $f : V \to V$ is said to be chaotic on V if*

1) f has sensitive dependence on initial conditions.

2) f s topologically transitive.

3) Periodic points are dense in V.

Definition 9. *Let $f : A \to A$, $f : B \to B$ be two maps, if there exists a continuous surjection $h : A \to B$ such that $h \cdot g = g \cdot h$, we say that these two maps f and g are topologically semi-conjugate.*

Theorem 1. *A non-zero polynomial is the n^{th} Chebyshev polynomial or its constant times iff the nonzero polynomial is the root of the differential equation*

$$\left(1 - x^2\right) y'' - xy' + n^2 y = 0 \, (n \in \mathrm{Z}_+).$$

Lemma 1. *If $f : A \to A$, $f : B \to B$ are topologically semi-conjugate,*

1) When p is the periodic point of f, then $h(p)$ is the periodic point of g;

2) When the periodic point of f is dense in A, the periodic point of g is dense in B, where h is the topologically semi-conjugate between f and g.

Lemma 2. *Assume $f : A \to B$ is a map, $A_0, A_1 \subset A$, then $f(A_0 \cap A_1) \subset f(A_0) \cap f(A_1)$.*

Lemma 3. *When $f : A \to A$ is topologically transitive, $g : B \to B$ is topologically semi-conjugate f via h, then g is topologically transitive.*

Lemma 4. *Let $R : S' \to S'$ be a map of the circle into itself, then $R(\theta) = n\theta \, (n \in \mathrm{Z}, n \geq 2)$ is chaotic, where θ is the radian value.*

The concrete proof of chaotic properties can be found in the literature [8] and the enhanced properties of Chebyshev polynomials that defined on interval $(-\infty, +\infty)$ still have the semi-group property (see [21]).

3 The Proposed Protocol

In this section, under the two-realm environment for two client with two servers, a chaotic maps-based authentication key agreement scheme is proposed which consists of three phases: registration phase, authentication key agreement phase and password update phase.

3.1 Notations

In this section, any server i has its identity ID_{S_i} and public key $(x, T_{K_i}(x))$ and a secret key K_i based on Chebyshev chaotic maps, a secure one-way hash function $H(\cdot)$, a pseudo-random function F,and a pair of secure symmetric encryption/decryption functions $E_K()/D_K()$ with key K. The concrete notations used hereafter are shown in Table1.

Table 1: Notations

Symbol	Definition
ID_A, ID_B, $ID_{Session}$	The identity of Alice, Bob and the session, respectively;
S_i, ID_{S_i}	The i^{th} server; The identity of the i^{th} server, respectively;
$a, b, S_a, S_b, S_{aa}, S_{bb}$	Nonces;
$(x, T_k(x))$	Public key based on Chebyshev chaotic maps;
K	Secret key based on Chebyshev chaotic maps;
$E_k(\cdot)/D_k(\cdot)$	A pair of secure symmetric encryption/decryption functions with the key K;
H	A secure one-way hash function;
F	Pseudo-random function;
$\|\|$	Concatenation operation.

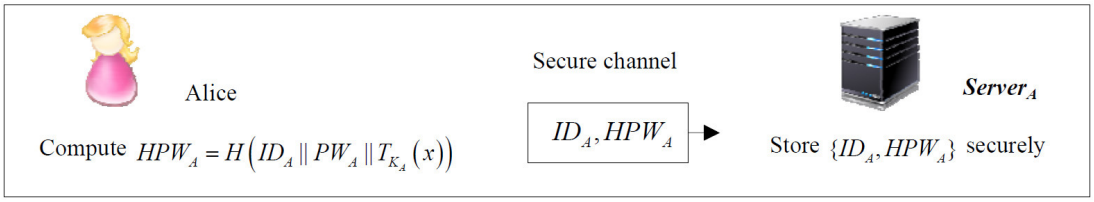


Figure 1: A authenticated expert registration phase

3.2 Registration Phase

Concerning the fact that the proposed scheme mainly relies on the design of Chebyshev chaotic maps-based in two-realm architecture, it is assumed that Alice can register at the serverA in the same realm by secure channel. The same assumption can be set up for servers. Figure 1 illustrates the server registration phase.

Step 1. When a user Alice wants to be a new legal user, she chooses her identity ID_A and password PW_A and sends $\{ID_A, HPW_A\}$ to the server via a secure channel.

Step 2. Upon receiving $\{ID_A, HPW_A\}$ from the Alice, the server A stores $\{ID_A, HPW_A\}$ in a secure way.

3.3 Authenticated Key Agreement Phase

This concrete process is presented in Figure 2.

Step 1. If Alice wishes to consult some personal issues establish with Bob in a secure way, but they are in different realm. Alice will choose a large and random a. Then the device of Alice will compute $T_a(x)$, $C_{A_1} = T_a(x)T_{HPW_A}T_{K_A}(x)$ and $Mac_{AS} = F_{T_aT_{K_A}(x)}(ID_{Session}||C_{A_1})$. After that, Alice sends $ID_A, ID_B, C_{A_1}, Mac_{AS}$ to $\mathbf{Server}_A$ where she registers on (The same way for Bob).

Step 2. After receiving the message ID_A, ID_B, C_{A_1}, Mac_{AS} from Alice, $\mathbf{Server}_A$ will do the following tasks:

1) $\mathbf{Server}_A$ uses HPW_A to compute $T_a(x) = C_{A_1}/T_{HPW_A}T_{K_A}(x)$.

2) $\mathbf{Server}_A$ examines whether is valid in terms of the $(ID_{Session}||C_{A_1})$.

3) $\mathbf{Server}_A$ selects a large and random integer S_a to compute $T_{S_a}(x)$, $C_{A_2} = T_a(x)T_{S_a}T_{K_B}(x)$, $Mac_{SAB} = F_{T_aT_{K_B}(x)}(ID_{Session}||C_{A_2})$ and sends $ID_A, ID_B, C_{A_2}, T_{S_a}(x), Mac_{SAB}$ to $\mathbf{Server}_B$ (The same way for $\mathbf{Server}_B$).

Step 3. After receiving the message ID_A, ID_B, C_{A_2}, $T_{S_a}(x)$, Mac_{SAB} from $\mathbf{Server}_A$, $\mathbf{Server}_B$ will uses K_B to compute $T_a(x) = C_{A_2}/T_{S_a}T_{K_B}(x) = C_{A_2}/T_{K_B}T_{S_a}(x)$. Then $\mathbf{Server}_B$ examines whether $Mac_{SAB} = F_{T_aT_{K_B}(x)}(ID_{Session}||C_{A_2})$ is valid in terms of the $(ID_{Session}||C_{A_2})$. $\mathbf{Server}_B$ selects a large and random integer S_{bb} and computes $T_{S_{bb}}(x)$, $C_{A_3} = T_{S_{bb}}T_{HPW_B}T_a(x)$, $Mac_{SB} = F_{T_aT_b(x)}(ID_{Session}||C_{A_3})$ and sends $ID_A, ID_B, C_{A_3}, T_{S_{bb}}(x), Mac_{SB}$ to Bob (The same way for $\mathbf{Server}_A$).

Step 4. After receiving the message ID_A, ID_B, C_{A_3}, $T_{S_{bb}}(x)$, Mac_{SB}, Bob uses HPW_B to compute

$$\begin{aligned} T_a(x) &= C_{A_3}/T_{S_{bb}}T_{HPW_B}(x) \\ &= C_{A_3}/T_{HPW_B}T_{S_{bb}}(x). \end{aligned}$$

Then Bob examines whether $Mac_{SB} = F_{T_{HPW_B}T_{S_{bb}}}(ID_{Session}||C_{A_3})$ is valid in terms of the $(ID_{Session}||C_{A_3})$. If holds, and the session key is $SK = F_{T_bT_a(x)}(1)$.(The same way for Alice). If any authenticated process does not pass, the protocol will be terminated immediately.

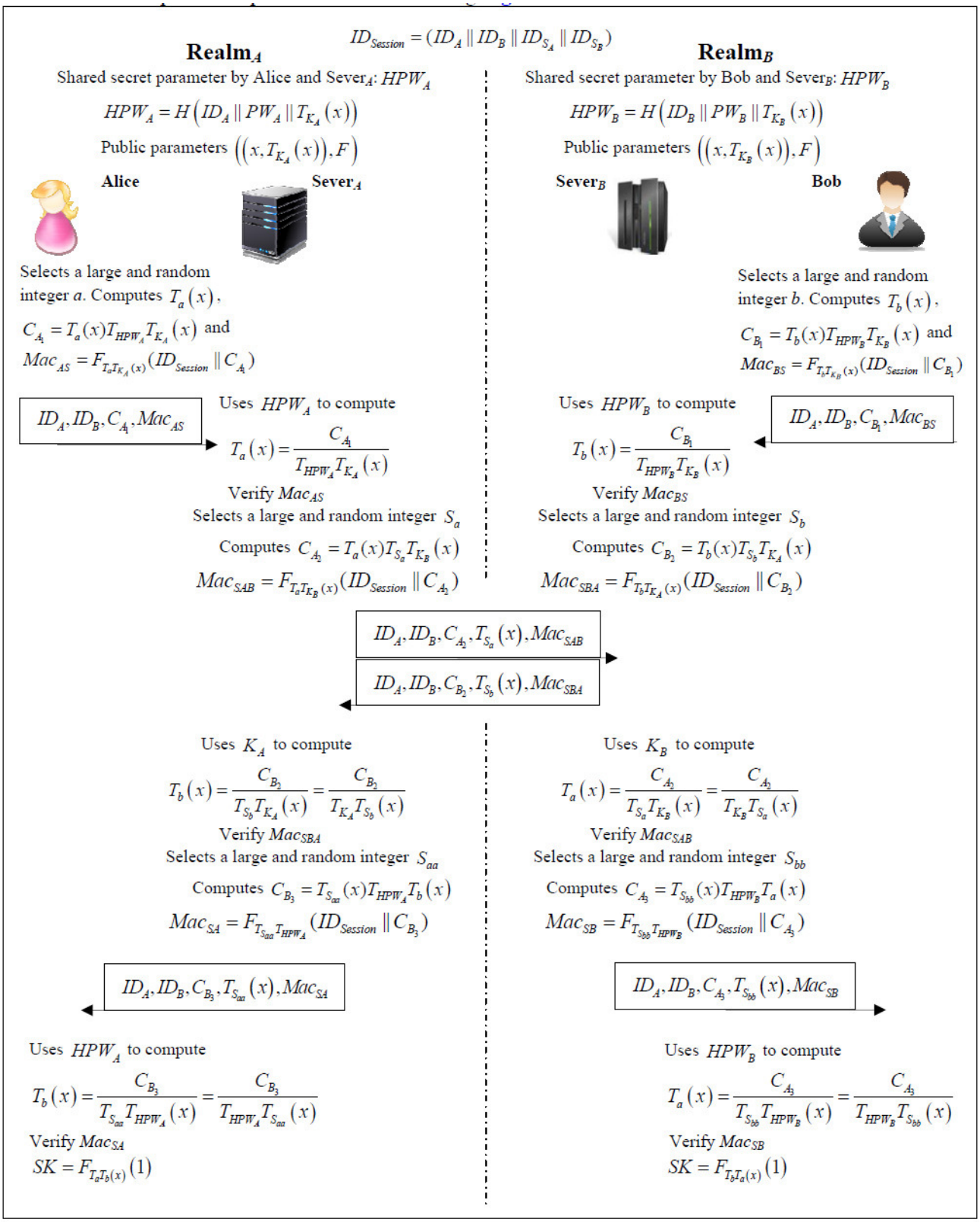


Figure 2: Authenticated key agreement phase

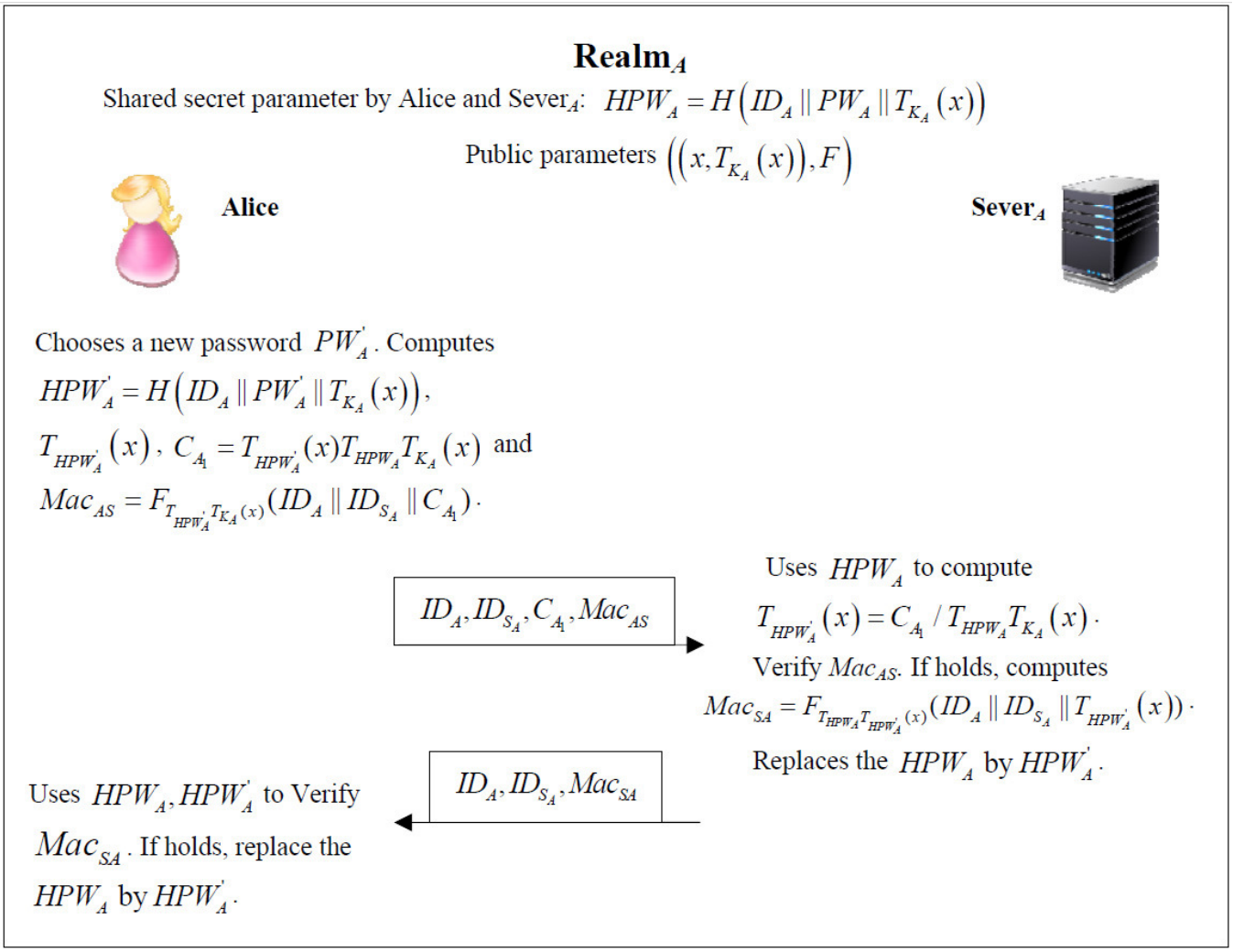


Figure 3: Password update phase

3.4 Password Update Phase

This concrete process is presented in the following Figure 3.

Step 1. If Alice wishes to update her password with $\mathbf{Server}_A$, Alice will choose a new memorable password $PW_A^{'}$. Then the device of Alice will compute $HPW_A^{'} = H\left(ID_A||PW_A^{'}||T_{K_A}(x)\right)$, $T_{HPW_A^{'}}(x)$, $C_{A_1} = T_{HPW_A^{'}}(x)T_{HPW_A}T_{K_A}(x)$ and $Mac_{AS} = F_{T_{HPW_A^{'}}T_{K_A}(x)}(ID_A||ID_{S_A}||C_{A_1})$. After that, Alice sends ID_A, ID_{S_A}, C_{A_1}, Mac_{AS} to $\mathbf{Server}_A$ where she registers on.

Step 2. After receiving the message ID_A, ID_{S_A}, C_{A_1}, Mac_{AS} from Alice, $\mathbf{Server}_A$ will do the following tasks:

1) $\mathbf{Server}_A$ uses HPW_A to compute $T_{HPW_A^{'}}(x) = C_{A_1}/T_{HPW_A}T_{K_A}(x)$.
2) $\mathbf{Server}_A$ examines whether $Mac_{AS} = F_{T_{HPW_A^{'}}T_{K_A}(x)}(ID_A||ID_{S_A}||C_{A_1})$ is valid in terms of the $(ID_A||ID_{S_A}||C_{A_1})$.
3) If holds, $\mathbf{Server}_A$ computes $Mac_{SA} = F_{T_{HPW_A}T_{HPW_A^{'}}(x)}(ID_A||ID_{S_A}||T_a(x))$ and sends ID_A, ID_{S_A}, Mac_{SA} to Alice. Replaces the $HPW_A$by$HPW_A^{'}$.

Step 3. After receiving the message ID_A, ID_{S_A}, Mac_{SA} from $\mathbf{Server}_A$, Alice will uses HPW_A, $HPW_A^{'}$ to compute $Mac_{SA}^{'} = F_{T_{HPW_A}T_{HPW_A^{'}}(x)}(ID_A||ID_{S_A}||T_{HPW_A^{'}}(x))$ to verify Mac_{SA}. If holds, Alice replaces the $HPW_A$by$HPW_A^{'}$.

4 Security Consideration

The section a theorem concerning the semantic security of our proposed protocol is given.

4.1 Security Model

We recall the protocol syntax and communication model [4, 11, 19]. The basic descriptions and some queries are shown in Table 2.

4.2 Security Proof

Theorem 2. *Let Γ be a two-party in two-realm PAKE protocol described in Figure 2. Let $F: \{0,1\}^n \to \{0,1\}^{l(n)}$ be a pseudo-random function ensembles. Because the DDH assumption holds in enhanced Chebyshev chaotic maps, then*

$$Adv_{x,T_u,F}^{2P2RPAKE}(t,R) \leq \frac{2q_e^2 + 3q_s^2 + 2(q_e+q_s)^2}{N_1}$$
$$+2(q_e+q_s)Adv^F + 2(\min\{q_e,q_r\} + \min\{q_s,q_r\})Adv^F$$
$$+2(q_e+q_s)Adv_{x,T_u}^{DDH} + \frac{q_s}{2^{n-1}} + \frac{(q_e+q_s)^2}{N_1}\frac{q_s}{N}$$

where n is a safe parameter, $l(\cdot)$ is a function that can be computed in polynomial time. N_1 is a large prime number, $u, T_u(x)$ are the private and public keys of the server, q_e, q_r, q_s represent the maximum number of Execute and Test that the adversary can inquire, and queries from Send-Client and Send-Server, N is the password dictionary D's size, Adv_{x,T_u}^{DDH} represents the probability of breaking the DDH hypothesis, and Adv^F denotes the probability of breaking the pseudo-random function ensembles.

In order to make the security proof simple, we firstly point out the differences between the literature [19] and our proposed protocol. Then we give the differences between the literature [11] and our proposed protocol. Finally, we will get Theorem 2.

1) The differences between the literature [19] and our proposed protocol. Using enhanced Chebyshev chaotic maps to replace ElGamal encryption. To be specific, $g^{x_2}, rg^{x_1}, Zg^{x_1}$ and $g^{x_1}h^{x_2}$ in the literature [19] should be replaced by $T_{x_2}(x), rT_{x_1}(x), ZT_{x_1}(x)$ and $T_{x_1}(x)T_{x_2}(h)$, respectively.

   The birthday paradox should be used to replace the probability of random events when the event collision occurs. According to the birthday paradox, the probability of collisions in output $T_n(x)$ is at most $q_s^2/2N_1$,where q_s denotes the maximum number of Send-Client and Send-Server queries.

   According to the birthday paradox, the probability of collisions in output $T_n(x)$ is at most $(q_s+q_e)^2/2N_1$,where q_s denotes the maximum number of Send-Client and Send-Server queries, q_e denotes the maximum number of Execute queries. Hence, the probability of distinguishing Mac_{**} with random integers is $(q_s+q_e)^2/2N_1$.

2) The differences between the literature [11] and our proposed protocol. We convert the low entropy secret password PW to high entropy cryptography key by a one-way hash function $HPW_A = H(ID_A||PW_A||T_{K_A}(x))$ which is more secure way than the literature [11] only stored password in the server database.

Different architecture. Our proposed protocol sets up in different realm and the two-party has different password with his/her service server. That means one Send-Client query will test two passwords in the same set. So in our protocol, when relating with N (N is the password dictionary D size), and it is the same with the literature [11].

Round 1. Our proposed protocol has one more Mac_{**} for each party, so there is must have one more $(q_s+q_e)^2/2N_1$.

Table 2: Descriptions the model and the queries

Symbol	Definition
Parties P_1, $\cdots$, P_n or (C_1, $\cdots$, C_n, S_1, $\cdots$, S_n)	Modelled by probabilistic Turing machines. Two non-empty sets: User, the set of all clients, and Server, the set of trusted servers constitute the participants in our 2P2RPAKE protocol.
Adversary Λ	A probabilistic Turing machine which controls all communication, with the exception that the adversary cannot inject or modify messages (except for messages from corrupted parties or sessions), and any message may be delivered at most once.
Sessions matching	If the outgoing messages of one are the incoming messages of the other.
$\prod_{U_1}^{i}$, $pid_{U_1}^{i}$, $sid_{U_1}^{i}$, $\prod_{U_2}^{j}$, $pid_{U_2}^{j}$, $sid_{U_2}^{j}$	Denote participant U_1's instance i, who is involved with a partner participant U_2 in a session. $\prod_{U_1}^{i}$ has the parner identification $pid_{U_1}^{i}$ and the session identification $sid_{U_1}^{i}$. The same means for $\prod_{U_2}^{j}$, $pid_{U_2}^{j}$, $sid_{U_2}^{j}$.
Execute ($\prod_{U_1}^{i}$, S^i, S_j, $\prod_{U_2}^{j}$)	This query returns the messages that were communicated in the course of an honest execution of the protocol among $\prod_{U_1}^{i}$, S^i, S_j, $\prod_{U_2}^{j}$.
Send-Client ($\prod_{U_1}^{i}$ ($k = 1, 2$), m)	This query returns the message that client instance $\prod_{U_k}^{i}$, which would generate upon receipt of message m.
Send-Server (S^k ($k = 1, 2$), m)	This query returns the message that server instance S^k would generate upon receipt of message m. When receiving a fabricated message by an adversary, the server instance S^k responds in the manner prescribed by the protocol.
Corrupt (U_k ($k = 1, 2$))	This query returns the session key of the client instance U_k ($k = 1, 2$).
Reveal ($\prod_{U_k}^{i}$ ($k = 1, 2$))	This query returns the password and the states of all instances of $U_k (k = 1, 2)$ only when it is defined.
Test ($\prod_{U_k}^{i}$ ($k = 1, 2$))	This query allows the adversary to be issued at any stage to a completed, fresh, unexpired session. A bit b is then picked randomly. If $b = 0$, the test oracle reveals the session key, and if $b = 1$, it generates a random value in the key space. The adversary Λ can then continue to issue queries as desired, with the exception that it cannot expose the test session.
Partnering	We say two instances $\prod_{U_1}^{i}$ and $\prod_{U_2}^{j}$ are partners iff: (a) They are successfully accepted; (b) $sid_{U_1}^{i} = sid_{U_2}^{j}$; (c) pid for $\prod_{U_1}^{i}$ is $\prod_{U_2}^{j}$ and vice versa; (d) No instance other than $\prod_{U_1}^{i}$ and $\prod_{U_2}^{j}$ accepts with a pid equal to $\prod_{U_1}^{i}$ or $\prod_{U_2}^{j}$.
Freshness	Let $\prod_{U_1,U_2,S_1,S_2}^{i}$ be a completed session by a party U_1 with some other party U_2, and $\prod_{U_2,U_1,S_2,S_1}^{j}$ be the matching session to $\prod_{U_1,U_2,S_1,S_2}^{i}$. We say that the session $\prod_{U_1,U_2,S_1,S_2}^{i}$ is fresh if U_1 and U_2 in session $\prod_{U_1,U_2,S_1,S_2}^{i}$ and the matching session $\prod_{U_2,U_1,S_2,S_1}^{j}$ are honest and the following conditions hold: (a) $\prod_{U_1,U_2,S_1,S_2}^{i}$ has accepted the request to establish a session key. (b) $\prod_{U_1,U_2,S_1,S_2}^{i}$ has not been revealed. (c) No matching conversation $\prod_{U_2,U_1,S_2,S_1}^{j}$ of $\prod_{U_1,U_2,S_1,S_2}^{i}$ has been revealed. (d) U_2, S has not been corrupted. (e) The adversary asks neither Send-Client $(\prod_{U_1}^{i}, m)$ nor Send-Client $(\prod_{U_2}^{j}, m)$ query.

Table 3: Security comparison existing protocols for 3PAKE based on Chebyshev chaotic maps and our protocol

	Model	KP	MA	AR	FS	UDOD	UKS	PCI	OFD
Our protocol	S	Yes	Yes	C2S2	Yes	Yes	Yes	Yes	Yes
Yang and Cao's protocol [19]	S	Yes	Yes	C2S	Yes	Yes	Yes	Yes	Yes
Lai et al.'s protocol [11]	S	Yes	Yes	C2S	Yes	Yes	Yes	Yes	Yes
Yoon-Jeon's protocol [20]	N	No	Yes	C2S	No	No	Yes	No	No
Xie et al.'s protocol [18]	N	Yes	Yes	C2S	Yes	Yes	Yes	No	No
Lee et al.'s protocol [12]	N	Yes	Yes	C2S	No	No	Yes	Yes	No

S standard model, N nonstandard model, KP key privacy, MA mutual authentication, AR architecture, C2S client-to-server, C2S2 Two-client-two-server, FS forward security, UDOD security against undetectable on-line dictionary attack, UKS security against unknown key-share attack, PCI security against password compromised impersonation attack, OFD security against off-line dictionary attack.

Round 2. The only difference between the literature [11] and our proposed protocol is that one server changes into two servers. So that brings about two points changed:

1) There are two more Mac_{**}, so the probability of distinguishing Mac_{**} with random integers is $(q_s + q_e)^2/2N_1$.
2) According to the birthday paradox, there are two more $T_n(x)$, so the probability of collisions in output $T_n(x)$ is at most q_s^2/N_1.

Round 3. It is the same with the literature [11]. The detailed descriptions of these games and lemmas are analogous to those in literature [11], with the differences discussed above, and therefore, they are omitted.

Theorem 3. *Our proposed two-realm PAKE protocol ensures key privacy against the server based on the fact that DDH assumption holds in the enhanced Chebyshev chaotic maps and F is a secure pseudo-random function ensemble, and*

$$Adv_D^{k_p}(\Lambda_{k_p}) \leq 4q_s Adv_{x,T_u}^{DDH} + 2q_e Adv^F$$

where q_e and q_s denote the maximum number of queries to the oracle Execute and Send-Client.

The proof of Theorem 3 is similar to that of Theorem 5.2 in [19] and Theorem 3 in [11]. The difference between our proposed protocol and the literature [19] is that we just replace the enhanced Chebyshev chaotic map values with the ElGamal discrete logarithm values. The difference between our proposed protocol and the literature [11] is that our proposed protocol is designed in different realm with different password, so some changed details can be described in Section 4.2.

Next, from the Table 3, we can see that the proposed scheme can provide secure session key agreement, perfect forward secrecy and so on. As a result, the proposed scheme is more secure and has much functionality compared with the recent related scheme.

5 Efficiency Analysis

5.1 The Comparisons Between Our Scheme and the Literature in Different Realms with Different Algorithms

Compared to RSA and ECC, Chebyshev polynomial computation problem offers smaller key sizes, faster computation, as well as memory, energy and bandwidth savings. In our proposed protocol, no time-consuming modular exponentiation and scalar multiplication on elliptic curves are needed. However, Wang [16] proposed several methods to solve the Chebyshev polynomial computation problem.

To be more precise, on an Intel Pentium4 2600 MHz processor with 1024 MB RAM, where n and p are 1024 bits long, the computational time of a one-way hashing operation, a symmetric encryption/decryption operation, an elliptic curve point multiplication operation and Chebyshev polynomial operation is 0.0005s, 0.0087s, 0.063075s and 0.02102s separately [10]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations.

For simplicity, the literatures [3, 6, 13, 15] in the different realms architecture, we omit the comparisons table detailedly. The reason is that our proposed protocol are mainly based on chaotic maps algorithms which is more efficient than the other algorithms, such as RSA and ECC, in the literatures [3, 10, 13, 15].

5.2 The Comparisons Between Our Scheme and the Literature with the Same Algorithms

Table 4 shows performance comparisons between our proposed scheme and the literature of [11, 12, 18, 19, 11, 20] in three-party architecture with chaotic maps.

Table 4: Cost comparison existing protocols for 3PAKE based on Chebyshev chaotic maps and our protocol

The others / Our protocol	R	RN (A/B/S) (A/B/S_A/S_B)	PKE (A/B/S) (A/B/S_A/S_B)	SKE (A/B/S) (A/B/S_A/S_B)	T (A/B/S) (A/B/S_A/S_B)
Our protocol	3	1/1/1/1	0/0/2/2	0/0/0/0	2/2/4/4
Yang and Cao's protocol [19]	4	2/2/3	0/0/1	0/0/1	0/0/0
Lai et al.'s protocol [11]	4	2/2/3	0/0/1	0/0/1	6/6/10
Yoon-Jeon's protocol [20]	5	2/1/0	2/2/0	1/1/1	2/2/0
Xie et al.'s protocol [18]	6	1/1/1	2/2/0	3/3/0	3/3/2
Lee et al.'s protocol [12]	5	1/1/1	2/2/0	4/4/0	3/3/2

The others / Our protocol	R	H (A/B/S) (A/B/S_A/S_B)	D (A/B/S) (A/B/S_A/S_B)	F (A/B/S) (A/B/S_A/S_B)
Our protocol	3	0/0/0/0	0/0/0/0	2/2/4/4
Yang and Cao's protocol [19]	4	0/0/0	0/0/0	4/4/2
Lai et al.'s protocol [11]	4	0/0/0	0/0/0	4/4/2
Yoon-Jeon's protocol [20]	5	2/0/2	1/1/2	0/0/0
Xie et al.'s protocol [18]	6	5/5/4	2/2/4	0/0/0
Lee et al.'s protocol [12]	5	4/4/7	0/0/0	0/0/0

R Round, RN Random number, PKE Public key encryption, SKE Secret key encryption. A: participant A, B: participant B, S: Single Server, SA: ServerA, SB: ServerB, T, D, H and F represent the time for performing a Chebyshev polynomial computation, a symmetric encryption/decryption, a one-way hash function and pseudo-random function, respectively.

6 Conclusion

In this paper, we conduct a comprehensive and general study of two-party in different realms PAKE protocol over standard model using chaotic maps. Most existing researches are concerning about concrete environment, such as two-party AKE or three-party AKE based on chaotic maps, but as far as we know, there is no general and extensible architecture about different realms based on chaotic maps has been proposed. However, through our exploration, we firstly clarify that the PAKE scheme using chaotic maps in different realms is more suitable for the real environment. Then, we proposed a suitable protocol that covers those goals and offered an efficient protocol that formally meets the proposed security definition. Finally, after comparing with related literatures respectively, we found our proposed scheme has satisfactory security, efficiency and functionality. Therefore, our protocol is more suitable for practical applications. For the future, we will investigate some extended function, such as the group authenticated key agreement or resistant quantum attack authenticated key agreement in different realm.

References

[1] M. S. Baptista, "Cryptography with chaos," *Physics Letters A*, vol. 240, no. 1, pp. 50–54, 1998.

[2] J. W. Byun, Ik R. Jeong, D. H. Lee, C. S. Park, "Password-authenticated key exchange between clients with different passwords," in *Information and Communications Security (ICICS'02)*, LNCS 2513, pp. 134–146, Springer, 2002.

[3] J. W. Byun, D. H. Lee, J. I. Lim, "EC2C-PAKA: An efficient client-to-client password-authenticated key agreement, *Information Sciences*, vol. 177, no. 19, pp. 3995–4013, 2007.

[4] R. Canetti, and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Advances in Cryptography (EUROCRYPT'01)*, LNCS 2045, pp. 453–474, Springer, 2001.

[5] L. Chen, *A Weakness of the Password-authenticated Key Agreement between Clients with Different Passwords Scheme*, ISO/IEC JTC 1/SC27 N3716.

[6] D. Denning, G. Sacco, "Timestamps in key distribution protocols," *Communications of the ACM*, vol. 24, no. 8, pp. 533–536, 1981.

[7] L. R. Devaney, *An Introduction to Chaotic Dynamical System*, Cummings Publishing Company Inc., The Benjammin, Menlo Park, 1986.

[8] J. C. Jiang, Y. H. Peng, "Chaos of the Chebyshev polynomials," *Natural Science Journal of Xiangtan University*, vol. 19, no. 3, pp. 37–39, 1996.

[9] J. Kim, S. Kim, J. Kwak, D. Won, "Cryptanalysis and improvements of password authenticated key exchange scheme between clients with different pass-

words," in *Proceedings of ICCSA'04*, LNCS 3044,pp. 895–902, Springer, 2004.

[10] L. Kocarev, and S. Lian, Chaos-Based Cryptography: Theory, Algorithms and Applications, pp. 5354, 2011.

[11] H. Lai, M. A. Orgun, J. Xiao, et al, "Provably secure three-party key agreement protocol using Chebyshev chaotic maps in the standard model," *Nonlinear Dynamics*, vol. 77, pp. 1427–1439, 2014.

[12] C. C. Lee, C. T. Li, C. W. Hsu, "A three-party password based authenticated key exchange protocol with user anonymity using extended chaotic maps," *Nonlinear Dynamics*, vol. 73, pp. 125–132, 2013.

[13] R. C. W. Phan, B. Goi, "Cryptanalysis of an improved client-to-client password-authenticated key exchange (C2C-PAKE) scheme," in *Proceedings of ACNS'05*, LNCS 3531, pp. 33–39, Springer, 2005.

[14] V. Shoup, *Sequences of Games: A Tool for Taming Complexity in Security Proofs*, Report 2004/332, International Association for Cryptographic Research (IACR), 2004.

[15] S. Wang, J. Wang, M. Xu, "Weakness of a password-authenticated key exchange protocol between clients with different passwords," in *Proceedings of ACNS'04*, LNCS 3089, pp. 414–425, Springer, 2004.

[16] X. Wang, and J. Zhao, "An improved key agreement protocol based on chaos," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, pp. 4052–4057, 2010.

[17] T. Wu, "The secure remote password protocol," in *Internet Society Network and Distributed System Security Symposium (NDSS'98)*, pp. 97–111, 1998.

[18] Q. Xie, J. M. Zhao, X. Y. Yu, "Chaotic maps-based three party password-authenticated key agreement scheme," *Nonlinear Dynamics*, vol. 74, pp. 1021–1027, 2013.

[19] J. H. Yang, T. J. Cao, "Provably secure three-party password authenticated key exchange protocol in the standard model," *Journal of System Software*, vol. 85, pp. 340–350, 2012.

[20] E. J. Yoon, I. S. Jeon, "An efficient and secure Diffie-Hellman key agreement protocol based on Chebyshev chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, pp. 2383–2389, 2011.

[21] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," in *Chaos Solitons Fractals*, vol. 37, no. 3, pp. 669–674, 2008.

[22] M. Zhang, "New approaches to password authenticated key exchange based on RSA," in *Advances in Cryptology (ASIACRYPT'04)*, LNCS 3329, pp. 230–244, Springer, 2004.

[23] H. F. Zhu, X. Hao, Y. F. Zhang and M. Jiang, "A biometrics-based multi-server key agreement scheme on chaotic maps cryptosystem," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 2, pp. 211–224, Mar. 2015.

[24] H. F. Zhu, M. Jiang, X. Hao and Y. Zhang, "Robust biometrics-based key agreement scheme with smart cards towards a new architecture," in *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 1, pp. 81–98, Jan. 2015.

[25] H. F. Zhu, Y. F. Zhang and Y. Zhang, "A one-way authentication key agreement scheme with user anonymity based on chaotic maps towards multi-server architecture," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 2, pp. 274–287, Mar. 2015.

Hongfeng Zhu obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hongfeng Zhu is a full associate professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Dr. Zhu had published more than 50 international journal and international conference papers on the above research fields.

Yifeng Zhang, 24 years old, an undergraduate from Shenyang Normal University, major in information security management. During the four years of college, after completing her studies, he enjoys reading the book related to this major. Under the guidance of the teacher, he has published two articles in EI journals.

Yan Zhang, 23 years old, an undergraduate from Shenyang Normal University, major in information security management. In the four years of college, after completing her studies, she enjoys reading the book related to this major. Under the guidance of the teacher, she has published two articles in EI journals.

Collaborative IDS Framework for Cloud

Dinesh Singh[1], Dhiren Patel[2], Bhavesh Borisaniya[2], and Chirag Modi[3]
(Corresponding author: Dinesh Singh)
Department of Computer Science & Engineering, Indian Institute of Technology, Hyderabad, India[1]
Department of Computer Engineering, National Institute of Technology, Surat, India[2]
Department of Computer Science & Engineering, National Institute of Technology Goa, India[3]
(Email: barehla88@gmail.com)
(Received Apr. 16, 2014; revised and accepted Jan. 16 & Mar. 4, 2015)

Abstract

Cloud computing is used extensively to deliver utility computing over the Internet. Defending network accessible Cloud resources and services from various threats and attacks is of great concern. Intrusion Detection System (IDS) has become popular as an important network security technology to detect cyber-attacks. In this paper, we propose a novel Collaborative IDS (CIDS) Framework for cloud. We use Snort to detect the known stealthy attacks using signature matching. To detect unknown attacks, anomaly detection system (ADS) is built using Decision Tree Classifier and Support Vector Machine (SVM). Alert Correlation and automatic signature generation reduce the impact of Denial of Service (DoS) /Distributed DoS (DDoS) attacks and increase the performance and accuracy of IDS.

Keywords: Anomaly detection, collaborative IDS, cloud security, intrusion detection, signature generation

1 Introduction

Users of a cloud request access from a set of web services that manage a pool of computing resources (i.e., machines, network, storage, operating systems, application development environments, application programs). When granted, a fraction of the resources from the pool they are dedicated to the requesting user until he or she releases it. Cloud computing combines several technologies like distributed computing, grid computing, virtualization, utility computing, network computing etc. Each of the involving technologies has vulnerabilities that cause several security and privacy issues. One of the major security challenges is to defend Cloud network from the attacks like IP spoofing, DNS poisoning, man-in-the-middle attack, port scanning, insider attack, Denial of Service (DoS) attack, and Distributed Denial of Service (DDoS) attack etc. [15].

To deal with such attacks, Intrusion Detection System (IDS) can be used. Intrusion detection is the act of detecting actions that attempt to compromise the Confidentiality, Integrity or Availability of a system/network. Security threats are divided into three categories [20]: (1) breach of confidentiality, (2) failure of authenticity, and (3) unauthorized denial of service.

Based on the protection objective, IDS are classified into three categories: Host-based (HIDS), Network-based (NIDS) and Distributed IDS. Host based IDS collects the internal activities (like system call) of a host and analyse for malicious activities. Network based IDS attempts to discover unauthorized access to a computer network by analyzing network traffic. Distributed IDS collects the events from multiple sources and analyzes collectively for malicious activity. On the basis of detection techniques, IDSs are divided in two categories [7] viz; Signature based and Anomaly based. Signature based IDS detects known attacks through matching signature in pre-stored attack signature base. Signatures are the well formatted patterns found in the attack. Thus they are limited to detecting known attacks. Anomaly based IDS store the behavior of previous events and construct a model to predict the behavior of the incoming events. These systems are able to detect both known as well as an unknown attack, however produce high false alarm and high computational cost. Isolated IDSs are not able to detect coordinated attack such as DDoS attacks. To detect such kind of attacks, we need collaborative IDS. A collaborative IDS framework consists of two main functional units [29]:

1) Detection Unit: A detection unit consists of multiple detection sensors, where each sensor monitors its own sub network or hosts separately and then generates low-level intrusion alerts.

2) Correlation Unit: A correlation unit transforms the low-level intrusion alerts into a high level intrusion report of confirmed attacks. There are three alert correlation approaches:

    a. Centralized approaches [29]: Each participating IDSs has only detection unit, while analysis unit is at the central server.

b. Hierarchical approaches [29]: Each IDS has detection unit. The entire system is organized into a hierarchy of small communication groups. Each group has its correlation unit that is responsible for correlation within the group and its processed data will be sent upward to a node at a higher level in the hierarchy for further analysis.

c. Fully distributed approach [29]: Each participant IDSs has both detection unit and correlation unit and communicates to each other using some protocol like peer-to-peer.

We are using a centralized approach as the importance of communication in cloud computing is vital. In comparison to fully distributed and hierarchical approaches, centralized approach is less scalable, but requires less communication overhead [29].

Shared and distributed resources in the Cloud system make it difficult to develop a security model for detecting intrusion and ensuring the data security and privacy in the Cloud. Because of transparency issue, no Cloud provider allows its customers to implement intrusion detection or security monitoring system extending into the management services layer providing back channel behind virtualized Cloud instances. IDS technology has been tested to be capable of working well in some large scale networks, however, its utilization and deployment in Cloud Computing is still a challenging task [1].

In this paper, we have proposed a Collaborative IDS (CIDS) which keeps the knowledge base up-to-date, produce low communication overhead and able to detect known and unknown attack with fast detection rate.

The rest of the paper is organized as follows: Section 2 discusses related work. Section 3 describes the theoretical background about classifiers used in our proposed approach. The proposed approach is discussed in Section 4. Section 5 describes the experimental setup, evaluation method and results. Section 6 concludes our research work with references at the end.

2 Related Work

Several IDS have been proposed to-date to detect intrusions in the traditional network and in the Cloud network.

Hwang et al. [8, 9] proposed a cooperative anomaly and intrusion detection system for a distributed network. The signature-based NIDS (Snort) is cascaded with a custom designed ADS. These two subsystems join hands to cover all trafic flow events, initiated by both legitimate and malicious users. Single connection intrusive attacks are detected by NIDS at the packet level by signature matching. Remaining unknown attacks, which cannot be detected by signature-based NIDS, are passed on to the ADS. A signature generator bridges the two sub-systems.

Lo et al. [13] proposed a system to reduce the impact of DOS and DDOS attacks. To provide such ability, IDSs in the cloud computing regions exchange their alerts with each other. In the system, each of IDSs has a cooperative agent used to compute and determine whether to accept the alerts sent from other IDSs or not. By this way, IDSs could avoid the same type of attack happening in future. But this system uses fully distributed alert correlation system which produces high communication overhead.

Modi et al. [16] proposed a framework to reduce the impact of DoS and DDoS which integrates a NIDS in the Cloud infrastructure. They combined Snort and decision tree (DT) classifier to implement their framework. It aims to detect network attacks in Cloud, while maintaining performance and service quality.

Sandar et al. [24] describe a new type of DDoS attack, called Economic Denial of Sustainability (EDoS) in Cloud services and proposed a solution framework for detecting EDoS attack. EDoS attacks are HTTP and XML based DDoS attack. The EDoS protection framework uses firewall and puzzle server to detect EDoS attack. Here, the authors demonstrated EDoS attack in the Amazon EC2 Cloud. However, it is not an adequate solution because it uses only traditional firewalls.

Combining the multiple techniques overcome the limitation of each other. Gaddam et al. [4] proposed a supervised anomaly detection using k-Means clustering and Decision Tree. A method to cascade k-Means clustering and the ID3 decision tree learning methods for classifying anomalous and normal activities in a computer network. First of all using k-Means, the dataset is partition in k clusters. Then the decision tree on each cluster refines the decision boundaries by learning the sub-groups within the cluster. To obtain a final decision on the classification, the decisions of the k-Means and ID3 methods are combined using two rules: (1) the Nearest-neighbor rule and (2) the nearest consensus rule. A similar approach is proposed by Yasami et al. [28] for unsupervised learning. However, the use of a serial combination of k-Means and ID3 increase the learning time. Detection on both Subject to algorithm and rules for final decision has also increased the detection time as well.

3 Theoretical Background

3.1 Snort

Snort [25], is a well-known open source packet sniffer and NIDS. It is configurable and freely available for multiple platforms (i.e. GNU/Linux, Window). The misuse IDS model used in Snort is based on matching of attack signature with pre-stored signatures associated with known attacks like the PoD, port-sweep, DoS-nuke, Tear-drop, and Saint, etc. The detection engine of Snort allows registering, alerting and responding to any known attack. Snort cannot detect unknown or multi-connection attacks [8, 9].

Decision Tree Classifier

Decision tree (DT) classifier [6, 16] is a supervised classification technique. It requires a labelled training dataset to construct a decision tree. As shown in Figure 1, the decision tree is a tree structure, where each non leaf node denotes a test on an attribute, each branch represents an outcome of the test, and each leaf node holds a class label.

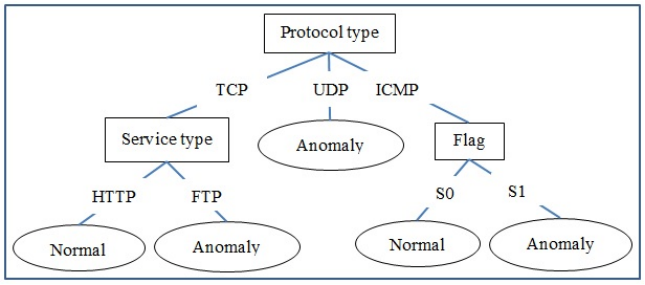


Figure 1: A sample decision tree

To test an unknown network traffic profile tuple (e.g. X), the attribute values of the X are tested against the decision tree. A path is traced from the root to a leaf node; class label of the leaf is the prediction for that tuple X.

For decision tree classifier, no domain knowledge or parameter setting is required, and therefore it is appropriate for exploratory knowledge discovery. It can handle high dimensional data and the representation of acquired knowledge in tree form is intuitive, and generally easy to assimilate by humans [16].In general, decision tree classifiers have good accuracy for categorical data values but in case of continuous data values it suffers from overfitting [22, 27]. However, successful use may depend on the data used for learning.

3.2 Support Vector Machine

Support Vector Machine (SVM) is based on statistical learning theory developed by Vapnik [6, 14]. The SVM approach is very popular for classification and regression problems because of its good generalization capability and its superiority in comparison with other machine learning paradigms. SVM solves the problem of over-fitting and can easily make a generalized model from the least number of samples. But their learning time increases rapidly with an increase in training size. SVMs were originally designed for binary-class classification; hence, it is straightforward to use this paradigm in the present problem for classification between normal and malicious behavior in the patterns of activity in the audit stream. In fact, SVMs [12, 14, 17] have been proposed as a powerful technique for intrusion detection classification. It classifies data by determining a set of support vectors, which are members of the set of training inputs that outline a hyperplane in feature space.

Let us assume $\{(x_1, y_1), ..., (x_n, y_n)\}$ be a training set with $x_i \in R_d$ and $y_i = \{-1, +1\}$ is the corresponding target class. The basic problem for training an SVM can be reformulated as:

$$Maximize : J = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \alpha_j y_i y_j (x_i^T, x) \quad (1)$$

$$Subject\ to \sum_{i=1}^{n} \alpha_i y_i = 0\ and\ \alpha_i \geq 0, i = 1, 2, ..., n$$

Kernel function is used for computation of dot products between vectors without explicitly mapping to another space. Use of a kernel function [18] addressed the curse of dimensionality and the solution implicitly contains support vectors that provide a description of the significant data for classification. Substituting Kernel $K(x_i^T, x)$ for in Equation (1) produces a new optimization problem:

$$Maximize : J = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \alpha_j y_i y_j K(x_i^T, x) \quad (2)$$

$$Subject\ to \sum_{i=1}^{n} \alpha_i y_i = 0\ and\ 0 \leq \alpha_i \leq C, i = 1, 2, ..., n$$

where C is soft margin parameter. Solving it for, gives m support vectors (SV), their respective values of α_i and the value of bias b. These SVs gives a decision function of the form

$$f(x) = \sum_{i=1}^{m} \alpha_i y_i K(x_i^T, x) + b, \quad (3)$$

where α_i are Lagrange multipliers, x is the test tuple and $f(x) = f(-1, +1)$ is its prediction.

4 Proposed CIDS Framework

As shown in Figure 2, we integrate NIDS module in each cloud cluster to detect network attacks. Correlation Unit (CU) is placed in any one cluster. NIDS detects the intrusions within a cluster and Correlation Unit provides collaboration between all cluster NIDSs. Bully [5] election algorithm is used to elect one best cluster for placement of CU on the basis of workload.

4.1 NIDS Architecture

As shown in Figure 3, we use Snort and an Anomaly Detection System (ADS) built using Decision Tree classifier and SVM classifier techniques. Snort is used to detect known attacks, whereas ADS predicts that the given event is malicious or not, by observing previously stored network events.

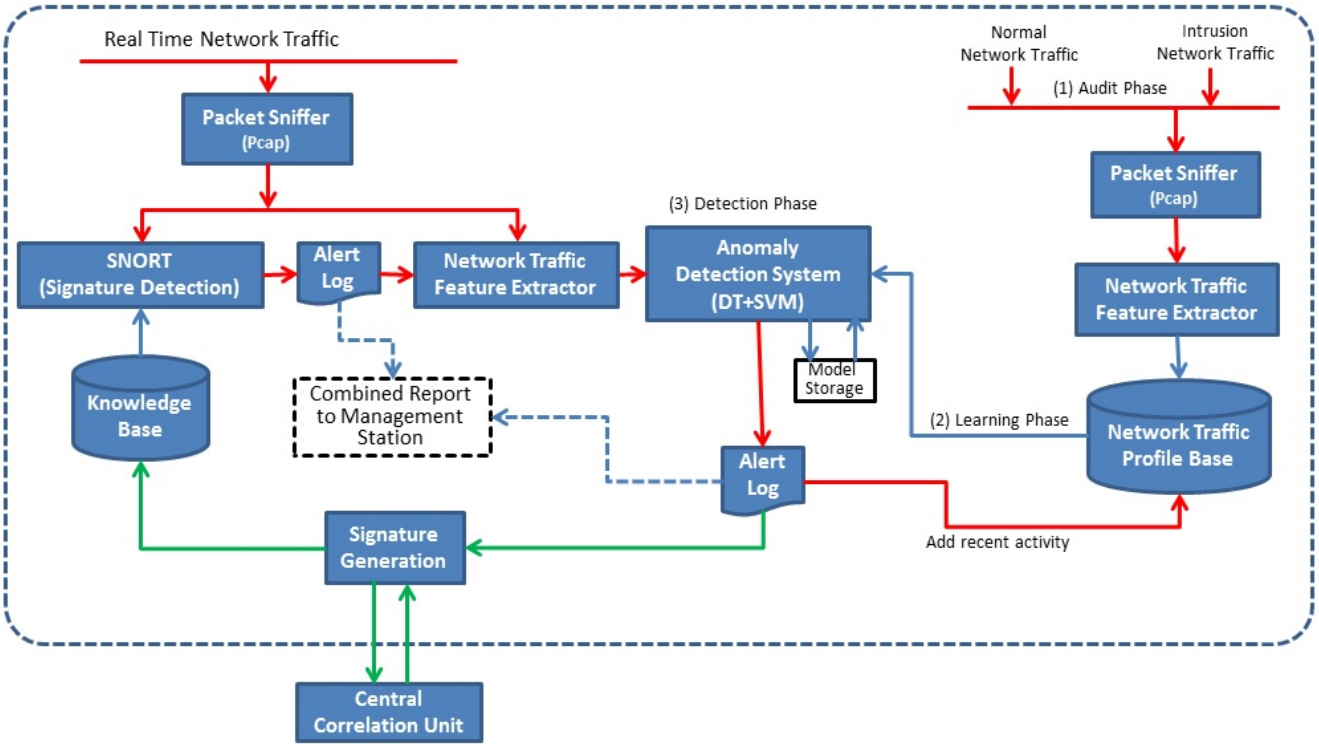


Figure 3: NIDS architecture

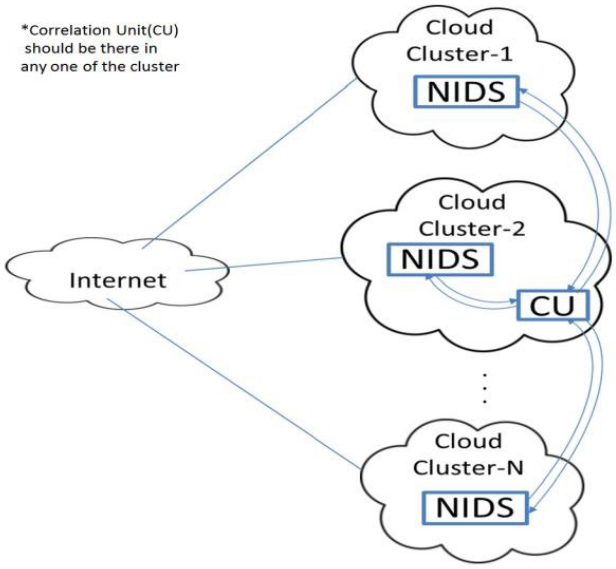


Figure 2: Proposed collaborative IDS framework in cloud

1) Audit Phase. During the audit phase, various (normal and intrusion) network traffic profiles are generated and stored. First we capture the normal traffic and generate network traffic profiles and give them class label as Normal. To generate malicious traffic, we perform various attacks and again capture the traffic and generate network traffic profiles and give them class label as Intrusion and store into the network traffic profile base. Network profile generation process is explained in Section 4.3.

2) Learning Phase: In this phase, a model for anomaly detection system is constructed from the network traffic profile base. The learning process of Anomaly Detection is shown in section 4.2.

3) Detection Phase: During the detection phase, we capture the real time traffic and generate network traffic profiles on the y and pass these profiles as input to the ADS. ADS generates the alert, if it found any correlation of the input profile with malicious profiles.

Incoming network traffic will pass through Snort; here known attacks are identified through signature matching. The remaining attacks are detected by ADS. An alert entry is made in the log, if an unknown attack is detected. If the frequency of an attack detected by ADS is crossing a frequency threshold T_f, then we go for generating a Snort based signature for those connections. This increases the performance of NIDS as Snort is able

to detect these frequent attacks in a short time. Once the signature is generated, we update local knowledge base as well as send this signature to a central correlation unit. The central correlation unit receives the signature sent by all the NIDSs in the Cloud network and make a decision on the bases of how much part of total NIDSs send the similar signature.

$$S > S_T \text{ where } S = \frac{No\ of\ IDS\ Support\ Same\ Signature}{Total\ No\ of\ IDS\ in\ the\ System}$$

$$and\ S_T = Threshold.$$

Value of S_T will be set by admin (as 0.5 for majority decision). If $S > S_T$ for an attack signature then correlation unit multicasts this signature to all the IDSs. They receive this signature and update their knowledge base.

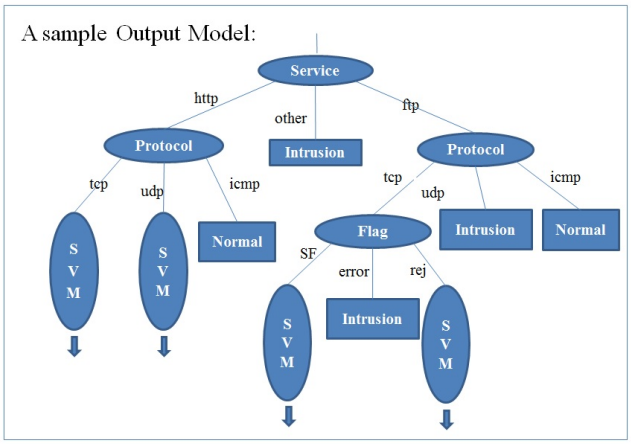


Figure 4: A sample model for anomaly detection

4.2 Proposed Anomaly Detection System

We split the training dataset using decision tree and build the SVM model on each subset. First, we call decision tree algorithm for attributes having categorical data values. We select a best attribute on the basis of maximum information gain and make the root node of the tree to use this attribute. The branches of this node are the distinct values of the selected attributes. These branches end on some other node. Then we split the entire data set into subsets with respect to each distinct value of selected attribute. We call the decision tree algorithm for each sub dataset recursively. If at some place, all profiles belong to a same class label then the leaf node with that class label is created, if not, then another attribute of categorical data values is selected to create an internal node like root node. If at any stage, no attribute with categorical data values remaining or the information gain of best attribute chosen is less than the threshold then a model is created using SVM for the continuous values. The output looks like as shown in Figure 4. The learning process is shown in Figure 5.

4.2.1 Learning Algorithm

Algorithm 1 Learning algorithm
$\mathbf{D}$ = *Set of Network Traffic Profiles used for training.*
$\mathbf{C}$ = *Set of Class Labels i.e. Intrusion, Normal.*
$\mathbf{A}$ = *Set of Attribute used to represent Network Connection Profiles.*
We divide the attributes into two subsets,
$\mathbf{A_S}$ = *Set of Symbolic (Categorical) value Attributes (e.g. Protocol, Service, flag etc.).*
$\mathbf{A_N}$ = *Set of Numeric (Continuous) value Attributes (e.g. Srcbyte, Dstbyte, count etc.).*
$\mathbf{T_{InfoGain}}$ = *Minimum Threshold for InfoGain*
$\mathbf{H}$ = *Hyperplane*

$$\mathbf{InfoGain(D)} = E(D) - \sum_{i=0}^{v} \frac{|D_i|}{|D|} E(D_i)$$

$$where\ \mathbf{E(D)} = -\sum_{i=0}^{m} p_i log_2(p_i)$$

E is the entropy and is the probability of appearance of Class label.
DecisionTree(D, A_S, A_N)

1: Begin
2: **if** (All Samples in $D \in C_i$) **then**
3: Create Leaf Node with Class Label C_i;
4: **end if**
5: **if** $(A_S = \phi)$ **then**
6: $H \leftarrow SVM(D, A_N)$; //construct the SVM model
7: Create Leaf Node with H;
8: **end if**
9: $A_{S-best} \leftarrow getBestAttribute(D, A_N)$;
10: **if** $A_{S-best}.InfoGain \leq T_{InfoGain}$ **then**
11: $H \leftarrow SVM(D, A_N)$;
12: Create Leaf Node with H;
13: **end if**
14: $Root \leftarrow createNode(A_{S-best})$;
15: $A_S \in A_S - A_{S-best}$;
16: **for** each value $V_i \in Domain(A_{S-best})$ **do**
17: $D_i \leftarrow D\ where\ (A_{S-best} = V_i)$;
18: $ChildTree \leftarrow$ DecisionTree(D_i, A_S, A_N);
19: Root.Child[i] $\leftarrow$ ChildTree;
20: Return *Root*
21: **end for**
22: End

4.2.2 Testing

To test an unknown profile on ADS, we trace the tree from root to leaf; if leaf node is a class label then this is the prediction. If a leaf node is an SVM model then the prediction is given by this SVM model.

4.3 Network Traffic Profile Generation

A packet sniffer (libpcap) is used to capture network packet frames from the data link layer and to assemble

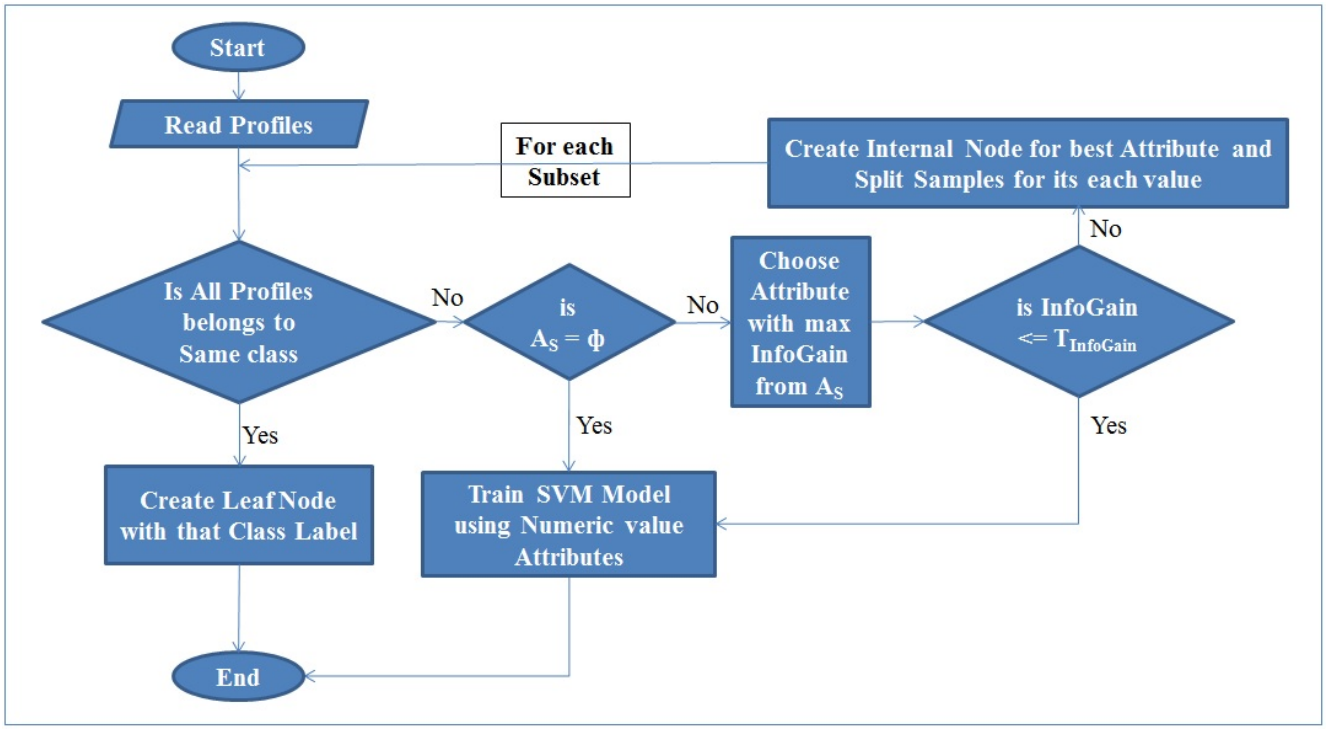


Figure 5: Flow chart of learning process of ADS

them as raw packet. The packets are collected for a complete connection. A connection is a sequence of packets starting and ending at some well-defined times, between which data flows to and from a source IP address to a target IP address under some well-defined protocol [11]. For generating a network profile, the network traffic feature extractor extracts the network features viz; basic, traffic and content (as in KDD'99 dataset) from the raw packets [11].

1) Basic Features: It involves all the attributes that are extracted from a TCP/IP connection, e.g., protocol, service, size of traffic flow etc.

2) Traffic based Features: These features are computed within time frame, and divided into two groups viz; same host features and same service features. Same host features involve the connections having same destination host within given time frame (E.g. 2 seconds) and statistics related to protocol, service, flag error etc. Same service features include the connections having same services within given time frame to calculate traffic related statistics.

3) Content based Features: In this category, data portions of the packets are examined. It involves only a single connection. To detect attacks (E.g. Remote to local and User to root) that are embedded in the data portions of the packets, suspicious behavior in the data portion is looked, e.g., number of failed login attempts, number of root access.

A Connection is identified as ($SrcIP$: $SrcPort$ $\rightarrow$ $DstIP$: $DstPort$ $Protocol$). As as soon as a new connection starts, we make an entry into Connection cache and capture all packets sent during communication. When the connection terminates then we extract basic features from header part, content features from payload and traffic statistics by comparing this connection with the previously established connection (during last t seconds). Where, t is the size of the sliding window.

4.4 Signature Generation

As shown earlier in Figure 3, signature generation is an independent process running side by side. For frequent attack, we generate Snort based signature. For this, we take the payload stream of all occurrences of the attack, find the longest common subsequence and represent it in the form of regular expression. On the basis of header information and regular expression, we write Snort rule as:

$$action\ protocol\ Source\ IP : Port \rightarrow$$
$$Destination\ IP : Port\ (msg : \text{“}Message\ to\ display\text{”}$$
$$pcre : [(< regex > | m < delim >< regex >$$
$$< delim >)\ ismxAEGRUBPHMCOIDKYS]$$ [23].

After generating signature, we verify it on normal connection. If no match found then we accept it. If it generates more number of false alarms then we discard it.

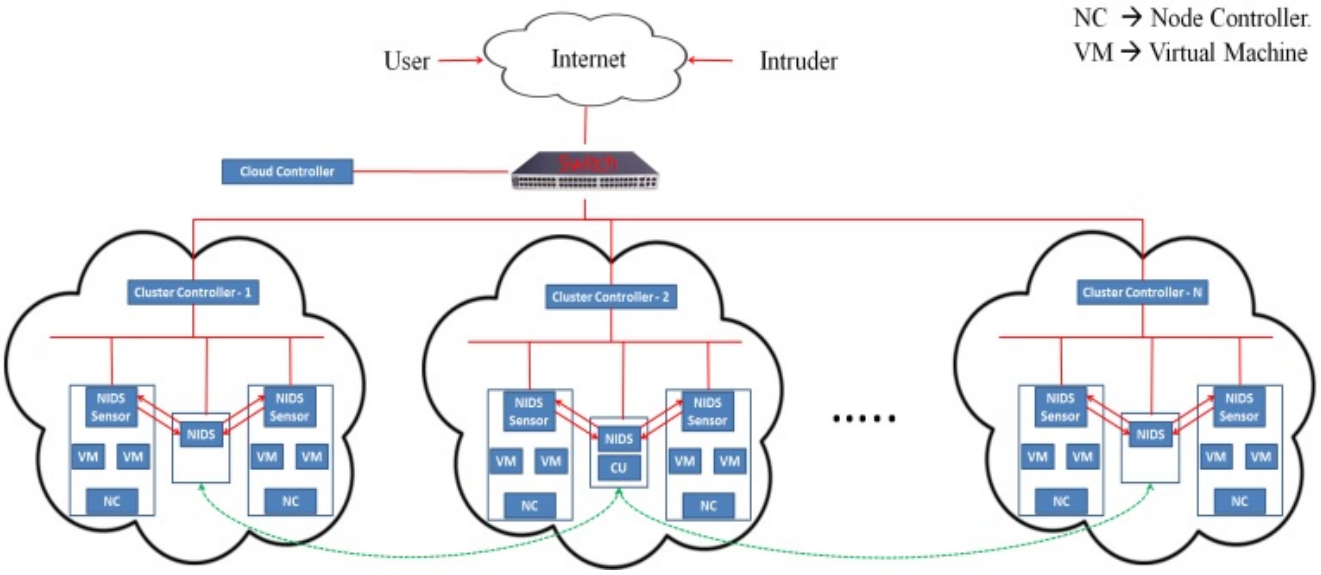


Figure 6: Experimental setup

5 Evaluation and Results

5.1 Experimental Setup

We installed eucalyptus 3.2.0 [3] cloud on CentOS 6.3. Cloud controller is on separate machine. There are $N(=3)$ cloud clusters. Each cluster contains multiple numbers of node controllers with multiple virtual machines running on each node. NIDS sensors are placed in all the Node controllers on the virtual bridge (br0) so that it can capture the internal traffic (i. e. VM-to-VM, VM-to-User etc.). We place the central database and remaining part of NIDS on a separate machine connected with the cluster. Only Node Controllers are allowed to access this machine. Correlation Unit is there in Cluster-2 as shown in Figure 6.

We use tcpdump and libpcap [26] sniffer to capture the packets. To train SVM, we use libsvm [2]. We use RBF kernel with $gamma = 0.125$ and $C = 2.0$. Window size $t = 2$ second. $S_T = 0.5$.

For evaluating performance results, we have used parameters viz; Intrusion Detected, Intrusion Missed, True Alarms, False Alarms, Accuracy, Learning and Detection time.

5.2 Results and Discussion

Evaluation of our anomaly detection system is carried on different datasets viz; KDD99 [11], NSL-KDD [21] and ITOC [10]. Details of these datasets and experiments are shown in Table 1 and Table 2.

Figure 7 shows the model generated after learning from the kddcup10% dataset. The time taken in learning is 46.616 seconds. There are 22 internal nodes, 108 leaf nodes with class label and 35 SVM models are created with the maximum height of tree is 4.

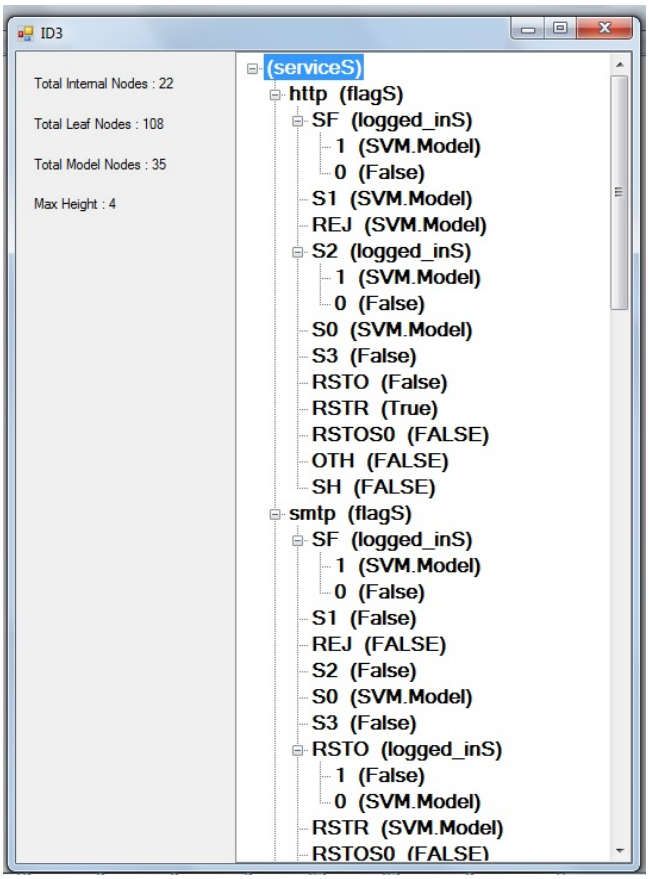


Figure 7: Screen shot of tree model generated after learning

Table 1: Details of the dataset

Training Dataset	Total Records	Intrusive Records	Normal Instances	No. of Attributes
KDD99 (10%)	4,94,021	3,96,743	97,278	41
KDD99	48,98,432	39,25,650	9,72,781	41
KDD99test (10%)	3,11,029	2,50,436	60,593	41
NSL-KDD	1,48,517	71,462	77,055	41
NSL-KDDtest	22,544	12,832	9,712	41
ITOC	4,00,000	1,67,879	2,32,121	27
ITOCtest	2,31,831	92,848	1,38,983	27

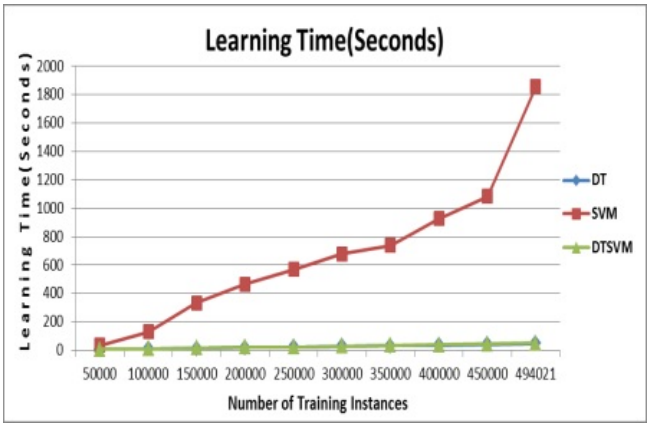


Figure 8: Comparison of learning time

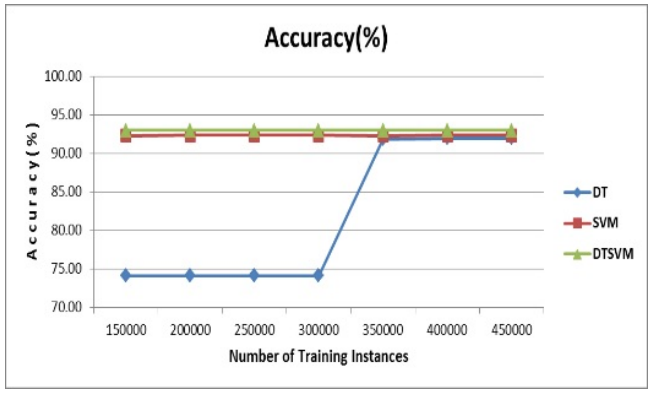


Figure 10: Comparison of accuracy

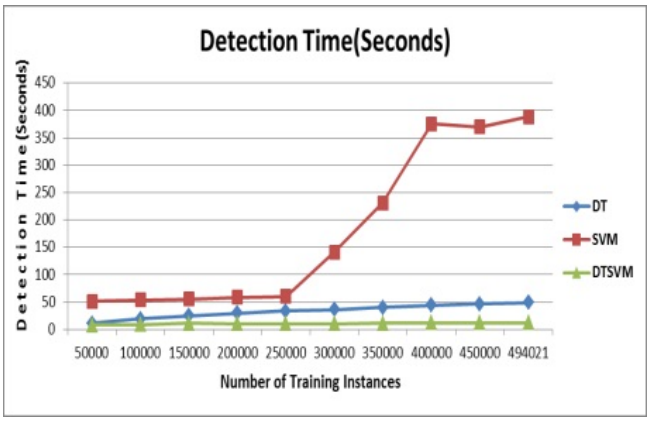


Figure 9: Comparison of detection time

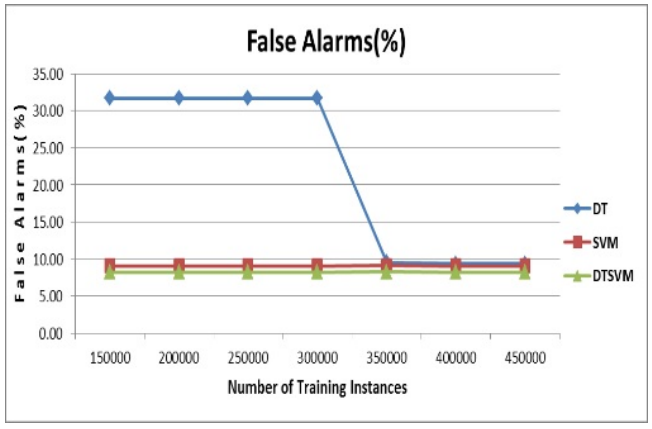


Figure 11: Comparison of false alarms

Table 2: Details of experiments

Test No.	Training Dataset	Test Dataset
Test 1	NSL-KDD	NSL-KDDtest
Test 2	KDD99(10%)	KDD99
Test 3	KDD99(10%)	KDD99test(10%)
Test 4	ITOC	ITOCtest

Figures 8, 9, 10, 11 show the behavior of decision tree, SVM and proposed ADS when we change the size of training dataset. For this we take training profiles from KDD99 (10%) and evaluate the KDD99test (10%). Figure 8 shows that learning time for the proposed ADS is almost equal to decision tree and much less than SVM. While as shown in Figure 9 the detection time is less in comparison to decision tree and SVM. Figure 10 shows that accuracy is higher than decision tree and SVM, while producing low false alarms as in Figure 11. Thus it outperforms both SVM and decision tree in terms of accuracy and computation time. Figure 12 shows the results of all the experiments listed in Tables 3 & 4 and their weighted average. Results on NSL-KDD (Test1) shows that 98.35% intrusions are detected, 1.65% intrusions are missing, 2.97% alarms are false and overall accuracy is 97.38%. Results on KDD99 (Test2) shows that 99.56% intrusions are detected, 0.44% intrusions are missing, 8.22% alarms are false and overall accuracy is 93.05%. Results on KDD99 (Test3) shows that 99.99% intrusions are detected, 0.01% intrusions are missing, 0.01% alarms are false and overall accuracy is 99.99%. Results on ITOC (Test4) shows that 86.84% intrusions are detected, 13.16% intrusions are missing, 28.34% alarms are false and overall accuracy is 84.30%. Weighted average results shows that detection time is 55 microseconds, 99.40% intrusions are detected, 0.60% intrusions are missing, 1.69% alarms are false and overall accuracy is 98.92%.

Table 3: Comparison of accuracy and detection rate

	Accuracy (%)	Detection Rate (%)
Multi SVM [14]	92.050	-
CT-SVM [12]	69.800	-
Decision Tree [16]	96.710	96.250
FER [16]	75.000	-
SVM [19]	-	98.630
Ripper Rule [19]	-	98.690
Decision tree [19]	-	98.750
DT+SVM	**98.92**	**99.40**

6 Conclusions

In proposed CIDS, cascading decision tree and SVM has improved the detection accuracy and system performance as they remove the limitation of each other. Use of DT makes the learning process speedy and split the dataset into small sub datasets. Use of SVM on each sub dataset reduce the learning time of SVM and overcome the overfitting and reduce the size of decision tree to make the detection faster. Collaboration between NIDSs prevents the coordinated attacks against cloud infrastructure and knowledge base remains up-to-date. We have performed experiments to detect the accuracy of our proposed approach with well-known KDD dataset and found encouraging results.

References

[1] B. Borisaniya, A. Patel, D. R. Patel, and H. Patel, "Incorporating honeypot for intrusion detec-tion in cloud infrastructure," in *Trust Management VI IFIP Advances in Information and Communication Technology*, pp. 84–96, Surat, India, May 2012.

[2] C. C. Chang and C. J. Lin, "LIBSVM: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, pp. 27:1–27:27, 2011.

[3] Eucalyptus, *Eucalyptus Website*, Sept. 27, 2015. (`http://www.eucalyptus.com`)

[4] S. R. Gaddam, V. V. Phoha, and K. S. Balagani, "A novel method for supervised anomaly detection by cascading k-means clustering and ID3 decision tree learning methods," *IEEE Transactions On Knowledge and Data Engineering*, vol. 19, no. 3, pp. 345–354, 2007.

[5] H. Garcia-Molina, "Elections in a distributed computing system," *IEEE Transactions on Computers,*, vol. 31, no. 1, pp. 48–59, 1982.

[6] J. Han and M. Kamber, *Data Mining Concepts and Techniques (2nd edition)*, San Francisco, CA: Morgan Kauf-mann Publishers, 2006.

[7] Li C. Huang and M. S. Hwang, "Study of an intrusion detection system," *Journal of Electronic Science and Technology*, vol. 10, no. 3, pp. 269–275, 2012.

[8] K. Hwang, M. Cai, Y. Chen, and M. Qin, "Hybrid intrusion detection with weighted signa-ture generation over anomalous internet episodes," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 1, pp. 41–55, 2007.

[9] K. Hwang, Y. Chen, and H. Liu, "Defending distributed systems against malicious intrusions and network anomalies," in *Proceedings of 19th IEEE International Symposium on Parallel and Distributed Processing*, Denver, Colorado, Apr. 2005.

[10] ITOC, *ITOC*, Sept. 27, 2015. (`https://www.itoc.usma.edu/research/dataset/`)

Table 4: Evaluation results

	Intrusion Detected(%)	**Intrusion Missed(%)**	**True Alarms(%)**	**False Alarms(%)**	**Accuracy (%)**
Test1	98.35	1.65	97.03	2.97	97.383
Test2	99.56	0.44	91.78	8.22	93.050
Test3	99.99	0.01	99.99	0.01	99.988
Test4	86.84	13.16	71.66	28.34	84.30
Wt. Avg.	99.40	0.60	98.31	1.69	98.92

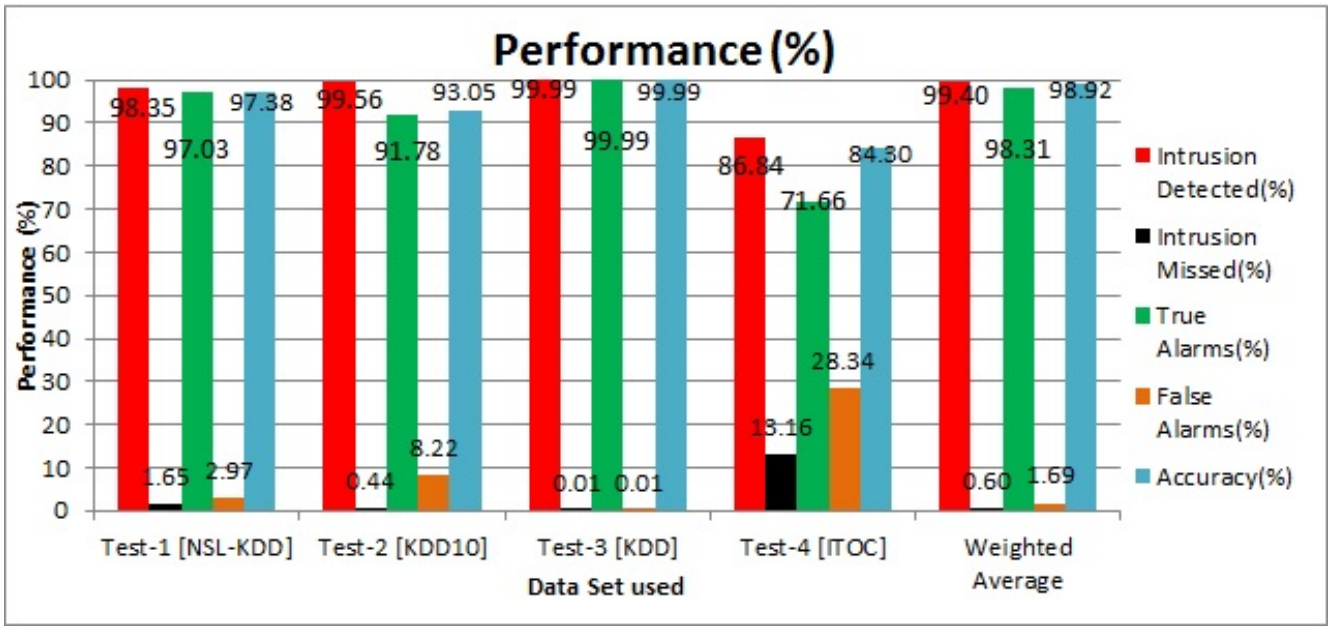


Figure 12: Evaluation results as per Tables 3 & 4 and their weighted average

[11] KDD, *KDD Cup 1999 Webpage*, Sept. 27, 2015. (`http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html`)

[12] L. Khan, M. Awad, and B. Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering," *The VLDB Journal*, vol. 16, no. 4, pp. 507–521, 2007.

[13] C. C. Lo, C. C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," in *39th International Conference on Parallel Processing Workshops*, pp. 280–284, San Diego, CA, Sep. 2010.

[14] A. Mewada, P. Gedam, S. Khan, and M. U. Reddy, "Network intrusion detection using multiclass support vector machine," *International Conference on ACCTA*, vol. 1, no. 2, pp. 2, 2010.

[15] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intru-sion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[16] C. Modi, D. Patel, B. Borisanya, A. Patel, and M. Rajarajan, "A novel framework for intrusion detection in cloud," in *Proceedings of the Fifth International Conference on Security of Information and Networks*, pp. 67–74, Jaipur, India, Oct. 2012.

[17] S. Mukkamala, G. Janoski, and A. Sung, "Intrusion detection using neural networks and support vector machines," in *Proceedings of the International Joint Conference on Neural Networks*, pp. 1702–1707, Honolulu, HI, May 2002.

[18] An na Wang, Y. Zhao, Y. T. Hou, and Y. L. Li, "A novel construction of svm compound kernel function," in *International Conference on Logistics Systems and Intelligent Management*, pp. 1462–1465, Harbin, Jan. 2010.

[19] R. C. A. Naidu and P. S. Avadhani, "A comparison of data mining techniques for intrusion detection," in *IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT'12)*, pp. 41–44, Ramanathapuram, Aug. 2012.

[20] R. M. Needham, "Denial of service: an example?," *Communications of the ACM*, vol. 37, no. 11, pp. 42–46, 1994.

[21] NSL, *The NSL-KDD data set*, Sept. 27, 2015. (`http://nsl.cs.unb.ca/NSL-KDD/`)

[22] G. Paliouras and D. S. Bree, "The effect of numeric features on the scalability of inductive learning programs," in *Proceedings of the European Conference in Machine Learning*, pp. 218–231, Crete, Greece, Apr. 1995.

[23] M. Roesch and C. Green, *Snort User?s Manual 2.9.3: The Snort Project*, Technical Report 2.9.3, May 2012.

[24] S. V. Sandar and S. Shenai, "Economic denial of sustainability (EDOS) in cloud services using http and xml based ddos attacks," *International Journal of Computer Applications*, vol. 41, no. 20, pp. 11–16, 2012.

[25] Snort, *Snort Website*, Sept. 27, 2015. (`http://www.snort.org`)

[26] Tcpdump, *Tcpdump and libpcap*, Sept. 27, 2015. (`http://www.tcpdump.org/`)

[27] M. Xu, J. Li Wang, and T. Chen, "Improved decision tree algorithm: ID3+," in *Intelligent Computing in Signal Processing and Pattern Recognition Lecture Notes in Control and Information Sciences*, pp. 141–149, Crete, Greece, Aug. 2006.

[28] V. Yasami, S. Khorsandi, S. P. Mozaffari, and A. Jalalian, "An unsupervised network anomaly detection approach by k-means clustering & ID3 algorithms," in *IEEE Symposium on Computers and Communications*, pp. 398–403, Marrakech, July 2008.

[29] C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection," *Computers & Security*, vol. 29, no. 1, pp. 124–140, 2010.

Dinesh Singh is currently pursuing the Ph.D. degree in Computer Science and Engineering from Indian Institute of Technology Hyderabad, India. He received the M. Tech degree in Computer Engineering from the National Institute of Technology, Surat, India, in 2013. He received B. Tech degree from R. D. Engineering College Ghaziabad, India, in 2010. He joined the Department of Computer Science and Engineering, Parul Institute of Engineering and Technology Vadodara, India as an assistant professor from 2013 to 2014. His research interests include machine learning, big data analytics, visual computing, cloud computing, intrusion detection.

Dhiren Patel is currently a professor in Computer Engineering Department at NIT Surat, India. He leads Security and Cloud computing group at NIT Surat. His research interests include Information Security, Cloud Computing & Trust Management, Internet of Things and Green IT. Prof. Patel has academic and research associations with IIT Gandhinagar (Visiting Professor/Adjunct Professor), with University of Denver USA (Visiting Professor), with City University London (Visiting Scientist - Cyber Security), with British Telecom UK (Visiting Researcher - Cloud Security and Trust), and with C-DAC Mumbai (Research Advisor - Security and Critical Infrastructure Protection). He has authored a book on Information Security (published by Prentice Hall in 2008) and numerous research papers.

Bhavesh Borisaniya is currently pursuing PhD from the Department of Computer Engineering at National Institute of Technology, Surat, India. His research interests include security in cloud computing and virtualization, intrusion detection system, and honeypot.

Chirag Modi is currently working in Computer Science and Engineering at National Institute of Technology Goa. He holds Ph. D (2010-2014) and M. Tech (2008-2010) in Computer Engineering from National Institute of Technology, Surat. Dr. Modi's research interests include security, privacy, data mining and cloud computing with primary focus on intrusion detection in cloud computing and privacy preserving data mining. Apart from contributing in various internal conferences, workshops and training programs, Dr. Modi has published many papers in reputed SCI journals and international conference proceedings. He is an active researcher in Computer Science field, and acting as a TPC member, Editor and Reviewer in many reputed international conferences as well as journal. In addition, he is frequently delivering an expert talk at many institutes and also explores many research areas.

Threshold Signature Scheme without Using Polynomial Interpolation

Lein Harn[1] and Feng Wang[2]
(Corresponding author: Lein Harn)
Department of Computer Science Electrical Engineering, University of Missouri-Kansas City[1]
5110 Rockhill Road, Kansas City, MO 64110, USA
College of Mathematics and Physics, Fujian University of Technology[2]
Fuzhou, Fujian, 350118, China
(Email: harnl@umkc.edu)
(Received Sept. 16, 2014; revised and accepted Jan. 16 & Feb. 8, 2015)

Abstract

In a (t, n) secret sharing scheme (SS), the secret is shared among n shareholders in such a way that (a) with t or more than t shares can recover the secret, and (b) with fewer than t shares cannot obtain the secret. The threshold signature scheme is an application that extends the SS to a digital signature scheme. In a threshold signature scheme, any t or more than t group members can represent the group to generate a group signature; but fewer than t group members cannot generate a group signature. So far, most threshold signature schemes are based on the linear polynomial. In other words, these threshold signature schemes need to overcome the problem of polynomial interpolation. In this paper, we propose a threshold signature scheme based on the Chinese Remainder Theorem (CRT). We describe how to set up the system by a trusted group manager initially and generate pairs of public and private keys for group members. Since our proposed scheme is based on the CRT, there is no polynomial interpolation. The security of our proposed threshold signature scheme is based on the difficulty of solving the discrete logarithm problem.

Keywords: Chinese remainder theorem, polynomial interpolation, multisignature, threshold signature

1 Introduction

Secret Sharing Schemes (SSs) were originally introduced by both Blakley [3] and Shamir [27] independently in 1979 as a solution for safeguarding cryptographic keys and have been studied extensively in the literature. SS has become one of the most basic tools in cryptographic research. In Shamir's SS, a secret s is divided into n shares by a dealer and shares are sent to shareholders secretly. The secret s is shared among n shareholders in such a way that (a) with t or more than t shares can recover the secret, and (b) with fewer than t shares cannot obtain the secret. Shamir's (t, n) SS is based on a linear polynomial and is unconditionally secure. There are other types of threshold SSs, for example, Blakley's scheme [3] is based on the geometry, Mignotte's scheme [22] and Asmuth-Bloom's scheme [1] are based on the Chinese remainder theorem (CRT).

In an SS, the shares can be used for reconstructing the secret for only one time. This is because, in the secret reconstruction, the secret and shares are known to all participated shareholders. Therefore, the efficiency of the SS is very low. However, in a digital signature algorithm, the secret is the private key used for generating a digital signature. Since most digital signature schemes are based on some computation assumptions, the private key can be reused for generating multiple signatures. If the SS is extended to protect the private key of a digital signature scheme, the efficiency of the SS can be improved since the private key of a digital signature is protected based on some computational assumptions.

The threshold cryptography was first introduced by Desmedt in 1987 [5]. Desmedt and Frankel [6] have also proposed the first non-robust threshold signature scheme based on the ElGamal's signature [8]. In a threshold signature scheme, a group manager (GM) is responsible for selecting a pair of private and public keys for the group. The GM divides the group private key into multiple shares (i.e., private keys of members) and gives each share to each member secretly. Later, any t or more than t members can work together to generate a group signature; but, fewer than t members cannot generate a group signature. It is a natural generalization to use the SS in the design of a threshold signature scheme. So far, most threshold signature schemes are based on the linear polynomial. In Shamir's SS based on the linear polynomial, the polynomial interpolation needs to be performed in a field Z_p where p is a prime. Harn [13] proposed a robust threshold signature scheme based on a variation of ElGamal signa-

ture scheme. In Harn's scheme, a special modulus p is selected by the GM where $p-1$ contains a small prime factor q (i.e., $q|p-1$). A generator g with order q is used to compute all modular exponentiations. Under this arrangement, the polynomial interpolation of Shamir's SS can be performed in Z_q. Gennaro et al. [10] have proposed a robust threshold DSS [23] signature.

Desmedt and Frankel [6] have mentioned the difficulty of designing threshold signature schemes based on the RSA signature scheme [25]. The problem is caused by the fact that the polynomial interpolation is over the ring $Z_{\phi(n)}$ where n is the RSA modulus and $\phi(n)$ is the Euler toting function and is not a prime. Desmedt and Frankel [7] have proposed a non-robust threshold RSA signature. Later, De Santis et al. [26] proposed a variation of the Desmedt and Frankel's scheme [7]; but trades interaction for large share size. Both schemes [7, 26] avoid the problem of polynomial interpolation over $Z_{\phi(n)}$ by working instead with over $Z_{\phi(n)}\lfloor x \rfloor/\Phi_q(X)$ where $\Phi_q(X)$ is the qth cyclotomic polynomial and q is a prime. But, this design leads to a much more complicate scheme. Gennaro et al. [11] and Shoup [29] have proposed techniques to make threshold RSA signature scheme robust. There are other types of threshold signature schemes, including Elliptic curve-based [28] and Pairing-based [9] threshold signature schemes in the literature. Readers can refer to [14] for more information on the development of threshold signature schemes.

In this paper, we propose an approach to avoid the problem of polynomial interpolation. We adopt the SS based on the CRT in the design of a threshold signature. Most research papers in the subject of the SS are based on the linear polynomial; but only a few papers are based on the CRT. Polynomial and CRT are two different mathematical tools which can be used to implement a SS scheme. Both tools share many interesting properties. For example, the secret sharing homomorphism proposed by Benaloh [2] implies that the additive sum of shares generated by polynomials/CRTs is a share of additive sum of polynomials/CRTs. On the other hand, both tools are different in many aspects. For example, there is no polynomial interpolation in using CRT. Kaya and Selcuk [16] proposed the first CRT-based threshold decryptions. Later, they proposed a CRT-based threshold DSS signature [17]. But, their scheme needs $2t$ shares to generate a valid threshold signature and the signature generation is very complicate. In 2012, Guo and Chang [12] proposed a weighted threshold signature based on based on the work of Iftene [15], Kaya and Selcuk [16], and generalized Chinese remainder theorem [20]. Their scheme utilizes the cryptographic techniques of extended Asmuth-Bloom sequences [1] based on GCRT and the RSA threshold signature scheme [18]. However, Guo and Chang's scheme is not provable security because that RSA signature is not provable security [21]. In our proposed CRT-based threshold signature, it needs only t or more than t users to jointly generate the signature. Our scheme utilizes the cryptographic techniques of Mignotte's (t, n) threshold SS [22] and Harn's multisignature signature scheme [13]. The signature generation is almost the same as the polynomial-based threshold signatures. We describe how to set up the system by a trusted GM initially and generate pairs of public and private keys for group members. Since our proposed scheme is based on the CRT, there is no polynomial interpolation. The security of our proposed threshold signature scheme is based on the difficulty of solving the discrete logarithm problem.

The rest of this paper is organized as follows. In the next section, we introduce some preliminaries that include CRT, Mignotte's (t, n) threshold SS and a modified signature scheme and multisignature scheme used in our design. In Section 3, we introduce the model of our proposed scheme including entities, informal model and security properties. We propose a novel threshold signature scheme based on the CRT in Section 4. Security analysis and comparisons are included in Section 5. We conclude in Section 6.

2 Preliminaries

In this section, we provide fundamental background used in our design, including the CRT, the Mignotte's threshold SS [22] and Harn's multisignature scheme [13].

2.1 Chinese Remainder Theorem [4]

Given following system of equations as

$$\begin{aligned} x &= s_1 \bmod p_1; \\ x &= s_2 \bmod p_2; \\ &\vdots \\ x &= s_t \bmod p_t, \end{aligned}$$

there is one unique solution as $x = \sum_{i=1}^{t}(N/p_i)\cdot y_i \cdot s_i \bmod N$ where $(N/p_i)\cdot y_i \bmod p_i = 1$, and $N = p_1 \cdot p_2 \cdot \ldots \cdot p_t$, if all moduli are pairwise coprime (i.e., $\gcd(p_i, p_j) = 1$, for every $i \neq j$.)

2.2 Review of Mignotte's Threshold SS

We review Mignotte's threshold secret sharing scheme [22] as follows.

Share generation: A sequence of pairwise coprime positive integers, $p_1 < p_2 < \ldots < p_n$, where p_i is the public information associated with each shareholder, U_i. These public integers need to satisfy that $p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n < p_1 \cdot p_2 \cdot \ldots \cdot p_t$.

For this given sequence, the dealer chooses the secret s in the range,$R_t = \{s \in Z | p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n < s < p_1 \cdot p_2 \cdot \ldots \cdot p_t\}$. We call this range, the **t-threshold range**. Share for the shareholder, U_i, is generated as $s_i = s \bmod p_i$, $i = 1, 2, \ldots, n$. s_i is sent to shareholder, U_i secretly.

Remark 1. *The numbers in the t-threshold range, R_t, are integers upper bounded by $p_1 \cdot p_2 \cdot \ldots \cdot p_t$, which is the smallest product of any t moduli, and lower bounded*

by $p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n$, which is the largest product of any $t-1$ moduli. The secret, s, selected in this range can ensure that (a) the secret can be recovered with any t or more than t shares (i.e., the product of their moduli must be either equal to or larger than $p_1 \cdot p_2 \cdot \ldots \cdot p_t$), and (b) the secret cannot be obtained with fewer than t shares (i.e., the product of their moduli must be either equal to or smaller than $p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n$). Thus, the t-threshold range determines the threshold of a (t, n) threshold SS.

Secret reconstruction: Given t distinct shares, for example, $\{s_{i_1}, s_{i_2}, \cdots, s_{i_t}\}$, the secret s can be reconstructed by solving the following system of equations as

$$\begin{aligned} x &= s_{i_1} \bmod p_{i_1}; \\ x &= s_{i_2} \bmod p_{i_2}; \\ &\vdots \\ x &= s_{i_t} \bmod p_{i_t}. \end{aligned}$$

Using the standard CRT, a unique solution x is given as $x = \sum_{r=1}^{t} (N/p_{i_r}) \cdot y_{i_r} \cdot s_{i_r} \bmod N$, where $N = p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_t}$ and $(N/p_{i_r}) \cdot y_{i_r} \bmod p_{i_r} = 1$.

2.3 Review of Harn's Multisignature Signature Scheme

An efficient digital multisignature signature is proposed in [13]. This multisignature signature allows multiple signers to work together to generate a digital multisignature corresponding to a message. The length of multisignature signature is equivalent to the length of each individual signature.

In this section, we first introduce the modified ElGamal signature scheme used to construct the multisignature signature. We present a formal security proof of this modified scheme. The original ElGamal signature scheme [8] was proposed in 1985; but the security was never proved equivalent to the discrete logarithm problem. In 1996, Pointcheval and Stern [24] used the Forking lemma to prove the security of a slight variation of the original ElGamal signature scheme.

The modified ElGamal signature scheme used to construct a multisignature consists of 3 steps as follows:

- Let p be a large prime and g be a generator of Z_p, then the public key is $y = g^x \bmod p$ and the private key is x;
- The signer picks $k \in Z_{p-1}$ randomly and a cryptographic hash function h, the signature of message m is (r, s) where $r = g^k \bmod p$ and $s = x \cdot h(m, r) - k \cdot r \bmod p - 1$;
- The verification of the signature checks the equation $y^{h(m,r)} = r^r \cdot g^s \bmod p$.

We assume that hash function h behaves like a random oracle, and hence we follow the established cryptographic techniques, i.e., the Oracle Replay Attack and the Forking Lemma as proposed in [24], to prove the security of modified ElGamal signature scheme.

Theorem 1. *The modified ElGamal signature scheme is secure under the random oracle model against known-message attack and against adaptively chosen message attack.*

Proof. For a formal security proof, the hash function $h = h(m, r)$ in modified signature scheme will be treated as a random oracle. We use the method of reductionist proof to prove this Theorem. Suppose that there is an adversary A who can break this scheme, then we can construct an algorithm B that can solve the discrete logarithm problem with non-negligible probability in probabilistic polynomial time. It is to say that given (p, g, y) we can design an algorithm B to output x which satisfies $y = g^x \bmod p$. The algorithm B is described as follows.

Algorithm B sends (p, g, y) to an adversary A, and A requests some queries.

h-query: B maintains a list $L_1 = (m, r, h)$ and initializes it to empty. If A provides a pair (m, r) for h-query, B checks if (m, r) has it in the list L_1. If it is, returns the corresponding h; otherwise, B picks a random $h \in Z_{p-1}$ as a returned value, and adds (m, r, h) into list L_1.

Signature query: B maintains a list $L_2 = (m, r, h, s)$ and initializes it to empty. If A provides a message m for Signature query, B checks if m is in the list L_2. If it is, returns the corresponding (r, s) as m's signature; otherwise, B picks random integers $u, v \in Z_{p-1}$, and computes $r = g^u \cdot y^v \bmod p$, $h = v \cdot g^u \cdot y^v \bmod p - 1$, and $s = -u \cdot g^u \cdot y^v \bmod p - 1$, and checks whether (m, r) is in the list L_1. If it is, returns failure; else, returns the signature (r, s) and adds (m, r, h, s) into the list L_2, adds (m, r, h) into the list L_1. Note that the probability of failure is less than the number of times of requested h-queries and Signature queries divided by the length of hash value times two.

Adversary A outputs a valid signature (r_1, s_1) of the message, m_1, where m_1 is not requested on Signature query.

Using the Oracle Replay Attack and the Forking Lemma as proposed in [24], we can obtain another valid signature (r_1, s_1') of message, m_1. In detail, B resets A two times. In the first time, B records all the transcripts that interacted with A, and in the second time, B does the same thing as the first time except h-query. For instance, B picks a random numbers h_1 as the returned value for the first time and a different random numbers h_1' for the second time when A request h-query on (m_1, r_1). After two rounds of interacting with B, A outputs two valid signatures, (r_1, s_1) and (r_1, s_1') of the message m_1 with different hash values, h_1 and h_1'. Then, A sends (r_1, s_1) and (r_1, s_1')

to B. because both (r_1, s_1) and (r_1, s_1') are m_1's valid signature. So, B obtains $y^{h_1} = {r_1}^{r_1} \cdot g^{s_1} \bmod p$ and $y^{h_1'} = {r_1}^{r_1} \cdot g^{s_1'} \bmod p$. Thus, we have $y^{h_1'-h_1} = g^{s_1'-s_1} \bmod p$. If $\gcd(h_1' - h_1, p-1) = 1$, it is easy to compute the discrete logarithm of y as $x = (h_1' - h_1)^{-1} \bmod p - 1$. This result contradicts to the discrete logarithm assumption. Note that the probability of $\gcd(h_1' - h_1, p-1) = 1$, is big enough and can reach $1/2$ if we let $p = 2q + 1$ for some prime q.

In the following, we assume that there are two signers, A and B, with their private and public keys, (x_A, y_A) and (x_B, y_B) respectively, where $y_A = g^{x_A} \bmod p$ and $y_B = g^{x_B} \bmod p$. To digitally generate a valid multisignature (r, s), by A and B, according to [13], they compute $r_A = g^{k_A} \bmod p$ and $r_B = g^{k_B} \bmod p$, where k_A and k_B are random secrets selected by A and B, respectively from Z_{p-1}. r_A and r_B are exchanged with each other. Then, they compute $r = r_A \cdot r_B \bmod p$. With knowledge of their private keys, they can solve s_A and s_B satisfying $x_A \cdot h(m, r) = s_A + k_A \cdot r \bmod p - 1$ and $x_B \cdot h(m, r) = s_B + k_B \cdot r \bmod p - 1$, respectively. The multisignature of a message m is (r, s), where $s = s_A + s_B \bmod p - 1$. The multisignature can be verified by a verifier by checking whether $y^{h(m,r)} = r^r \cdot g^s \bmod p$. In the next section, we propose a threshold signature scheme based on this multisignature scheme to allow any t or more than t members to represent a group to generate a threshold signature.

There is a threshold signature scheme in [13] which integrates both Shamir's (t, n) SS and Harn's multisignature scheme. In fact, most existing threshold signature schemes are based on the linear polynomial. In the next section, we propose a novel approach to design a threshold signature scheme based on the CRT. We believe that our design opens a new direction to enable CRT-based SS to be integrated into other cryptographic functions. □

3 Models of Proposed Threshold Signature Scheme

3.1 Entities

In our proposed threshold scheme, there is a GM to register n members initially. The GM needs to select a pair of private and public keys of the group and divide the group private key into n shares. Each share will be sent to each member secretly. Later, any t or more than t members can work together to generate a group signature; but, fewer than t members cannot generate a group signature. Any verifier can use the group public key to verify the group signature.

3.2 Informal Model of Our Proposed Scheme

We assume that the GM selects a pair of private and public keys, (x, y), of the group and divides the group private key into n shares, $x_i, i = 1, 2, \ldots, n$, for members in the group, $U = \{U_1, U_2, \ldots, U_n\}$. Each member, U_i, will receive a share (i.e., private key), x_i, from the GM initially as his/her private key. In other words, the GM uses the Mignotte's (t, n) threshold SS to compute private keys, $(x_1, x_2, \ldots, x_n)$ for group members initially. The threshold signature generation, TSS, allows any t or more than t members to generate a group signature. The group signature can be verified according to the signature verification, VS, using the group public key. i.e.,

TSS: $(m, x_{i_1}, x_{i_2}, \ldots, x_{i_t}) \rightarrow$a group signature; where $\forall U_{i_r} \in U$;

VS: (m, a group signature, group public key)$\rightarrow$yes/no.

3.3 Properties

We propose a threshold signature scheme with the following properties:

Protection of private keys. Our scheme protects the secrecy of private keys of the group and members; otherwise, private keys can be used to generate only one group signature.

Unforgibility of group signature. Our scheme ensures that (a) any t or more than t members can work together to generate a valid group signature, and (b) fewer than t members cannot generate a valid group signature.

Fixed length of threshold signature. Our scheme ensures that the length of a threshold signature is fixed (i.e., not depending on the number of signers).

Efficiency of verification. The verification of a group signature is based on the group public key.

4 Proposed Threshold Signature Scheme

4.1 Outline of Our Design

In our proposed scheme, there is a trusted GM who is responsible for setting up the system initially. The GM needs to select public parameters and a pair of private and public keys of the group. The GM needs to register all members initially and follow the Mignotte's SS to divide the group private key into shares (private keys of members) and send a private key, x_i, for each member.

In the threshold signature generation, each group member needs to use his/her private key to generate an individual signature. The individual signature needs to be sent to a signature combiner. The signature combiner can be any participated member who is responsible to collect all individual signatures and produce a group signature. The signature combiner needs to verify each individual signature and then combine all individual signatures into a group signature.

4.2 Proposed Threshold Signature Scheme

Public and private key generation: The GM selects a sequence of pairwise coprime positive integers, $p_1 < p_2 < \ldots < p_n$, where p_i is the public information associated with member, U_i. These public integers need to satisfy that $p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n < p_1 \cdot p_2 \cdot \ldots \cdot p_t$. In addition, the GM selects a prime modulus, p, where integers in the set, $\{p_1, p_2, \ldots, p_n\}$, are divisors of $p-1$ (i.e., $p_1, p_2, \ldots, p_n | p-1$), a generator, g, of the subgroup of order $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ such that $1 < g < p$.

For this given sequence, the GM chooses the private key x of the group as an integer in the range $R_t = \{x \in Z | p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n < x < p_1 \cdot p_2 \cdot \ldots \cdot p_t\}$. The public key of the group is $y = g^x \bmod p$. Private key of the member, U_i, is generated as $x_i = x \bmod p_i$. The public key of the member, U_i, is computed as $y_i = g^{x_i} \bmod p$. x_i is sent to each member, U_i, secretly.

Remark 2. *Following steps are used to generate the generator g.*

1) $e = (p-1)/N$;
2) *Set α be any integer satisfying $1 < \alpha < p-1$, such that α differs from any value previously tried;*
3) $g = \alpha^e \bmod p$.;
4) *If $(g = 1)$, then go to step 2; otherwise return g.*

The following lemma proves the order of the generator.

Lemma 1. *For any nonnegative integer b if $g = \alpha^{(p-1)/N} \bmod p$, then $g^b = g^{b \bmod N} \bmod p$.*

Proof. From the Fermat theorem, since $\gcd(\alpha, p) = 1$, we have $\alpha^{p-1} \bmod p = 1$. Hence, for any nonnegative integer c, we have $g^{cN} \bmod p = (\alpha^{(p-1)/N})^{cN} \bmod p == (\alpha^{p-1})^c \bmod p = 1$. Thus, any nonnegative integer b can be represented as $b = dN + z$, where $0 < d, z < N$. Then,$g^b \bmod p = g^{dN+z} \bmod p == g^z \bmod p$. Since $z = b \bmod N$. we have proven this lemma. □

Threshold signature generation:

The proposed scheme allows any t or more than t members to represent the group to generate a group signature. Assume that members in the subset $U = \{U_{i_1}, U_{i_2}, \cdots, U_{i_t}\}$ want to generate a group signature for a message m. There are two parts involved in this phase.

Individual signature generation and verification.

Every member U_{i_v} randomly selects an integer $k_v \in Z_N$ and computes $r_v = g^{k_v} \bmod p$. r_v is made available to all other members in the subset U. After receiving all values, $r_v, v = 1, 2, \ldots, t$, every member U_{i_v} computes $r = (r_1 \cdot r_2 \cdot \ldots \cdot r_t)^{N \backslash N'} \bmod p$, where $N = (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$ and $N' = (p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_t})$. Then, every member U_{i_v} uses his/her private key, x_{i_v}, to generate a partial signature of the message m as $s_v = (N'/p_{i_v}) \cdot w_{i_v} \cdot x_{i_v} \cdot h(m, r) - k_v \cdot r \bmod N'$, where $(N'/p_{i_v}) \cdot w_{i_v} \bmod p_{i_v} = 1$. The individual signature, (r_v, s_v) of member U_{i_v} is sent to the signature combiner.

Once receiving the individual signature, (r_v, s_v), from member U_{i_v}, the signature combiner uses the public key, y_{i_v} of member U_{i_v} to verify whether $y_{i_v}^{(N/p_{i_v}) \cdot w_{i_v} \cdot h(m,r)} \stackrel{?}{=} g^{(N/N') \cdot s_v} \cdot r_v^{(N/N') \cdot r} \bmod p$. If it is, the individual signature has been successfully verified.

Theorem 2. *If $y_{i_v}^{(N/p_{i_v}) \cdot w_{i_v} \cdot h(m,r)} = g^{(N/N') \cdot s_v} \cdot r_v^{(N/N') \cdot r} \bmod p$, the individual signature has been verified successfully.*

Proof. With the knowledge of the secrets, x_{i_v} and k_v, member U_{i_v} is able to compute $s_v = (N'/p_{i_v}) \cdot w_{i_v} \cdot x_{i_v} \cdot h(m, r) - k_v \cdot r \bmod N'$, where $N' = p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_t}$. Since N' is a factor of N (i.e., $N' | N$), we have $g^{(N/N')}$ is a generator of the subgroup of order N'. Hence, we can get

$$\begin{aligned} y_{i_v}^{(N/p_{i_v}) \cdot w_{i_v} \cdot h(m,r)} &= (g^{(N/N')})^{(N'/p_{i_v}) \cdot x_{i_v} \cdot w_{i_v} \cdot h(m,r)} \\ &= (g^{(N/N')})^{s_v} \cdot (g^{(N/N')})^{k_v \cdot r} \\ &= g^{(N/N') \cdot s_v} \cdot r_v^{(N/N') \cdot r} \bmod p. \end{aligned}$$

□

Threshold signature generation. After all individual signatures, $(r_v, s_v), v = 1, 2, \ldots, t$, having been verified successfully, the threshold signature, (N', r, s) of the message m is computed as $s = (N/N') \cdot (\sum_{v=1}^{t} s_v \bmod N')$.

Threshold signature verification: Using the group public key, y, the threshold signature, (N', r, s) of the message m can be verified by first checking whether N is divisible by N' and then checking whether $y^{(N/N') \cdot h(m,r)} \stackrel{?}{=} g^s \cdot r^r \bmod p$. If it is, threshold signature has been successfully verified.

Theorem 3. *If N is divisible by N', and $y^{(N/N') \cdot h(m,r)} = g^s \cdot r^r \bmod p$, the threshold signature has been verified successfully.*

Proof. It is obvious that since $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ and $N' = p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_t}$. N is divisible by N'. In addition, since every individual signature, (r_v, s_v) satisfies $s_v = (N'/p_{i_v}) \cdot w_{i_v} \cdot x_{i_v} \cdot h(m, r) - k_v \cdot r \bmod N'$, the threshold signature s is $s = (N/N') \cdot (\sum_{v=1}^{t} s_v \bmod N') = (N/N') \cdot (\sum_{v=1}^{t} (N'/p_{i_v}) \cdot w_{i_v} \cdot x_{i_v} \cdot h(m, r) - k_v \cdot r \bmod N')$. According to the secret reconstruction in Mignotte's SS, we have

$$x = \sum_{v=1}^{t} (N'/p_{i_v}) \cdot w_{i_v} \cdot x_{i_v} \bmod N'.$$

Table 1: Comparison with other schemes

Scheme	**Kaya and Selcuk's scheme [17]**	**Guo and Chang's scheme [12]**	**Our scheme**
Players for generating (t, n) *signature*	$2t$	t	t
Whether or not provable security	Yes	No	Yes
Which signature scheme is based on	DSS	RSA	Harn's multisignature signature scheme [13]
Which secret sharing scheme is based on	Asmuth and Bloom's threshold SS [1]	Weighted threshold SS [15]	Mignotte's threshold SS [22]

Thus, we have

$$s = (N/N')\cdot(x\cdot h(m,r) - \sum_{v=1}^{t} k_v\cdot r \bmod N').$$

Hence, we can get

$$\begin{aligned} y^{(N/N')\cdot h(m,r)} &= g^s\cdot(g^{(N/N')})^{(r\cdot\sum_{v=1}^{t} k_v) mod N'} \bmod p \\ &= g^s\cdot(\prod_{v=1}^{t} r_v)^{(N/N')\cdot r} \bmod p \\ &= g^s\cdot r^r \bmod p. \end{aligned}$$

□

5 Security Analysis and Comparisons

In the following discussion, we analyze the properties described in Section 3.3 and compare our scheme with some other threshold schemes [12, 17].

Protection of private keys. Every member U_{i_v} needs to use his/her private key, x_{i_v} to generate an individual signature of the message m as $s_v = (N'/p_{i_v})\cdot w_{i_v}\cdot x_{i_v}\cdot h(m,r) - k_v\cdot r \bmod N'$. The private key, x_{i_v}, cannot be recovered by other members since there is one more secret, k_{i_v}, known only to the member, U_{i_v}.

Unforgibility of group signature. The private key, x, of the group is protected by the SS. It needs t or more than t members to recover the group private key. With fewer than t private keys cannot recover the group private key and therefore cannot generate a valid group signature.

Similar to [19, 30], we suppose that there is an adversary A who can corrupt at most $t-1$ members at the beginning of the signature. The adversary A adaptively chooses messages $m_1, m_2, \ldots, m_k$ for signature query, then the adversary A attempts to forge a valid signature for new message m. If there is no such adversary can successfully forge a valid signature for m with non-negligible probability, we say the threshold signature scheme unforgibility.

Theorem 4. *Our proposed threshold signature scheme is secure under the random oracle model against known-message attack and against adaptively chosen message attack.*

Proof. Suppose an adversary A with $t-1$ corrupted members can break the proposed threshold signature scheme. Without loss of generality, we assume that the corrupted members are $U_1, U_2, \ldots, U_{t-1}$. It is to say that the adversary A can forges a signature (N', r, s) of m which satisfies $y^{(N/N')\cdot h(m,r)} = r^r\cdot g^s \bmod p$. In fact, the adversary A cannot obtain the private key x from $t-1$ corrupted members because the private key is protected by the SS, and therefore cannot generate a signature (N', r, s) of m which satisfies $y^{(N/N')\cdot h(m,r)} = r^r\cdot g^s \bmod p$ without knowing private key x according to Theorem 1. Thus, the adversary A must use the $t-1$ private keys of corrupted members to compute the forged signature. In other words, the adversary generates the $t-1$ individual signatures (r_v, s_v) of m satisfying $y_{i_v}^{(N'/p_{i_v})\cdot w_{i_v}\cdot h(m,r)} = g^{(N/N')\cdot s_v}\cdot r_v^{(N/N')\cdot r} \bmod p$, for $v = 1, 2, \ldots, t-1$. Then, the adversary computes $s_t = s - \sum_{v=1}^{t-1} s_v \bmod N'$ and $r_t = r^{(N/N')^{-1} mod N'}\cdot(r_1\cdot r_2\cdot\ldots\cdot r_{t-1})^{-1} \bmod p$ without knowing the private key x_t. Obviously, (r_t, s_t) satisfies $y_t^{(N'/p_t)\cdot w_t\cdot h(m,r)} = g^{(N/N')\cdot s_t}\cdot r_t^{(N/N')\cdot r} \bmod p$; however, in a similar approach as used in proving Theorem 1, it is impossible since this result contradicts to the discrete logarithm assumption. □

Fixed length of threshold signature. The length of the threshold signature is identical to the length of an individual signature.

Efficiency of verification. Any verifier does not need to know the signers of a group signature. The group signature is verified using the public key of the group.

Next, we compare our scheme with some other threshold schemes [12, 17] which are based on the Chinese Remainder Theorem too. The result of comparisons is described in Table 1. Since RSA signature is not provable

security [21], the scheme [12] is not provable security because that the verification of scheme [12] is the same as RSA signature. Furthermore, we can use the existing message-signature pairs (M_1, s_1) and (M_2, s_2) to forge a new message-signature pairs $(M_1 \cdot M_2, s_1 \cdot s_2)$ [21] easily. Therefore, our scheme is more secure than scheme [12]. As for scheme [17], it needs $2t$ players to generate a (t, n) threshold signature. Therefore, our scheme is more efficient than scheme [17] because our scheme needs t players to generate a (t, n) threshold signature.

6 Conclusions

A threshold signature scheme is a useful tool to support the group-oriented application. The threshold signature enables t or more than t members to represent a group to generate a group signature; but, fewer than t group members cannot generate a group signature. Most existing threshold signature schemes are based on the linear polynomial. We propose a threshold signature scheme based on the CRT. By selecting parameters properly, the CRT-based SS can be applied in designing a threshold signature scheme. We believe that our design opens a new direction to enable CRT-based SS to be integrated into other cryptographic functions.

References

[1] C. A. Asmuth, J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. IT-29, no. 2, pp. 208–210, 1983.

[2] J. C. Benaloh, "Secret sharing homomorphisms: keeping shares of a secret," in *Proceedings of Advances in Cryptology (Crypto'86)*, LNCS 263, pp. 251–260, Springer, Aug. 1986.

[3] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of American Federation of Information Processing Society (AFIPS'79)*, pp. 313–317, New York, USA, June 1979.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory (Graduate Texts in Mathematics), Fourth ed.*, Springer-Verlag Press, 2000.

[5] Y. Desmedt, "Society and group oriented cryptography: a new concept," in *Proceedings of Advances in Cryptology (Crypto'87)*, LNCS 293, pp. 120–127, Springer, 1978.

[6] Y. Desmedt, Y. Frankel, "Threshold cryptosystems," in *Proceedings of Advances in Cryptology (Crypto'89)*, LNCS 435, pp. 307–315, Springer, Aug. 1989.

[7] Y. Desmedt, Y. Frankel, "Shared generation of authenticators and signatures," in *Proceedings of Advances in Cryptology (Crypto'91)*, LNCS 576, pp. 457–569, Springer, Aug. 1991.

[8] T. ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT- 31, no. 4, pp. 469–472, 1985.

[9] W. Gao, G. Wang, X. Wang, Z. Yang, "One-round ID-based threshold signature scheme from bilinear pairings," *Informatica*, vol. 20, pp. 461–476, 2009.

[10] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Robust threshold DSS signatures," in *Proceedings of Advances in Cryptology (Eurocrypt'96)*, LNCS 1070, pp. 354–371, Springer, May 1996.

[11] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Robust and efficient sharing of RSA functions," in *Proceedings of Advances in Cryptology (Crypto'96)*, LNCS 1109, pp. 157–172, Springer, Aug. 1996.

[12] C. Guo, C. C. Chang, "Proactive weighted threshold signature based on Generalized Chinese Remainder Theorem," *Journal of Electronic Science and Technology*, vol. 10, pp. 250–255, 2012.

[13] L. Harn, "Group-oriented (t,n) threshold digital signature scheme and digital multisignature," *IEE Proceedings of Computer Digital Technique*. vol. 141, pp. 307–313, 1994.

[14] M. S. Hwang, T. Y. Chang, "Threshold signatures: current status and key issues," *International Journal of Network Security*, vol. 1, pp. 123–137, 2005.

[15] S. Iftene, "General secret sharing based on the Chinese remainder theorem with applications in e-voting," *Electronic Notes in Theoretical Computer Science*, vol. 186, pp. 67–84, 2007.

[16] K. Kaya, A. A. Selcuk, "Threshold cryptography based on Asmuth-Bloom Secret sharing," *Information Sciences*, vol. 177, pp. 4148–4160, 2007.

[17] K. Kaya, A. A. Selcuk, "Sharing DSS by the Chinese Remainder Theorem," *Journal of Computational and Applied Mathematics*, vol. 259, pp. 495–502, 2014.

[18] K. Kaya, A. A. Selcuk, "Robust threshold schemes based on the Chinese remainder theorem," in *Proceedings of Advances in Cryptology (AFRICACRYPT'08)*, Casablanca, Morocco, 2008.

[19] S. Kim, J. Kim, J. H. Cheon, S. Ju, "Threshold signature schemes for ElGamal variants," *Computer Standards & Interfaces*, Vol. 33, pp. 432–437, 2011.

[20] Y. P. Lai, C. C. Chang, "Parallel Computation Alalgorithms for Generalized Chinese Remainder Theorem," *Computers and Electrical Engineering*, vol. 29, pp. 801–811, 2003.

[21] W. Mao, *Modern Cryptography: Theory and Practice*, Publishing House of Electronic Industry, Beijing, China, 2004.

[22] M. Mignotte, "How to share a secret," in *Proceedings of Cryptography-Proceedings of the Workshop on Cryptography*, LNCS 149, pp. 371–375, Springer, 1983.

[23] National Institute of Satndards and Technology (NIST), The digital signature standard proposed by NIST, 1992.

[24] D. Pointcheval, J. Stern, "Security proofs for signature schemes," in *Proceedings of Advances in Cryptology (Eurocrypt'96)*, LNCS 1070, pp. 387–98, Springer, May 1996.

[25] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of ACM*, vol. 21, pp. 120–126, 1978.
[26] A. De Santis, Y. Desmedt, Y. Frankel, M. Yung, "How to share a function securely," in *Proceedings of 26th Annual ACM Symposium on Theory of Computing (STOC'94)*, pp. 522–533, Canada, May 1994.
[27] A. Shamir, "How to share a secret," *Communications of ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[28] Y. Shang, X. Wang, Y. Li, Y. Zhang, "A general threshold signature scheme based on Elliptic Curve," in *Proceedings of the 2nd International Conference on Computer and Information Application (ICCIA'12)*, pp. 89–92, Taiyuan, Shanxi, China, Dec. 2012.
[29] V. Shoup, "Practical threshold signatures," in *Proceedings of Advances in Cryptology (Eurocrypt'00)*, LNCS 1807, pp. 207–220, Springer, May 2000.
[30] H. Xiong , Z. G. Qin, F.G. Li, "Identity-based Threshold Signature Secure in the Standard Model," *International Journal of Network Security*, Vol. 10, pp. 75–80, 2010.

Lein Harn received the B.S. degree in electrical engineering from the National Taiwan University in 1977, the M.S. degree in electrical engineering from the State University of New York-Stony Brook in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota in 1984. In 1984, he joined the Department of Electrical and Computer Engineering, University of Missouri- Columbia as an assistant professor, and in 1986, he moved to Computer Science and Telecommunication Program (CSTP), University of Missouri, Kansas City (UMKC). While at UMKC, he went on development leave to work in Racal Data Group, Florida for a year. Currently, he is a Professor at the Department of Computer Science Electrical Engineering, UMKC. His research interests include cryptography, network security, and wireless communication security. He has published a number of papers on digital signature design and applications and wireless and network Security. He has written two books on security. He is currently investigating new ways of using secret sharing in various applications.

Feng Wang was born in Shandong province, China, in 1978. He received his B.S. degree in Mathematics from Yantai Normal University (now named Ludong University), Yantai, in 2000 and the M.S. degree in Applied Mathematics from the Guangzhou University, Guangzhou, in 2006. Currently, he is a Lecturer in the College of Mathematics and Physics at Fujian University of Technology and a visiting scholar in Department of Information Engineering and Computer Science at Feng Chia University. His research interests include computer cryptography and information security.

A Reversible Data Hiding Scheme Based on Histogram Modification in Integer DWT Domain for BTC Compressed Images

Shun Zhang, Tiegang Gao, Liang Yang
(Corresponding author: Shun Zhang)

College of Software, Nankai University
Weijin Road 94#, Nankai District, Tianjin, China
(Email: shentengvip@gmail.com)
(Received May 30, 2014; revised and accepted Jan. 12 & Apr. 22, 2015)

Abstract

Reversible data hiding is an efficient way for embedding additional data into cover media, which can reversibly recover the original cover media when the additional data is extracted. It has been widely utilized in secure communication and copyright protection. A reversible data hiding scheme imposed on the quantized coefficients of compressed images based on block truncation coding (BTC) is proposed in this paper. Through rearranging the quantized coefficients of BTC images into matrix form, two sampled images are constructed. A histogram modification based reversible data hiding scheme in the integer discrete wavelet transform (integer DWT) domain is adopted on the constructed images. Additional data is embedded into the middle and high frequency sub-bands of the constructed image after integer DWT. Experimental results and analysis have demonstrated that, both higher embedding capacity and lower distortion have been achieved with the proposed scheme compared with existing reversible data hiding schemes for BTC compressed images.

Keywords: Reversible data hiding, Integer DWT, Histogram modification, Block Truncation Coding

1 Introduction

Data hiding is the process that embeds additional data into the cover media while causes distortion as little as possible to cover media. There are two main applications of data hiding. One is secure communication, which is always called steganography. It is considered much safer than traditional encryption, because it conceals the existence of secure communication. The other one is copyright protection and authentication for the cover media, which is often called digital watermarking. Reversible data hiding is the data hiding that can reversibly recover the original cover media after the additional data is extracted. Due to the reversibility, it can be used in a lager field, such as medical image surgery, military imagery, and remote sensing imagery and so on.

Many reversible data hiding schemes have been proposed in recent years [1, 3, 7, 8, 9, 14, 17, 18, 19, 20, 21, 22, 24]. There are there ways to achieve the reversibility. The first one is lossless compressing the cover image to make room for data hiding [7]. The second one is to expand the differences between adjacent pixels to embed the additional data [1, 20]. The last one is to shift the histogram of the cover media and to embed the additional data into the gap of the shifted histogram [3, 9, 14, 18, 19, 21, 22, 24]. Reversible data hiding based on compression makes use of the redundancy of cover image. Therefore, the characters of the cover image limit the capacity and quality of these schemes. Difference expansion based reversible data hiding scheme [20] hides one bit data by extending the difference between two neighbor pixels. And the embedding capacity is improved by extending n-1 pairs of neighbor pixel differences to hide n-1 bits information in [1]. However, the quality of the cover image drops quickly when the embedding capacity increases. Schemes based on histogram modification cause less distortion. However, the obvious drawback of histogram modification based schemes is that the embedding capacity is limited to the peak point of the histogram [18]. Two measures can be applied to increase the embedding capacity: raising the peak points height or increasing the number of peak points of the histogram. Many improved schemes based on the two measures were proposed. Lin et al. [14] adopted a multi-level embedding strategy to increase the capacity. Some prediction difference expansion based schemes were also proposed to generate the histogram for data hiding, which increased the height of the histogram. Tsai et al. [21] proposed a prediction model to get the prediction errors for the histogram modification, which explored the similarity of neighbor pixels. Kim et al. [9] sampled the original image

to get a predicted image based on the sampled images. The differences between the predicted image and these sampled images were calculated. Then the histograms of the difference images were generated for the data embedding. Recently, a reversible data hiding method based on histogram modification was proposed in [3]. It divided the cover image into the smooth blocks and complex blocks. Additional data was embedded into the smooth blocks for a higher embedding capacity and lower distortion. A reversible information hiding scheme suitable for embedding small amounts of data was proposed in [17]. It offered flexible embedding capacity and low overhead.

With the development of information technology, more and more multimedia is being produced. The image is one of the most important one. The storage and processing of the raw images are space consuming and resources consuming. Therefore, images are compressed before they are stored and processed in advance. The compression strategies include transformed domain methods and the spatial domain methods. The JPEG compression based on discrete cosine transform (DCT) and the JPEG2000 compression based on discrete wavelet transform (DWT) are transformed domain methods. The vector quantization (VQ) compression [15] and block truncation coding (BTC) compression [6, 11] are the spatial domain methods. Reversible data hiding for compressed images are sometimes of greater importance compared with reversible data hiding on the raw images. The first reversible watermarking scheme for JPEG compressed images was proposed in [7]. After that, a differential energy watermarking (DEW) algorithm for JPEG/MPEG streams, which embedded label bits by selectively discarding high frequency DCT coefficients in certain image regions, was proposed in [10].

BTC [6] compression is a block based lossy image compression technique. It represents the image with many quantized coefficients and one bitmap. Reversible data hiding schemes for BTC compressed images generally utilize the coefficients and the bitmap as the cover media. A genetic algorithm was adopted in [2] to generate an optimal common bitmap. The original three bitmaps of the colored BTC compressed images were replaced with the common bitmap. Additional data was embedded into the common bitmap and the orders of the quantized coefficients. An improved common bitmap was constructed in [5], which improved the embedding capacity. The difference expansion strategy was adopted in [4] to hide the secret data reversibly. Additional data was embedded into the BTC compressed image by swapping sequence of the high mean value and the low mean value in the compressed code in [12]. A histogram constructed from the bitmap of the BTC compressed images was shifted to embed additional data in [13]. The histogram shifting technique was also employed in [16] to embed the secret data into the quantization levels of the compressed codes. However, the embedding capacity is rare in [13, 16]. To increase the embedding capacity and reduce the distortion to the cover image, a well-designed histogram modification based reversible data hiding scheme for BTC compressed images is proposed in the followings.

The scheme utilizes the quantized coefficients of the BTC compressed images to achieve the reversible data hiding. The high mean values and low mean values of every block in the BTC compressed stream can construct two matrixes that are just like two sampled prediction image of the original image. Therefore, some traditional data hiding schemes can be utilized in the design of data hiding scheme for BTC compressed images. This paper imposes the integer DWT on the constructed images, and embeds additional data into the histograms of the middle and high frequency sub-bands in the integer DWT domain. The scheme has achieved high embedding capacity and low distortion in the experiments. Besides, compared with some existing schemes, better performances have been achieved with the proposed scheme.

The rest of the paper is organized as follows. Some related techniques are introduced in Section 2. The main algorithm is proposed in Section 3. Section 4 demonstrates the experimental results and the corresponding analysis, and Section 5 draws the conclusions.

2 Related Works

2.1 Absolute Movement Block Truncation Coding

Block Truncation Coding (BTC) is a simple and efficient way for lossy image compression. Different from those transform domain compression schemes, such as JPEG compression and JPEG 2000, BTC compression is imposed in the spatial domain. It is less time-consuming and more suitable for those real-time applications with low computational ability. The BTC compression transforms an image into a set with two vectors and one bitmap (H, L, BM), where H and L are two vectors with quantized high mean values and low mean values, and BM is a bitmap that indicates which quantized value should be selected in the compressed image. An improved image compression scheme based on BTC, which was called Absolute Movement Block Truncation Coding (AMBTC) was proposed in [11]. Similar to BTC, the AMBTC firstly blocks images into non-overlapping blocks with size$k \times k$. Then every block in the image is represented by a high mean value h, a low mean value l, and a bitmap bm. Suppose an image I with size $m \times n$ is blocked into $k \times k$ sized blocks. For every block $X_i = \{x_j, j = 1, 2, \cdots, k \times k\}, i = 1, 2, \cdots, (m \times n)/(k \times k)$, calculate the mean value:

$$\bar{x}_i = \frac{1}{k \times k} \sum_{j=1}^{k \times k} x_j, \tag{1}$$

where x_j is the j^{th} pixel of the block. Then the low mean value l_i and high mean value h_i are calculated with:

$$l_i = \frac{1}{k \times k - q} \times \sum_{x_j < \bar{x}_i} x_j, \quad (2)$$

$$h_i = \frac{1}{q} \times \sum_{x_j \geq \bar{x}_i} x_j, \quad (3)$$

where q is the number of pixels greater or equal to the mean value $\bar{x}_i$ of the block. Then the bitmap of the block bm_i is calculated with:

$$bm_i = \left\{ \begin{array}{ll} 1 & \text{if } x_j \geq \bar{x}_i \\ 0 & \text{otherwise} \end{array} \right\} \quad (4)$$

Finally, block X_i is represented with (h_i, l_i, bm_i), and all the blocks constitutes the set (H, L, BM). When decompressing the compressed image, every 1 in the bitmap bm_i is replaced by the grey value h_i and every 0 in the bitmap bm_i is replaced by the grey value l_i. An example that compresses one block from image Lena is presented in Figure 1. The block is extracted from pixel values of $(128 : 131, 128 : 131)$ in the standard Lena image. In Figure 1, (a) is the original image block; (b) is the bitmap of the block; (c) is the reconstructed compressed block.

2.2 Reversible Data Hiding in Integer-DWT Domain Based on Histogram Modification

The reversible data hiding scheme proposed in [23] embeds data in the integer-DWT domain, which has achieved both high data embedding capacity and low distortion to the cover image. The histograms of the middle and high frequency sub-bands (LH, HL, HH) after integer DWT are of Laplacian-like distributions [24], which is beneficial to histogram modification based data hiding. Therefore, they are shifted to generate the gap for data hiding. The structure of the image Lena is presented in Figure 2. An example of the histogram modification based data hiding method, which embeds data into the LH sub-bands of the constructed image, is presented in Figure 3. The generated histogram of sub-band LH is depicted in Figure 3 (a). Then the histogram is shifted to both sides by an embedding strength (Figure 3 (b)). At last, data is embedded by expanding the histogram between and, and the histogram after embedding is as Figure 3 (c).

2.2.1 Reversible data embedding

The histograms of LH, HL, HH sub-bands are generated and data is embedded into the coefficients by histogram modification as presented in Figure 3. For every coefficient in the sub-bands, given an embedding strength parameter q. If $C \geq q$, then C is shifted to $C + q$; else if $C \leq -q$, then C is shifted to $C - q + 1$; else $C \leftarrow 2 \times C + B$, where B is the data to be embedded. The embedding strength parameter q is encoded as the key for data extraction.

2.2.2 Data extraction and reversible recovery of the matrix before embedding

Generate the histograms of middle and high frequency sub-bands and shift these histograms to extract the hidden data. The original coefficients matrixes are reversibly recovered with the following steps. For every coefficient C of LH, HL, HH sub-bands, given an embedding strength parameter q. If $C \geq 2 \times q$, then C is shifted to $C - q$; else if $C \leq -2 \times q + 1$, then C is shifted to $C + q - 1$; else $C \leftarrow floor(C/2)$, and data is extracted: $B = \mathrm{mod}(C, 2)$. All the coefficients of sub-bands LH, HL, HH are reversibly recovered and the extracted B is the data embedded before.

3 Proposed scheme

The BTC compression divides the original image into blocks, and then quantizes the blocks into the high mean values and the low mean values and a bitmap that indicates the quantized values. The quantized high mean values and low mean values of the blocks just construct two sampled images, which are utilized for reversible data hiding. The original image Lena and the sampled image constructed with its high mean values and low mean values after BTC compression are presented in Figure 4. The block size is. Sub-image (a) is the original image Lena with size 512×512; sub-image (b) is the constructed image from the high mean values; and sub-image (c) is the constructed image from the low mean values. Obviously, the size of the two constructed image is 128×128.

The two constructed images is similar to the original image only with a smaller size according to the human visual system. Therefore, traditional reversible data hiding schemes can also be utilized on the constructed images to achieve the reversible data hiding on the BTC compressed images. The efficient reversible data hiding scheme based on the histogram modification in the integer DWT domain is imposed on the constructed images. Suppose the original image I with size $m \times n$ is compressed for the reversible data hiding. Detailed steps of the reversible data hiding scheme for BTC compressed images are as follows:

1) Divide I into $k \times k$ sized blocks $X = \{X_i, i = 1, 2, \cdots, (m \times n)/(k \times k)\}$;

2) Calculate the coefficients of compressed image (H, L, BM) with method given in Section 2.1, where H and L are vectors with size $(1, (m \times n)/(k \times k))$, BM is a binary matrix with size (m, n);

3) Construct the sampled images, denoted as I_h and I_l, respectively with the high mean values vector H and the low mean values vector L;

4) Impose the integer DWT on I_h and I_l to get the four sub-bands LL, LH, HL, HH for data hiding;

192	187	162	162
195	173	172	171
188	171	170	150
185	184	159	140

(a) Original

1	1	0	0
1	1	0	0
1	0	0	0
1	1	0	0

(b) Bitmap

186	186	162	162
186	186	162	162
186	162	162	162
186	186	162	162

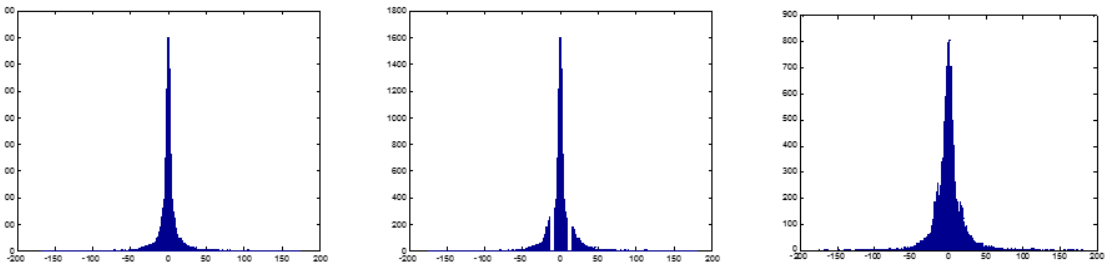
(c) Compressed

Figure 1: An example of AMBTC compression

LL	LH
HL	HH

(a) Image 'Lena' after one level integer DWT (b) The structure of the sub-bands of DWT

Figure 2: Structure of the image Lena after one level integer DWT



(a) Original (b) Shifted (c) Embedded

Figure 3: An example of histogram modification and data hiding process

5) Select the LH, HL, HH sub-bands of I_h and I_l after integer DWT to embed data with the method proposed in Section 2.2.1;

6) Impose inverse integer DWT on the corresponding sub-bands to get the $I_h{}'$ and $I_l{}'$ that contains hidden data;

7) Scan $I_h{}'$ and $I_l{}'$ to reconstruct the coefficients vectors H' and L', and then (H', L', BM) is the BTC compressed image with hidden data. In fact, the LL sub-bands after integer DWT can also be utilized for the data hiding, which may increase the embedding capacity. In the receiving end, with the encoded (H', L', BM), the compressed image with hidden data is decoded. Besides, the hidden data is extracted, and the original BTC compressed image is reversibly recovered.

The data extraction process is the inverse process of data hiding. Detailed steps for extracting the hidden data and reversible recovery of the original BTC compressed image are presented as follows.

1) Construct the sampled image with hidden data $I_h{}'$ and $I_l{}'$ by scanning the coefficients vectors H' and L';

2) Impose the integer DWT on the $I_h{}'$ and $I_l{}'$ to get the four sub-bands LL, LH, HL, HH;

3) Extract the hidden data from the four sub-bands of $I_h{}'$ and $I_l{}'$, and then recover LL, LH, HL, HH with method proposed in Section 2.2.2;

4) Impose the inverse integer DWT on the four recovered sub-bands to get the recovered I_h and I_l;

5) Reconstruct the quantized coefficients vectors H and L, and then the (H, L, BM) is recovered.

The additional data is hidden into the quantized vectors through histogram modification operated on the integer DWT domain. The bit map remains unchanged throughout the data hiding and extraction processes. In fact, the bitmap can also be incorporated for the data hiding, which will increase the embedding capacity further. Besides, the arrangements between the high mean values and low mean values can be utilized to present some data, which will also increase the embedding capacity.

4 Experiments

The proposed scheme has been imposed on different images to testify the validity. The standard images selected from the USC-SIPI image database are adopted for the demonstration. Random bit streams are embedded into these images as the hidden data. All the experiments are performed on the MATLAB 2012a running on a personal computer with CPU of AMD Phenom (tm) X4 810 Processor 2.6GHz, memory of 4 GB, and the operating system of Windows 7 x64 Ultimate Edition.

The original image Peppers, the image after BTC compression and the BTC compressed image with hidden data are presented in Figure 5 respectively.

The blocking strategy with different sizes in the BTC compression produces different quantized coefficients vectors. Therefore, different sampled images with different sizes are constructed, which affect the embedding capacity. The distortion caused to the BTC compressed images can be measured by the peak signal-to-noise ratio (PSNR), which is calculated as follows:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}(dB), \tag{5}$$

where

$$MSE = \frac{1}{N_1 \times N_2} \sum_{1}^{N_1} \sum_{1}^{N_2} (I_{i,j} - I'_{i,j}). \tag{6}$$

Different images with different BTC compression parameters and different embedding strength parameters are tested. Detailed data is presented in the following figures. The embedding capacity and PSNR of images that are compressed by BTC with block size 2×2 are presented in Figure 6. The horizontal axes represents different embedding strength parameters, while the vertical axes represents the embedding capacity and PSNR respectively in plot (a) and plot (b). The embedding capacity and PSNR of images that are compressed by BTC with block size 4×4 are presented in Figure 7. The horizontal axes represents different embedding strength parameters, while the vertical axes represents the embedding capacity and PSNR respectively in plot (a) and plot (b). The embedding capacity and PSNR of images that are compressed by BTC with block size 8×8 are presented in Figure 8. The horizontal axes represents different embedding strength parameters, while the vertical axes represents the embedding capacity and PSNR respectively in plot (a) and plot (b).

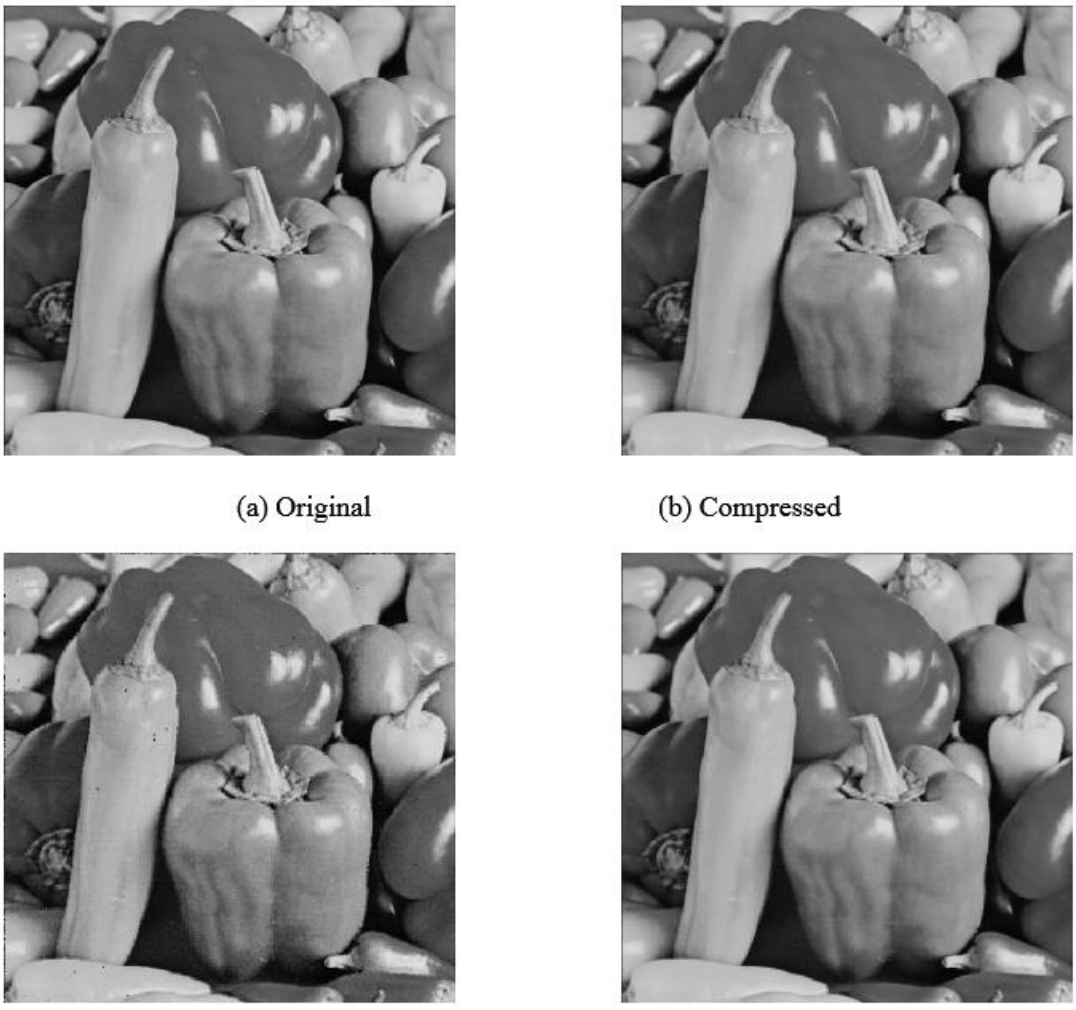
It is clear that, the embedding capacity increases when the embedding strength increases. However, the PSNR decreases at the same time. The embedding capacity decreases when the block size in the BTC compression increases. That is because the constructed images become smaller when the block size become bigger. Moreover, there will be less pixels left for hiding additional data. Embedding data into the constructed images will enlarge the distortion caused to the compressed images in some degree. Larger blocks are easier to be affected because more pixels will be changed when the same amount of pixels are modified in the constructed image.

Comparisons with existing schemes are presented in Table 1. The embedding strength parameters are $q = 8$ and $q = 2$ respectively in the tow comparisons. The block size of BTC compression is 4×4.

As can be seen in the Table 1, better performances are got with the proposed scheme. In fact, more data can be

(a) Original (b) Constructed with high mean values (c) Constructed with low mean values

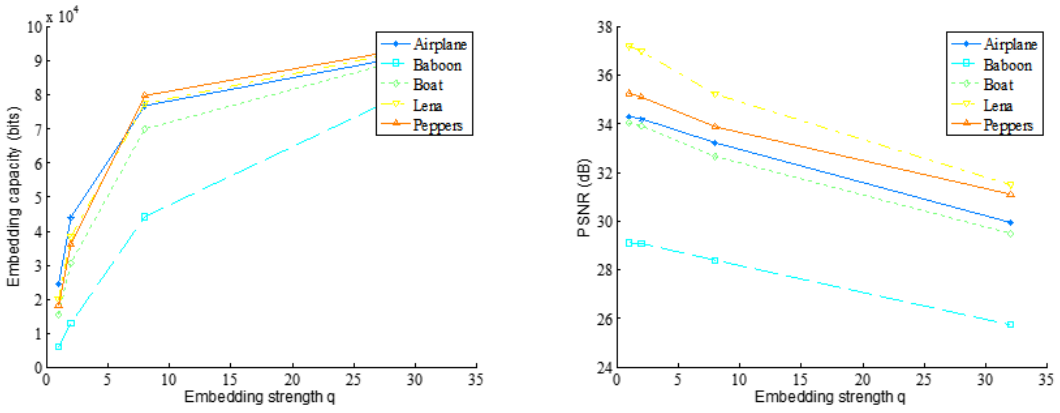
Figure 4: Lena image and it constructed sampled images



(a) Original (b) Compressed

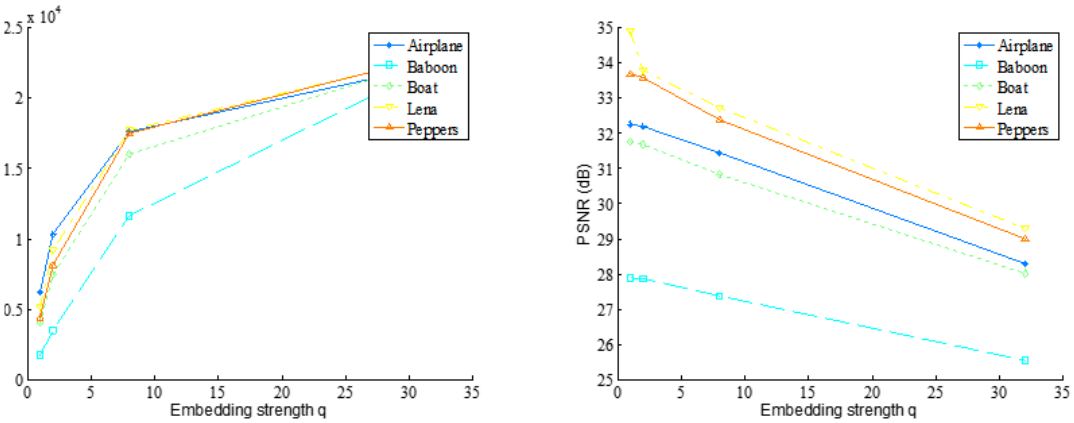
(c) Embedded (d) Recovered

Figure 5: Lena image and it constructed sampled images



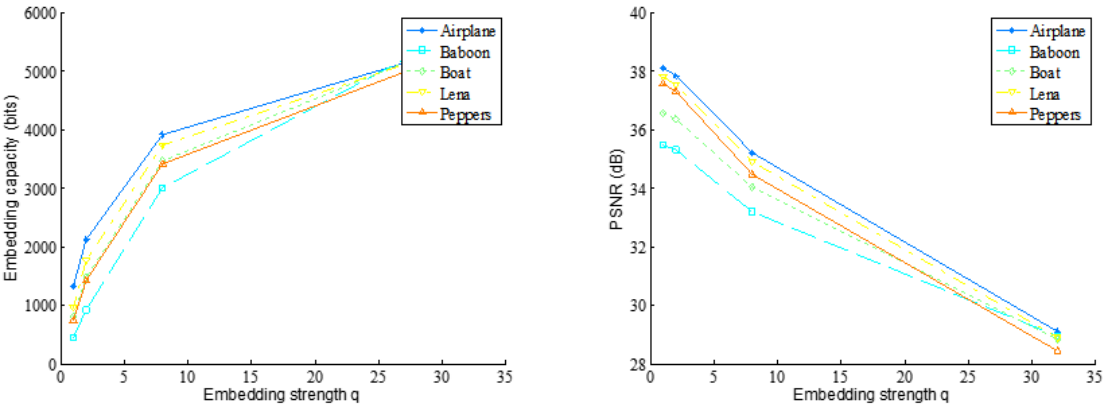
(a) Embedding capacity (b) PSNR

Figure 6: Embedding results with BTC block size 2×2



(a) Embedding capacity (b) PSNR

Figure 7: Embedding results with BTC block size 4×4



(a) Embedding capacity (b) PSNR

Figure 8: Embedding results with BTC block size 8×8

Table 1: Comparison with existing schemes

Image	Proposed with $q=8$		Li et al. [12]		Proposed with $q=2$		Lo et al. [16]	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Airplane	17600	31.4257	17375	31.033	10349	32.1805	7073	32.914
Baboon	11626	27.3667	-	-	3458	27.8537	-	-
Boat	16008	30.8236	17061	31.151	7418	31.6798	5387	31.751
Lena	17705	32.7076	16684	32.041	9174	33.7687	4025	33.364
Peppers	17487	32.3810	21969	31.595	8093	33.5590	4882	33.873

embedded into the BTC compressed images with higher embedding strength. The PSNR will decrease along with the embedding capacity increase, of course. Besides, the embedding strength can be decided adaptively according to the features of the cover media and the need of the actual applications. Different block sizes can be adopted in the process of BTC compression. The proposed scheme can achieve higher embedding capacity and cause lower distortion when a smaller block size is selected, which can be seen from Figure 6, Figure 7 and Figure 8. For example, if the block size in the BTC compression is 2×2, better results are got in Table 2. The embedding strength $q=8$ in the experiments.

The reversible data hiding scheme adopted in the proposed scheme has larger embedding capacity compared with similar histogram modification based reversible hiding schemes. Besides, the histogram modification schemes imposed on the constructed images has better performance itself, compared with those data hiding schemes based on the bitmap, or on the pattern of the low mean vectors and high mean vectors in the BTC compressed images. The proposed scheme will never change the sizes of the BTC compressed images. Therefore, it keeps the compression rate of the original BTC compressed image, which will never reveal the existence of additional data.

5 Conclusion

A reversible data hiding scheme for BTC compressed images is proposed in this paper. Based on the high mean values and low values in the BTC compression, we constructed two sampled images for the data hiding process. A histogram modification based scheme in the integer DWT domain is utilized to achieve the high embedding capacity and low distortion. Through the proposed construction method of sampled images, traditional reversible data hiding schemes can be adjusted to realize the data hiding on the BTC compressed images. Besides, some other data hiding strategies were also mentioned in the paper to further improve the performances of the scheme.

Acknowledgments

The work described in this paper was supported by the Key program of National Science Fund of Tianjin, China (Grant NO. 11JCZDJC16000). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147–1156, 2004.

[2] C. C. Chang, C. Y. Lin, and Yi H. Fan, "Lossless data hiding for color images based on block truncation coding," *Pattern Recognition*, vol. 41, no. 7, pp. 2347–2357, 2008.

[3] C. C. Chang, T. S. Nguyen, and C. C. Lin, "Reversible image hiding for high image quality based on histogram shifting and local complexity," *International Journal of Network Security*, vol. 16, no. 3, pp. 208–220, 2014.

[4] Z. F. Chen, Yu X. Su, and Z. M. Lu, "Reversible data hiding for btc-compressed color images using difference expansion," *ICIC Express Letters, Part B: Applications*, vol. 2, no. 5, pp. 1213–1218, 2011.

[5] Y. C. Chou and H. H. Chang, "A high payload data hiding scheme for color image based on btc compression technique," in *Proceedings of 4th IEEE International Conference on Genetic and Evolutionary Computing (ICGEC'10)*, pp. 626–629, 2010.

[6] E. J. Delp and O. R. Mitchell, "Image compression using block truncation coding," *IEEE Transactions on Communications*, vol. 27, no. 9, pp. 1335–1342, 1979.

Table 2: Optimized comparison with existing schemes

Image	Li et al. [12]		Proposed		Lo et al. [16]	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Airplane	17375	31.033	76678	33.2088	7073	32.914
Baboon	-	-	44204	28.3893	-	-
Boat	17061	31.151	69998	32.6636	5387	31.751
Lena	16684	32.041	77337	35.2198	4025	33.364
Peppers	21969	31.595	79575	33.8742	4882	33.873

[7] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for jpeg images," in *Proceedings of IEEE International Conference on Information Technology: Coding and Computing*, pp. 223–227, 2001.

[8] Li C. Huang, L. Yu Tseng, and M. S. Hwang, "The study on data hiding in medical images," *International Journal of Network Security*, vol. 14, no. 6, pp. 301–309, 2012.

[9] K. Su Kim, M. J. Lee, H. Y. Lee, and H. K. Lee, "Reversible data hiding exploiting spatial correlation between sub-sampled images," *Pattern Recognition*, vol. 42, no. 11, pp. 3083–3096, 2009.

[10] G. C. Langelaar and R. L. Lagendijk, "Optimal differential energy watermarking of dct encoded images and video," *Ieee Transactions on Image Processing*, vol. 10, no. 1, pp. 148–158, 2001.

[11] M. Lema and O. R. Mitchell, "Absolute moment block truncation coding and its application to color images," *IEEE Transactions on Communications*, vol. 32, no. 10, pp. 1148–1157, 1984.

[12] C. H. Li, Z. M. Lu, and Yu X. Su, "Reversible data hiding for btc-compressed images based on bit-plane flipping and histogram shifting of mean tables," *Information Technology Journal*, vol. 10, no. 7, pp. 1421–1426, 2011.

[13] C. C. Lin and X. L. Liu, "A reversible data hiding scheme for block truncation compressions based on histogram modification," in *International Conference on Genetic and Evolutionary Computing*, pp. 157–160, 2012.

[14] C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recognition*, vol. 41, no. 12, pp. 3582–3591, 2008.

[15] Y. Linde, A. Buzo, and R. M. Gray, "An algorithm for vector quantizer design," *IEEE Transactions on Communications*, vol. 28, no. 1, pp. 84–95, 1980.

[16] C. C. Lo, Yu C. Hu, Wu L. Chen, and C. M. Wu, "Reversible data hiding scheme for btc-compressed images based on histogram shifting," *International Journal of Security and its Applications*, vol. 8, no. 2, pp. 301–314, 2014.

[17] Q. Mao, C. C. Chang, and T. F. Chung, "A reversible steganography suitable for embedding small amounts of data," *International Journal of Network Security*, vol. 16, no. 4, pp. 295–303, 2014.

[18] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," in *Proceedings of the 2003 IEEE International Symposium on Circuits and Systems (ISCAS'03)*, vol. 2, pp. II-912–II-915, 2003.

[19] W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 6, pp. 906–910, 2009.

[20] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[21] P. Tsai, Yu C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, vol. 89, no. 6, pp. 1129–1143, 2009.

[22] C. H. Yang and M. H. Tsai, "Improving histogram-based reversible data hiding by interleaving predictions," *IET Image Processing*, vol. 4, no. 4, pp. 223–234, 2010.

[23] S. Zhang, T. Gao, and G. Sheng, "A joint encryption and reversible data hiding scheme based on integer-dwt and arnold map permutation," *Journal of Applied Mathematics*, vol. 2014, pp. 12, 2014.

[24] Z. Zhao, H. Luo, Z. M. Lu, and J. S. Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery," *International Journal of Electronics and Communications*, vol. 65, no. 10, pp. 814–826, 2011.

Shun Zhang born in 1986, is a Ph.D. candidate in in College of Software, Nankai University, China. His current research interests include watermarking, reversible data hiding, and multi-media security.

Tiegang Gao is a Prof. in College of Software, Nankai

University, China since 2006. His current research interests include information security, multimedia information processing and software engineering.

Liang Yang born in 1992, is a M.S. candidate in in College of Software, Nankai University, China. His current research interests include information security, reversible data hiding, and multimedia security.

An Improved Anonymous Buyer-Reseller Watermarking Protocol

Fuh-Gwo Jeng[1], Jyun-Ci Huang[2], and Tzung-Her Chen[2]
(Corresponding author: Tzung-Her Chen)

Department of Applied Mathematics, National Chiayi University[1]
Department of Computer Science and Information Engineering, National Chiayi University[2]
300 University Rd., Chia-Yi City, Taiwan 60004, R.O.C.
(Email: thchen@mail.ncyu.edu.tw)
(Received June 17, 2014; revised and accepted Jan. 16 & Apr. 2, 2015)

Abstract

Although digital watermarking protocols have been studied extensively for achieving copyright protection over the Internet for many years, the new issue of second-hand watermarking protocols has been largely ignored. Cheung and Curreem first proposed a buyer-reseller watermarking protocol for digital content redistribution in the second-hand markets. Later, Chen et al. showed that Cheung and Curreem's scheme is vulnerable to malicious attacks and further proposed a simple improvement. However, in this paper, we show that the aforementioned schemes are still insecure, specifically by seller cheating problems, and propose an improved one. Moreover, the proposed scheme accounts for requirements of anonymity, unlinkability, coalition-resistance, and traitor traceability.
Keywords: Buyer-reseller, copyright protection, digital watermarking, second-hand market, watermarking protocol

1 Introduction

As life becomes more digitalized, large amounts of text, images, audio or video are digitalized and, thus, on-line transaction has drawn much attention [21]. To protect these digital contents, digital watermarking [6, 14, 15, 17] and digital watermarking protocols [13] have been proposed for solving the copyright protection problem.

Almost all proposed watermarking protocols focus on first-hand markets [2, 3, 7, 9, 10, 11, 12, 13, 16, 19]. The watermarking protocols for securing transactions of digital contents in a second-hand market have been afforded less effort despite the high potential for financial returns. There are several reasons why industry is so profitable.

First, buyers are willing to purchase second-hand digital contents because of lower prices and identical quality. Second, the second-hand environment welcomes resellers. Third, sellers are willing to accept the market discipline and join the second-hand market if they can benefit sufficiently from transactions.

The key difference between a traditional second-hand market and the digital second-hand market is whether or not the reseller can keep a copy. In a traditional second-hand market, if the reseller sells the content, (s)he no longer owns the content anymore. However, in a digital second-hand market, if the reseller sells the content, (s)he may still have a private copy. Then, (s)he may have the opportunity to redistribute the copy. Therefore, in a second-hand market for digital content, we not only need to consider the rights and illegal redistribution between the seller and the buyer, but also the reseller.

Taking second-hand scenarios into account, the following requirements must be met:

Asymmetry: In a secure watermarking protocol, the buyer is the only one who is both aware of and also possesses the watermarked digital content. Therefore, if an illegal copy is found, the seller can trace the identity of the buyer who distributed the copy and prove to the judge that the buyer is guilty of illegal distribution. On the other hand, the buyer cannot deny charge by claiming that the unauthorized copy was distributed by the seller, or the reseller.

Anonymity: If requested, the identity of a buyer should not be exposed unless (s)he is confirmed to be an illegal distributor.

Malicious insiders (seller, buyer and reseller): A malicious insider may intend to benefit from reselling unauthorized copies by means of the following cases.

1) If the seller intends to cheat a buyer, (s)he may distribute a watermarked copy that has already been sold to the buyer.
2) The reseller may intend to benefit from reselling unauthorized copies.

Table 1: The notations used in this paper

B, S, R, CA, J:	A buyer, seller, reseller, watermark certification authority and the judge, respectively;
ID_B:	Identity of **B**;
$X' = X \oplus W$:	Embeds watermark W into original content X to form watermarked content X';
V_B, V_R:	The watermarks indicating the transactions from the buyer and reseller;
B $\rightarrow$ **S**: M:	**B** delivers message M to **S**;
$E_k(.), D_s(\cdot)$:	The encryption function with the public key k and decryption function with the private key s;
$H(\cdot)$:	A one-way hash function;
$Sign_s(M)$:	Digital signature of message M signed by the private key s.

3) The buyer may claim that the unauthorized copy was resold by the seller, or the reseller.

Unlinkability: Sellers and resellers cannot determine whether any two transactions belong to the same buyer or not.

Coalition resistance: Two or more buyers cannot cooperate to obtain another buyer's transaction information.

Traitor traceability: When a pirated copy is found, it must be easy to distinguish who is the traitor.

Inspired by Memon and Wong's scheme, Cheung and Curreem [5] proposed a buyer-reseller watermarking protocol (hereby shortened to CC) for digital contents redistributing in digital second-hand market. Later, Chen et al. [4] showed that the CC scheme is still susceptible to seller cheating and reseller cheating problems. Chen et al. then proposed an improved one (hereby shortened to CHT) with anonymity.

In this paper, we will show that both of the CC and the CHT schemes, which violate the asymmetry requirement, are not immune to the seller cheating problem and an enhanced one is proposed. Thanks to the tool of commutative cryptosystem, the reseller's watermarked content can be encrypted before transmitting to the seller. In this way, the seller is not aware of the reseller's watermarked content and the seller cheating problem can be solved. Naturally, the proposed protocol also satisfies all above precautionary requirements.

2 Review and Security Analysis of the CC and the CHT Schemes

In this section, the CHT scheme is briefly reviewed while the CC scheme is similar and, thus, omitted. Table 1 gives the notations used through this paper.

To begin with, the kernel technique of watermarking protocol should be mentioned. Memon and Wong's watermarking protocol adopts a public key cryptosystem that is a privacy homomorphism with respect to the watermark insertion operator. Here, the watermark insertion operation is $X \oplus W = \{x1 \oplus w1, x2 \oplus w2, \cdots, xm \oplus wm, xm+1 \oplus wm+1, \cdots, xn \oplus wn\}$ and $\oplus$ is a privacy homomorphism with respect to a binary operator for the public-key cryptosystem. It is well-know that the RSA cryptosystem is a privacy homomorphism with respect to multiplication. Precisely, $Ek(a \oplus b) = Ek(a) \oplus Ek(b)$ is hold where a and b are in the message space. A specific construction by combining the well-known spread-spectrum watermarking technique proposed by Cox et al. [6] and the RSA cryptosystem is given in [13] with respect to multiplication.

2.1 Review of the CHT Scheme

2.1.1 Registration Protocol

The buyer **B** asks for a temporary transaction key pair from **CA**. **CA** generates a short-term key pair (pk_B^*, sk_B^*) and a watermark W for **B**. Then **CA** sends them to the buyer securely.

1) **B** $\rightarrow$ **CA:** A certificate of **B**'s identity including the public key pk_B.
CA verifies the validation of **B**'s identity and pk_B by checking the certificate.

2) **CA** $\rightarrow$ **B:** $E_{pk_B}((pk_B^*, sk_B^*), E_{pk_B^*}(W), Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*))$.
CA generates a watermark W and the temporary key pair (pk_B^*, sk_B^*), and computes $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$ and $E_{pk_B}((pk_B^*, sk_B^*), E_{pk_B^*}(W), Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*))$ where sk_{CA} is CA's private key.

3) **B** decrypts the received message and checks the validity of $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$. **CA** also stores ID_B and pk_B^* in the table.

2.1.2 Watermark Insertion Protocol

The reseller **R** may designate a transaction proxy, for example an auction web site, and the buyer directly communicates with the transaction proxy via the Internet.

1) **B** → **R:** $E_{pk_B^*}(W), pk_B^*, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$.
The buyer **B** sends the message $\{E_{pk_B^*}(W),\ pk_B^*,\ Sign_{sk_{CA}}(E_{pk_B^*}(W),\ pk_B^*)\}$ to the reseller **R**.

2) **R** → **S:** $E_{pk_B^*}(W), pk_B^*, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*), X_R$.
R forwards the message $\{E_{pk_B^*}(W),\ pk_B^*,\ Sign_{sk_{CA}}(E_{pk_B^*,pk_B^*}),\ X_R\}$ to the seller **S** where X_R is the content that **B** intends to buy.

3) **S** extracts V_R from X_R and searches V_R in the database. If V_R does not exist, X_R is not a legal copy of **R**; otherwise, **S** checks the validity of $E_{pk_B^*}(W)$ by verifying $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$ with **CA**'s public key. If it fails, the operation is terminated; otherwise, **S** performs the following operations.

   - **S** generates a new transaction watermark V_B to denote this transaction, where V_B is embedded into X_R to form $X_B = X_R \oplus V_B$.
   - **S** generates a random permutation function $p_B(.)$ and computes
   $$p_B(E_{pk_B^*}(W)) = E_{pk_B^*}(p_B(W)).$$
   - **S** computes
   $$E_{pk_B^*}(X_B') = E_{pk_B^*}(X_B) \oplus E_{pk_B^*}(p_B(W)).$$
   - **S** stores $E_{pk_B^*}(W), pk_B^*, V_B, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*), p_B(.)$ in the database and transfers R's ownership from the database to another reselling database.

4) **S** → **R:** $E_{pk_B^*}(X_B'), M, Sign_{sk_S}(M, pk_R^*)$.
S sends the message $E_{pk_B^*}(X_B'), M, Sign_{sk_S}(M, pk_R^*)$ to **R** where M indicates this reselling transaction and pk_R^* denotes the reseller's short-time public key already stored in the database before and sk_S is **S**'s private key. Then the reseller verifies $M, Sign_{sk_S}(M, pk_R^*)$ and keeps them as a certificate.

5) **R** → **B:** $E_{pk_B^*}(X_B')$.
R sends $E_{pk_B^*}(X_B')$ to **B**.

6. **B** decrypts $E_{pk_B^*}(X_B')$ to obtain $X_B' = X_B \oplus p_B(W)$ with the private keys sk_B^*.

2.1.3 Dispute Resolution Protocol

If an unauthorized copy Y is found by **S**, **S** extracts the transaction watermark V_B or V_R and searches the database to retrieve pk_B^* or pk_R^*. If only V_R is found, **R** is sued. If both V_B and V_R are found, **B** is sued. Then **CA** is requested to reveal who owns pk_B^* (or pk_R^*). The following is an example if both V_B and V_R are found.

1) **S** → **J:** $E_{pk_B^*}(W), pk_B^*, V_B, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$, and $p_B(.)$.
S sends the message $\{E_{pk_B^*}(W),\ pk_B^*,\ V_B,\ Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*),\ p_B(.)\}$ to **J**.

2) **J** verifies the validity of $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$, then computes, $E_{pk_B^*}(Y), E_{pk_B^*}(p_B(W))$ and finally checks whether $E_{pk_B^*}(p_B(W))$ exists in $E_{pk_B^*}(Y)$ or not. If it is found, **B** is convicted guilty; otherwise, (s)he is innocent. Finally, **J** asks **CA** to show the identity of the buyer who owns pk_B^*.

2.2 Security Analysis

Both of the CC and the CHT schemes are vulnerable to the seller cheating problem. In the watermark insertion protocols of the CC and the CHT schemes, the reseller **R** needs to return the copy X_R to the seller **S**. Once **S** obtains X_R, (s)he can illegally distribute X_R or sell X_R to other buyers, so called the seller cheating problem [4]. Because the digital content X_R still contains the watermark of **R**, **R** will be potentially sued in the dispute resolution protocol if an unauthorized copy Y of X_R is found by **S**. Neither the CC scheme nor the CHT scheme accounted for this problem. Specifically, the buyer-reseller watermarking protocols in the literature do not guarantee asymmetry property. To this end, we will propose an enhanced scheme to prevent **S** from obtaining **R**'s copy X_R.

3 The Proposed Scheme

Prior to describing the proposed scheme, the preliminary, commutative cryptosystem adopted in [18], is introduced to prevent seller cheating problems which exist in both of the CC and the CHT schemes.

3.1 Commutative Cryptosystem

Commutative cryptosystems are often used in mental poker games [20]. The basic concept is that the encryption and decryption order does not matter if some secret messages needed to be encrypted and decrypted twice or more, respectively.

A cryptosystem E is said to be commutative if it satisfies the following property: for any two keys K_1 and K_2 and any message m, $E_{K_1}(E_{K_2}(m)) = E_{K_2}(E_{K_1}(m))$ and $D_{K_2}(E_{K_1}(E_{K_2}(m))) = E_{K_1}(m)$, where $D(.) = E^{-1}(.)$.

An example [8] of ElGamal-type commutative cryptosystem is given below. Assume two parties, Alice and Bob, have

$$\begin{aligned} K_A &= (p, g_A, x_A, y_A) : y_A = g_A^{x_A} (mod\ p) \\ K_B &= (p, g_B, x_B, y_B) : y_B = g_B^{x_B} (mod\ p), \end{aligned}$$

where x_A and y_A (x_B and y_B) are the private and public key pair of Alice (Bob).

Encryption.

To encrypt a message m, Alice first chooses a random value number r_A and computes the ciphertext $C_A = (C_{A1}, C_{A2})$, where

$$\begin{aligned} C_{A1} &= g_A^{r_A} \bmod p, \\ C_{A2} &= m * y_A^{r_A} \bmod p. \end{aligned}$$

Bob chooses a random value number r_B and encrypts Alice's ciphertext C_A to obtain $C_B = (C_{B1}, C_{AB})$, where

$$\begin{aligned} C_{B1} &= g_B^{r_B} \bmod p, \\ C_{AB} &= m * y_A^{r_A} * y_B^{r_B} \bmod p. \end{aligned}$$

In reality, whether Alice or Bob does the encryption operation first will not affect the result, $C = (C_{A1}, C_{B1}, C_{AB})$.

Decryption.

Suppose Alice uses her private key to decrypt first, i.e.

$$\begin{aligned} C' &= C_{AB} * (C_{A1}^{x_A})^{-1} \\ &= m * y_B^{r_B} mod\ p. \end{aligned}$$

Then Bob uses the private key to decrypt, where

$$C' * (C_{B1}^{x_B})^{-1} = m \bmod p.$$

The result will not be affected by whether Alice or Bob does the operation first.

3.2 Registration Protocol

The registration protocol is the same as that in Section 2.1.1. Therefore, it is omitted here.

3.3 Watermark Insertion Protocol

The reseller may designate a transaction proxy, for example an auction web site, and the buyer directly communicates with the transaction proxy using a MIX network [1] via the Internet. Note that the watermarking insertion requires a privacy homomorphism such as RSA-based cryptosystem mentioned in Section 2.

1) **B** $\rightarrow$ **R:** $E_{pk_B^*}(W), pk_B^*, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$.
The buyer **B** sends the message $\{E_{pk_B^*}(W),\ pk_B^*,\ Sign_{sk_{CA}}(E_{pk_B^*}(W),\ pk_B^*)\}$ to the reseller **R**.

2) **B** $\rightarrow$ **R:** $E_{pk_B^*}(W), pk_B^*, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$, $E_{pk_R^*}(X_R), AGR, Sign_{sk_R^*}(AGR \parallel E_{pk_R^*}(X_R))$.
R first negotiates with **S** to set up a common agreement, AGR, which explicitly states the ownership transfer rights and obligations from **R** to **B** of X_R. Then (s)he computes $E_{pk_R^*}(X_R)$ and $s_1 = Sign_{sk_R^*}(AGR \parallel E_{pk_R^*}(X_R))$, where pk_R^* denotes the reseller's short-time public key already stored in the database before.

3) After receiving **R**'s message, **S** performs the following operations.

- **S** verifies the signature $s_1 = Sign_{sk_R^*}(AGR \parallel E_{pk_R^*}(X_R))$ for checking whether the messages are sent from **R**. If yes, (s)he computes the message authentication code (MAC) value $m' = H(E_{pk_R^*}(X_R), pk_R^*)$.
- **S** uses pk_R^* as a keyword and searches the record of pk_R^*. From the matched record, (s)he selects m and checks if m is equal to the computed m' or not where $m = H(E_{pk_R^*}(X_R), pk_R^*)$ is computed in the first-hand transaction. If not, X_R is not a legal copy of **R**. Otherwise, **S** checks the validity of $E_{pk_B^*}(W)$ by verifying $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$ with **CA**'s public key. If it fails, **S** terminates the transaction.
- **S** generates a new transaction watermark V_B which is embedded into X_R, to denote this transaction to get X_B, precisely,

$$\begin{aligned} & E_{pk_B^*}(E_{pk_R^*}(X_B)) \\ = \ & E_{pk_B^*}(E_{pk_R^*}(X_R)) \oplus E_{pk_B^*}(E_{pk_R^*}(V_B)). \end{aligned}$$

- **S** generates a random permutation function $p_B(.)$ and computes

$$p_B(E_{pk_B^*}(E_{pk_R^*}(W))) = E_{pk_B^*}(E_{pk_R^*}(p_B(W))).$$

- **S** computes $E_{pk_B^*}(E_{pk_R^*}(X'_B))$ and the new MAC value m as follows.

$$\begin{aligned} & E_{pk_B^*}(E_{pk_R^*}(X'_B)) \\ = \ & E_{pk_B^*}(E_{pk_R^*}(X_B)) \oplus E_{pk_B^*}(E_{pk_R^*}(p_B(W))) \end{aligned}$$

and

$$m = H(E_{pk_B^*}(E_{pk_R^*}(X'_B)), pk_B^*).$$

- **S** stores $E_{pk_B^*}(W)$, pk_B^*, m, V_B, $Sign_{sk_{CA}}(E_{pk_B^*}(W),\ pk_B^*)$, and $p_B(.)$ in the database; transfers R's ownership from the database to another reselling database.
- **S** generates M and $Sign_{sk_s}(M, pk_R^*)$, where M indicates this reselling transaction.

4) **S** $\rightarrow$ **R:** $E_{pk_B^*}(E_{pk_R^*}(X'_B)), M, Sign_{sk_S}(M, pk_R^*)$.
S sends the message $\{E_{pk_B^*}(E_{pk_R^*}(X'_B)),\ M,\ Sign_{sk_S}(M, pk_R^*)\}$ to **R**.

5) **R** $\rightarrow$ **B:** $E_{pk_B^*}(X'_B)$.
R computes $D_{sk_R^*}(E_{pk_B^*}(E_{pk_R^*}(X'_B))) = E_{pk_B^*}(X'_B)$ and verifies M by checking the validation of $Sign_{sk_S}(M, pk_R^*)$ and keeps them as a certificate. Then, **R** sends $E_{pk_B^*}(X'_B)$ to **B**.

6) **B** decrypts $E_{pk_B^*}(X'_B)$ to obtain $X'_B = X_B \oplus p_B(W)$ with the private key, sk_B^*.

3.4 Dispute Resolution Protocol

This subprotocol is the same as that in Section 2.1.3, and thus omitted here.

4 Security Analysis and Discussions

The main security problem in the buyer-reseller watermarking protocol comes from the seller-cheating problem that the seller obtains the sold copy X_R. Hence, the proposed improvement aims at avoiding this security concern by maintaining the asymmetry property. The security of the proposed buyer-reseller watermarking protocol is based on the following assumptions.

Assumption 1. *By a well-constructed MIX mechanism, the seller or an attacker gains no information about who purchased the digital content since the communication is untraceable.*

Assumption 2. *To guarantee the anonymity of buyer-reseller watermarking protocol, buyers must refresh the short-term transaction key pairs.*

First, we shall focus on how the proposed scheme can resist the seller cheating problems. Second, further discussions will be shown.

4.1 Seller Cheating Problems

Lemma 1. **S** *cannot cheat* ***B*** *by means of either reselling the watermarked copy which was sold to some buyer or impersonating a buyer to launch the transaction protocol.*

Proof. If **S** wants to cheat **B**, (s)he must obtain the watermarked content $X'_B = X_B \oplus p_B(W) = X_R \oplus V_B \oplus p_B(W)$ of **B**. However, the watermarked content X'_B is well protected by asymmetric encryption in the form of $E_{pk^*_B}(X'_B)$. Without the corresponding private key sk^*_B, **S** cannot decrypt the encrypted X'_B to obtain X'_B. Since **S** cannot obtain a watermarked content X'_B, therefore, **S** cannot illegally distribute X'_B and accuse **B** of piracy.

Furthermore, if **S** intends to impersonate **B**, (s)he faces the same problem as (s)he lacks the private key sk^*_B necessary to decrypt the watermarked content.

In sum, **S** cannot cheat **B**. □

Lemma 2. **S** *cannot cheat* ***R*** *by means of either reselling the watermarked copy which was sold to the reseller or maliciously accuse the reseller of piracy if an unauthorized copy is found.*

Proof. If **S** wants to cheat **R**, (s)he must obtain the watermarked content X_R of **R**. Since X_R is well protected by commutative cryptosystem, **S** has no efficient way to obtain X_R. Therefore, **S** cannot distribute X_R and accuse **R** of piracy.

Furthermore, **S** intends to maliciously accuse the reseller of piracy if an unauthorized copy, which was resold to a buyer but illegally redistributed by that buyer, is found. In the watermarking insertion phase, **R** keeps M and $Sign_{sk_S}(M, pk^*_R)$ as a certificate. **R** has this evidence to show (s)he is innocent. □

Theorem 1. *The proposed buyer-reseller watermarking protocol can resist the seller cheating problems.*

Proof. By **Lemmas 1** and **2**, **S** has no feasible way to cheat either **B** or **R**. Therefore, the proposed protocol can resist the seller cheating problems. □

4.2 Further Discussions

1) **Malicious Reseller.**
A malicious reseller **R** may send a fake $E_{pk^*_R}(X_R)$ to cheat **S**. Since X_R is encrypted by pk^*_R, **S** can not extract V_R. **S** can verify the validity of the received $E_{pk^*_R}(X_R)$ by comparing the computed MAC value $m' = H(E_{pk^*_R}(X_R), pk^*_R)$ and the stored value $m = H(E_{pk^*_R}(X_R), pk^*_R)$. If not identical, **S** rejects this transaction.

   Furthermore, **R** has no feasible way to frame **B**, either. Without the corresponding private key sk^*_B, **R** cannot decrypt the encrypted X'_B to obtain X'_B. Since **R** cannot obtain a watermarked content X'_B, therefore, **R** cannot illegally distribute X'_B and frame **B** later.

2) **Malicious Buyer.**
Since the seller and the reseller are unaware of the watermarked copy, the buyer cannot reasonably claim that the unauthorized copy was resold by the seller or the reseller. If **B** illegally distributes X'_B, (s)he can be traced in the way of the protocol in **Section. 3.4**.

3) **Anonymity.**
In the proposed protocol, the reseller uses a short-term key pair (pk^*_R, sk^*_R) for a transaction. During the transaction, the seller only knows a short-term public key, pk^*_R. Besides, The buyer uses a short-term key pair (pk^*_B, sk^*_B) for a transaction, too. The reseller only knows a short-term public key, pk^*_B. The seller does not know who the reseller/buyer is and the reseller does not know who the buyer is. In addition, by **Assumption 1**, the seller gains no information about who purchased the digital content. In this way, anonymity is guaranteed.

4) **Unlinkability.**
Buyers use their short-term key pairs for anonymous transaction. If a buyer reuses the short-term key pair for various transactions, some of the buyer's habits may be revealed. In the proposed protocol, both the sellers and the resellers know the triple $\{E_{pk^*_B}(W), pk^*_B, Sign_{sk_{CA}}(E_{pk^*_B}(W), pk^*_B)\}$. By **Assumption 2**, sellers and resellers cannot determine whether any two transactions belong to the same buyer or not.

5) **Coalition-Resistance.**
If two or more buyers collude (say B_1 and B_2), they still can not forge another buyer's transaction message $\{E_{pk^*_{B_3}}(W), pk^*_{B_3}, Sign_{sk_{CA}}(E_{pk^*_{B_3}}, pk^*_{B_3})\}$

Table 2: Comparison between the related schemes and the proposed scheme

Requirements	Memon-Wong [13]	Lei et al. [12]	Cheung-Currem [5]	Chen et al. [4]	The proposed
First-hand	Yes	Yes	Yes	Yes	Yes
Second-hand	No	No	Yes	Yes	Yes
Asymmetry	Yes	Yes	No*	No*	Yes
Anonymity	No	Yes	No	Yes	Yes
Unlinkability	N/A	N/A	N/A	Yes	Yes
Coalition resistance	Yes	Yes	Yes	Yes	Yes
Traitor traceability	Yes	Yes	Yes	Yes	Yes

*: Sellers might have watermarked copies sent from resellers in the second-hand scenario.

from their transaction messages $\{E_{pk^*_{B_1}}(W),\ pk^*_{B_1},\ Sign_{sk_{CA}}(E_{pk^*_{B_1}}(W),\ pk^*_{B_1})\}$ and $\{E_{pk^*_{B_2}}(W),\ pk^*_{B_2},\ Sign_{sk_{CA}}(E_{pk^*_{B_2}}(W),\ pk^*_{B_2})\}$. It goes without saying that it is not feasible to calculate the private key.

6) **Traitor Traceability.**
It is easy to distinguish who is the real traitor, since the buyer's transaction watermark is stored in the database and the reseller's transaction watermark is stored in the reselling database. The seller can distinguish who is the real illegal distributor. With the help of CA, the traitor can be traced and revealed by searching the database.

At the end of this section, Table 2 gives the further functionality comparisons between the related works and the proposed scheme. The proposed buyer-reseller watermarking protocol not only satisfies the requirements for second-hand markets which the earlier [12, 13] are not suitable for, but also provides the secure protocol compared with the other two buyer-reseller protocols [4, 5]. The traditional buyer-seller watermarking protocols [12, 13] do not support the second-hand market. The second-hand buyer-seller watermarking protocols [4, 5] are shown insecure by lacking asymmetry property.

Furthermore, Table 3 provides the comparison of computation cost. Since the computational cost of hash function is much lower than that of public-key operations, it is omitted in Table 3. In the dispute resolution subprotocol, the cost of the proposed scheme is almost the same as that of the related schemes. In the registration and watermark insertion subprotocols, they cost more than the CC and the CHT related subprotocols. The extra computation cost in the proposed protocol is mainly due to the inclusion of commutative encryption, which is adopted to enhance security for the protocol in the proposed scheme.

5 Conclusions

As the fact that a digitalized second-hand market has high commerce potential [4], researchers have rarely addressed the watermarking protocols for digitalized second-hand markets, transactions of digital contents. Although the existing CC and CHT schemes aim at this end, the authors show that the CC and CHT schemes cannot resist the seller-cheating problem. Therefore, it is worthwhile to remedy security weaknesses. Thus an improved second-hand watermarking protocol is proposed, in which all above mentioned requirements are satisfied including asymmetry, anonymity, resistance to malicious insiders, unlinkability, resistance to coalition attacks and traitor traceability.

Acknowledgments

This work was partially supported National Science Council, Taiwan, R.O.C., under contract by NSC 102-2221-E-415-014 and NSC 102-2221-E-415-007.

References

[1] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[2] C. L. Chen, C. C. Chen, D. K. Li and P. Y. Chen, "A verifiable and secret buyer-seller watermarking protocol," *IETE Technical Review*, pp. 1–10, 2014.

[3] T. H. Chen, G. Horng, "A lightweight and anonymous copyright-protection protocol," *Computer Standards and Interfaces*, vol. 2929, no. 2, pp. 229-237, 2007.

[4] T. H. Chen, G. Horng, and D. Tsai, "An anonymous buyer-reseller watermarking protocol," *Journal of the Chinese Institute of Engineers*, vol. 28, no. 3, pp. 535–538, 2005.

[5] S. C. Cheung and H. Currem, "Rights protection for digital contents redistribution over the internet," in *Proceedings of 26th Annual International Computer Software and Applications Conference*, pp. 105–110, 2002.

Table 3: Comparison of performance between the CC, CHT schemes and the proposed scheme for (a) registration and watermark insertion protocols and (b) dispute resolution protocol

(a)

Operation	Watermark embedding	Signing/verifying	Public-key en(de)cryption
Schemes	B/ R / S/ CA/ J	B/ R / S/ CA/ J	B/ R / S/ CA/ J
CC [5]	0 / 0 / 3 / 0 / 0	1 / 0 / 1 / 2 / 0	1 / 0 / 1 / 1 / 0
CHT [4]	0 / 0 / 3 / 0 / 0	1 / 1 / 2 / 2 / 0	2 / 0 / 1 / 2 / 0
Ours	0 / 0 / 2 / 0 / 0	1 / 2 / 2 / 2 / 0	2 / 2 / 4 / 2 / 0

(b)

Operation	Watermark extraction	Signing/verifying	Public-key en(de)cryption
Schemes	S/ J	S/ J	S/ J
CC [5]	1 / 1	0 / 1	0 / 1
CHT [4]	2 / 1	0 / 1	0 / 1
Ours	2 / 1	0 / 1	0 / 1

[6] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1673–1687, 1997.

[7] Z. Eslami, M. Kazemnasabhaji and N. Mirehi, "Proxy signatures and buyer-seller watermarking protocols for the protection of multimedia content," *Multimedia Tools and Applications*, vol. 72, pp. 2723–2740, 2014.

[8] J. Gwi, K. Sakurai, and J. H. Park, "Does it need trusted third party? Design of Buyer-Seller watermarking protocol without trusted third party," in *Proceedings of ACNS'03*, LNCS 2846, pp. 265–279, Springer, 2003.

[9] A. Kumar, S. P. Ghrera and V. Tyagi, "A comparison of buyer-seller watermarking protocol (BSWP) based on discrete cosine transform (DCT) and discrete wavelet transform (DWT)," in *Proceedings of the 49th Annual Convention of the Computer Society of India (CSI'15)*, vol. 1, pp. 401–408, 2015.

[10] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for on-line trade using information gap between buyer and merchant," *IEICE Transactions on Fundamentals*, vol. E89-A, no. 4, pp. 1725–1737, 2006.

[11] S. H. Lee, S. G. Kwon, and K. R. Kwon, "Mobile 3D secure transmission based on anonymous buyer-seller watermarking protocol," *Recent Advances in Communications and Networking Technology*, vol. 3, pp. 33–43, 2014.

[12] C. L. Lei, P. L. Yu, P. L. Tsai, and M. H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 13, no. 12, pp. 1618–1626, 2004.

[13] N. Memon and P. W. Wong, "A Buyer-Seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 10, no. 4, pp. 643–649, 2001.

[14] S. C. Pei, J. M. Guo, and H. Lee, "Novel robust watermarking technique dithering halftone images," *IEEE Signal Processing Letters*, vol. 12, no. 4, pp. 333–336, 2005.

[15] X. Qi and J. Qi, "A robust content-based digital image watermarking scheme," *Signal Processing*, vol. 87, no. 6, pp. 1264–1280, 2007.

[16] L. Qian and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer's rights," *Journal of Visual Communication and Image Representation*, vol. 9, no. 3, pp. 194–210, 1998.

[17] J. M. Shieh, D. C. Lou, and M. C. Chang, "A semi-blind digital watermarking scheme based on singular value decomposition," *Computer Standards and Interfaces*, vol. 28, no. 4, pp. 428–440, 2006.

[18] C. Wang, H. F. Leung, S. C. Cheung, and Y. Wang, "Use of cryptographic technologies for privacy protection of watermarks in internet retails of digital contents," in *Proceedings of the 18th International Conference on Advanced Information Networking and Applications*, vol. 1, pp. 414–419, 2004.

[19] S. Yong and S. H. Lee, "An efficient fingerprinting scheme with symmetric and commutative encryption," in *Proceedings of IWDW'05*, LNCS 3710, pp. 54–66, Springer, 2005.

[20] W. Zhao, V. Varadharajan, and Y. Mu, "A secure mental poker protocol over the internet," in *Proceedings of the Australasian Information Security Workshop*, vol. 21, pp. 105–109, 2003.

[21] S. F. Tzeng, M. S. Hwang, and H. B. Chen, "A secure on-line software transaction scheme," *Computer Standards and Interfaces*, vol. 27, no. 3, pp.303–312, Mar. 2005.

Fuh-Gwo Jeng received his M.S. in computer and information science from National Chiao Tung University and Ph.D. degree at the Institute of Computer Science, National Chung Hsing University, Taiwan. He is presently an associate professor of Department of Applied Mathematics, Nation Chiayi University. His research interests include information security and computer graphics.

Jyun-Ci Huang received his M.S. in Department of

Computer Science and Information Engineering from National Chiayi University in 2008. His research interests include information security, and image security.

Tzung-Her Chen was born in Tainan, Taiwan, Republic of China, in 1967. He received the B.S. degree in Department of Information & Computer Education from National Taiwan Normal University in 1991 and the M.S. degree in Department of Information Engineering from Feng Chia University in 2001. In 2005, he received his Ph.D. degree in Department of Computer Science from National Chung Hsing University. He has been with Department of Computer Science and Information Engineering at National Chiayi University as Professor since August 2011. His research interests include information hiding, multimedia security, digital rights management, network security. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.

Performance Analysis of Location Privacy Preserving Scheme for MANETs

Bhawani Shanker Bhati and Pallapa Venkataram
(Corresponding author: Pallapa Venkataram)
Protocol Engineering and Technology Unit, Department of ECE, Indian Institute of Science
Bangalore 560012, India
(Email: pallapa@ece.iisc.ernet.in)
(Received June 24, 2014; revised and accepted Jan. 16 & June 13, 2015)

Abstract

We consider the problem of preserving node's location privacy which is essential for minimizing the attacks during multi-hop routing in MANETs. As by intercepting and analyzing the transmitted packets, intermediate nodes (conventionally, assumed to be trustworthy) can track sender and receiver nodes, and can also trace the route between them. Earlier approaches attempts to preserve the location privacy by changing node-IDs or masking the location information, but results in high cost and degradation of service quality. To overcome these drawbacks, this paper presents: 1) a novel rough set based Location Privacy Preserving (LPP) scheme during route establishment; and 2) an efficient Data Transfer scheme for Location Privacy Preserving based Routes (DTLPPR) during data transfer. Analysis of trustworthiness of neighbor nodes using Discrete Time Markov Chain, and proposed scheme in terms of *location privacy* and *route untraceability* is presented. Analytical work is validated using simulations.

Keywords: Location privacy, mobile ad hoc networks, rough set, route untraceability, trust attributes

1 Introduction

The self-organizing, decentralized and infra-structureless features of MANETs provide a promising solution for several real world applications [4]. The nodes functions as both a router and a host, and communicate with other nodes which are not in its transmission range through intermediate nodes by establishing a route and then transferring the data packets. Though nodes are considered to be trustworthy, but a few nodes might be malicious and launch attacks: 1) by using the information such as sender/receiver identity, locations, neighborhood, etc.; and 2) by overhearing and analyzing the data packets over wireless links. Thus, malicious nodes can track the location of a mobile node, and can also trace the route [10]. Location of the nodes is utilized to reduce overhead and achieve high throughput with low delay [7]. However, if the user's mobility or location is not safeguarded, malicious node can build user mobility profile and link the information to user identities or addresses.

1.1 Location Privacy

The unsought for leak of location and analysis of overheard data packets, results in location breach, thereby launching attacks which can disrupt MANET. Thus, location privacy preserving scheme is a critical requirement for minimizing the attacks, and also for the successful operation of MANET. Location privacy prevents sender and receiver from being revealed to any untrusted nodes, and also provides an untraceable route. Most of the earlier works, rely on: (1) Changing the node identity (node-ID); or (2) Masking of the location information by adding noise. However, they result in high cost and degradation of service quality. In addition, limited resource is one of the major problems. As a result, earlier works are unsuitable for resource constraint MANET. This necessitates the development of a low cost scheme to preserve location privacy without affecting the services.

1.2 Proposed Location Privacy Preserving Scheme

In order to preserve the location privacy, we propose a novel rough set based Location Privacy Preserving (LPP) scheme, and an efficient Data Transfer scheme for Location Privacy Preserving based Routes (DTLPPR). LPP scheme, establishes an untraceable route through trusted nodes (acts as temporary sender for their next hop), where trust value is determined by the trust attributes (defined using Rough set theory). In DTLPPR scheme, sender (or temporary sender) node randomly generates a challenge in *challenge generation period*. For every challenge received, trusted neighbor node sends back a response message to its sender. We mention that, sender (or tem-

porary sender) node selects two trusted neighbor nodes, one extra node for backup to overcome data loss due to route failures. The proposed schemes can be used for any ad hoc network by adapting the nature of communications and security challenges of that network, however, in this work we consider MANET. We theoretically analyze the trustworthiness, location privacy and route untraceability. The performance of proposed scheme is evaluated by performing simulations, and also comparing with earlier works. The contributions of this paper are: (1) *Location Privacy* - Preserving location privacy of sender and receiver nodes, by not revealing who are the originator and receiver of data packets to any node, except the designated trusted intermediate nodes; (2) *Route Untraceability* - Route established is not revealed, i.e., malicious nodes cannot identify the trusted intermediate nodes; (3) *Trustworthiness of neighborhood* - A Discrete Time Markov Model is proposed to evaluate the trustworthiness; and (4) *Data Transfer scheme* - Strengthening the location privacy, by ensuring that data is received by designated trusted node.

1.3 Organization of The Paper

The rest of the paper is organized as follows. In Sections 2 and 3, some of the earlier works and definitions used are given, respectively. Section 4, explains proposed location privacy scheme. Section 5, discusses the performance of proposed scheme against some of the attacks. We theoretically analyze the proposed scheme in Section 6, and provide simulation results in Section 7. Finally, we conclude in Section 8.

2 Related Works

Earlier works on preserving location privacy, rely on changing the node-IDs [2, 9, 20, 26, 31] or masking of the location information by adding noise [11, 21, 27, 28]. In the former approach, a node uses pseudonyms instead of real node-ID. Further, to strengthen the location privacy, nodes change their pseudonyms time-to-time [2], which makes it difficult for an attacker node to link the data packets for longer time period. In [19], authors discuss the impact on the performance due to frequently changing node-IDs for the Vehicular Adhoc Network (VANET). The major challenges faced are: when to change the pseudonyms, and how to conceal the relevance between old and new pseudonyms. For example, density of neighbor vehicles is used as a threshold value for pseudonym change [20]. In [26], the receiver node's location is exposed for route discovery, and then pseudo identifiers of communicating nodes are used for data delivery. MASK [31] enables both network-layer and MAC-layer communications without disclosing real identities. ANODR [9], assigns a random route pseudonym to each hop on the route to provide an untraceable and intrusion tolerant routing. However, MASK and ANODR introduces high overheads due to changing pseudonyms. In the later approach, location information is safeguarded by adding noise to original location information. A geographical mask [11], is used to add deterministic or stochastic noise to original location of a point. A similar approach is presented in [21], where the location information is perturbed by different levels for different groups, thus allowing obfuscation of a mobile node's exact location. As location information is perturbed, there is degradation in service quality. An approach to achieve receiver anonymity is presented in [27] that uses fuzzy receiver positions, and the data packets for a receiver node are delivered to nodes within a geographical area called anonymity zone. [28] preserves node's location information by defining a safety level. If a region has high safety level, then it is less likely for an attacker to determine the nodes within that region. In [32], the location privacy is preserved by dissociating node's location information and identity. In [3] presents, two schemes SECLOUD to conceal the true sender/receiver nodes, i.e., the attacker cannot identify the true sender/receiver; and ANONYRING to hide the sender/receiver nodes within a group of nodes forming a ring. The techniques given in [5] focuses on passive routing attacks, and addresses venue anonymity, privacy of network topology and privacy of node's motion pattern. In [24], by combining signature and Weil Pairing, an anonymous and authenticated communication scheme in VANET, namely ATCS, is presented. [1] prevent driver's (node in VANET) privacy by using a security scheme, where authentication and driver's privacy trade-offs are discussed. However, [3, 32, 24] and [1], does not consider route untraceability. Earlier works on preserving location privacy, mainly focus on the route establishment stage, and do not pay much attention to data transfer stage. [30] address issues on anonymous authentication, and proposes an efficient communication protocol for VANET based on conditionally anonymous ring signature. [13] points out security pitfalls of important secure routing protocols. and also propose a secure routing protocol against active attackers using digital signatures. [30] and [13] do not consider the passive attackers.

3 Definitions

3.1 Rough Sets

Rough set theory introduced in early 1980's [15] is used extensively in various fields [23], mainly for reasoning about knowledge and classification. The data is represented using an information table, denoted as $I = < U, A, V, f >$, where U is a non-empty finite set of objects called universe, A is a non-empty finite set of attributes, $V = V_{a_1} \cup V_{a_2} \cup ...V_{a_K}$ (V_{a_i} is the value of the attribute 'a_i') and 'f' is an information function which appoints the attribute value to every object in U. Table 1 represents set of all neighbor nodes as universe and their trust attributes as set of attributes. Trust attributes considered are Node History (NodeHist), Node Reliability

Table 1: Rough set concepts for trust in MANET

Symbol	Definition
$U = \{n_1, n_2, ..., n_M\}$	Non - empty finite set of 1-hop neighbor nodes
$A = \{a_1, a_2, ..., a_K\}$	Non - empty finite set of attributes: Node History, Resource Availability and Node Reliability
V_{a_i}	Value of the attribute 'a_i'

(NodeRel) and Resource Availability (RscAvl). Rough set concepts, classify the nodes into three separate regions: positive region (PosR), negative region (NegR) and boundary region (BndR), based on their trust attributes. Considering, $T \subseteq A$ and $Y \subseteq U$, then the approximation of Y is determined based on the information in T, by finding *T-lower* ($T_l(Y) = \{e \in U | [e]_T \subseteq Y\}$) and *T-upper* ($T_u(Y) = \{e \in U | [e]_T \cap Y \neq \phi\}$) approximations of Y. $[e]_T$ is the equivalence classes of *T-indiscernibility* relation. The nodes in $T_l(Y)$ can be certainly the elements of Y and the nodes in $T_u(Y)$ can be possible elements of Y, based on the trust attributes in T. Using the $T_l(Y)$ and $T_u(Y)$, universe U is divided into three disjoint regions: (1) *Positive region*, PosR(Y) = $T_l(Y)$; (2) *Negative region*, NegR(Y) = U - $T_u(Y)$; and (3) *Boundary region*: BndR(Y) = $T_u(Y)$ - $T_l(Y)$. In this paper, we define trusted neighbor nodes as PosR, non-trusted neighbor nodes as NegR and medium trusted neighbor nodes as BndR. However, we mainly focus on positive region for determining the trustworthiness, which is explained in Section 6.1.

3.2 Trust Attributes

The trustworthiness is determined based on trust attributes (see Table 1). Now, we briefly describe each one of these trust attributes: (1) **Node History** reflects the behavior of a node, and it depends on percentage of packets forwarded (ratio of number of packets forwarded to number of packets received) and percentage of packets dropped (ratio of number of packets dropped due to malicious behavior to number of packets received), where no feedback about the packet drop indicates a malicious behavior and the packet drop count (due to malicious behavior) is incremented; (2) **Node Reliability** indicates node's ability to provide higher delivery rates and to minimize the number of route failures, and it depends on Neighbor Node's Traversal Time (NNTT) and link stability between nodes. The NNTT is defined as the time taken by a node on average to process a packet. For simplicity, we consider that the NNTT and link stability parameters can be low, medium or high based on predefined threshold values, and Table 3 shows the values that can be taken by node reliability attribute. The link stability can be measured based on signal strength, where 'low' indicates that link between nodes will expire soon and 'high' indicates that link between nodes will sustain for longer time; (3) **Resource Availability** indicates the nodes richness in terms of availability of resources to support applications, and depends on bandwidth and battery power. We consider that the bandwidth and battery power resource values can be low, medium or high based on application dependent threshold values. Table 4 shows the values that can be taken by resource availability attribute. We mention that the node reliability attribute parameters can be assigned finer values, for example: very low, low, medium, high and very high values. Similarly, we can assign finer values to node history attribute parameters and resource availability attribute parameters. However, for simplicity we have assigned the parameter values as shown in Tables 2, 3 and 4.

Table 2: Node history (NodeHist) attribute values

Packets Forwarded(%)	Packets Dropped(%)	NodeHist Value
[0,51)	[51,100]	1 (= suspicious)
[0,51)	[0,51)	2 (= normal)
[51,100]	[0,51)	3 (= good)

Table 3: Node reliability (NodeRel) attribute values

Link Stability	NNTT	NodeRel Value
Low	Medium	1
Low	High	
Medium	High	
Low	Low	2
Medium	Medium	
High	High	
Medium	Low	3
High	Low	
High	Medium	

Table 4: Resource availability (RscAvl) attribute values

Bandwidth	Battery Power	RscAvl Value
Low	Low	1 (= Low)
Low	Medium	
Medium	Low	
Medium	Medium	2 (= Medium)
High	Low	
Low	high	
Medium	High	3 (= High)
High	Medium	
High	High	

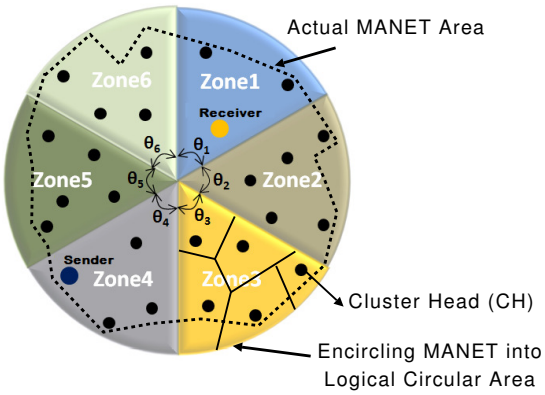


Figure 1: MANET division into 6 zones

4 Proposed Location Privacy Scheme

In this Section, we discuss our proposed rough set based location privacy scheme. First, we describe the network and attack models, and then details on tracing of trust attributes, construction of information tables and selection of trusted neighbor node is provided. Finally, we present our proposed schemes LPP and DTLPPR in detail.

4.1 MANET Model

We assume that a MANET is built with bidirectional wireless links. As earlier works [27, 32], we assume that every node have the knowledge of their positions (e.g., through GPS, WiFi-based positioning system), and a node can get the position information of other nodes using any secure positioning service [12, 25]. We assume that MANET is logically divided into 'N' number of zones (see [8]). However, we assume that area of MANET is circular in nature and it is divide into six zones, as shown in Figure 1. The MANET is divide into zones of equal angles ($\theta_1 = \theta_2 = \theta_3 = \theta_4 = \theta_5 = \theta_6 = \theta = 60°$) with respect to the center of MANET. In the case, when MANET is not circular, we encircle the MANET into a logical circular area to enable zone formation. The zones are further divided into clusters by considering a node as a cluster head (node with high resources) having set of nodes at most 2-hops away, and maintaining trust attribute values for the nodes within its cluster.

4.2 Attack Model

Threats in MANET may come from within as well as from outside. The attackers from outside (or external attackers), are able to passively receive data packets within their hearing range, and then determine the location and identity of node sending the data packets. On the other hand, attackers from within (or internal attackers) are the active nodes pretending to be legitimate node and sending packets to gain knowledge about other nodes location and identity. Earlier works have focused on active attacks which are done through viruses or Trojans. In this work, we focus on the passive attacks, where we consider that the attackers have following goals: (1) Obtain information such as sender and receiver nodes of the data packets; and (2) Trace the route taken by the data packets. By analyzing the traffic, an attacker can obtain these information. We mention some of the attacks [17] due to traffic analysis: (1) *Packet Tracing Attack* - By overhearing transmission of data packets as they traverse from sender to receiver, an attacker may determine the communicating nodes and also trace the route; and (2) *Timing Analysis Attack* - An attacker can monitor the packet departure and packet arrival times, and use this information to determine the sender and receiver. The attackers can overhear the transmission of data packets within their hearing range. However, their computing resources are limited, i.e., encrypted data cannot be decrypted easily, and the attacker cannot locate the nodes using secure position service.

4.3 Tracing Trust Attributes

To provide confidentiality during zone-based tracing of trust attributes, nodes use t-degree polynomial functions [22] to privately send information to their neighbor nodes and cluster head. A node-n (in zone Z_1) should be aware of the functions $h_{1,l}(x)$, where l = 1, 2, ..., 6 (six zones). The first index and second index in function $h_{k,l}(x)$ represents destination zone-id (k) and source zone-id (l) of the information packets, respectively. When node-n in Z_1 sends its information to node in Z_2, it sends out an encrypted packet (encrypting using key determined from t-degree polynomial) $E_{h_{2,1}(n)}$(node-n, *information*, *timestamp*). The "*information*" field consists parameter values of trust attributes (eg., battery power status, NNTT, etc.) and "*timestamp*" field indicates freshness of the information. When neighbor nodes of node-n receive this information, they make an entry in their Neighbor Node Information Table (NNIT). Similarly, nodes within a cluster send information to their cluster head, and the cluster head makes an entry in its Cluster Node Information Table (CNIT). However, in this case, nodes use cluster-id instead of destination zone-id, and its own node-id instead of source zone-id.

4.4 Information Table

The nodes and cluster heads represent the received information in the form of NNIT and CNIT, respectively. The row of NNIT represents the neighbor nodes and each column represents their trust attributes. Table 5 shows an example of NNIT at node-S, with A, B, C, D, E, F and G as neighbor nodes (for Figure 2). Here, we consider node history (*TA-1*), node reliability (*TA-2*) and resource availability (*TA-3*) as trust attributes for neighbor nodes. The CNIT is similar to NNIT, except that it has information on all the nodes within cluster. The

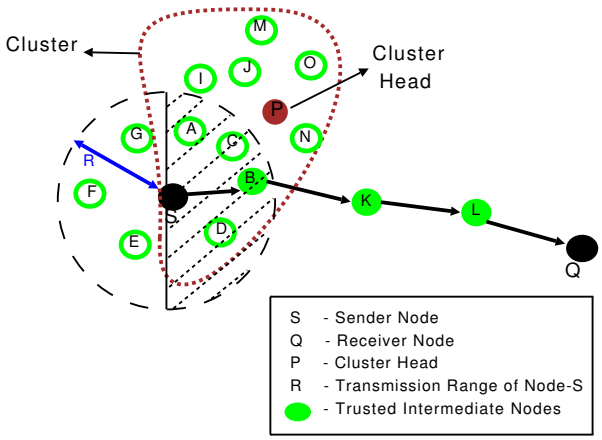


Figure 2: Node-S with its neighborhood and cluster head node-P

Table 5: Rough set based NNIT at node-S

Node-S	*TA-1*	*TA-2*	*TA-3*
A	2	1	2
B	3	3	2
C	2	1	2
D	1	1	2
E	3	2	3
F	1	1	2
G	3	1	2

Table 6: Rough set based CNIT at cluster head-P

Cluster Head-P	*TA-1*	*TA-2*	*TA-3*
A	1	3	1
B	2	3	2
C	1	2	3
D	3	1	2
I	1	1	1
J	3	1	1
M	1	1	3
N	3	1	2
O	3	2	1
S	1	2	3

row in CNIT represents cluster members and each column represents their trust attributes, as shown in Table 6 (for Figure 2).

4.5 Trusted 1-hop Neighbor Node Selection

The selection of trusted node is to: (1) Save node's power by avoiding unnecessary transmission. (2) Effectively utilize the bandwidth. (3) Increase the packet delivery rate. (4) Provide location privacy. The sender (or temporary sender) selects a trusted node among its neighbor nodes with the highest trust value. The trust value of a node-k, calculated by node-i (denoted as TV_k^i) is given by, $TV_k^i = \beta * TV_k^i + (1-\beta) * TV_k^{CH}$. β is the self-weightage factor, first term ($TV_k^i = \sum_j (W_j^k * V_j^k(nnit))$) is direct trust calculated by the sender (or temporary sender) and second term ($TV_k^{CH} = \sum_j (W_j^k * V_j^k(cnit))$) is indirect trust calculated based on the feedback from node-k's cluster head. W_j^k is the weight assigned to trust attribute-j for node-k, $j \in$ {NodeRel, NodeHist, RscAvl}, $V_j^k(nnit)$ and $V_j^k(cnit)$ are the values of trust attribute-j for node-k from NNIT and CNIT, respectively. As, sender node has knowledge of the receiver's position (using secure position service), trust value is calculated only for neighbor nodes towards receiver node, i.e., neighbor nodes within shaded region of Figure 2. For example, in Figure 2, node-B and node-C are selected for data transmission and backup, respectively (by assigning equal weights to trust attributes and $\beta = 0.6$).

4.6 Location Privacy Preserving (LPP) Scheme

LPP scheme establishes an untraceable route, while preserving location privacy. First, nodes privately send information to their neighbor nodes and also to cluster head (see Section 4.3). Second, each node maintains a NNIT, and cluster head maintains a CNIT (see Section 4.4). Third, NNIT and CNIT are used to determine the trusted neighbor nodes (see Section 4.5). Finally, an untraceable route is established.

4.6.1 Route Establishment With Trusted Neighbor Nodes

When a sender has data for a receiver, and if there is no trusted neighbor node (towards receiver) in sender's routing table, then route establishment stage (hop-by-hop basis) is initiated, as explained here. Sender selects a trusted neighbor node (with highest trust value), and then establishes connection with it, using route request (rreq) and route reply (rrep) messages, and finally transmits the data packets to selected trusted neighbor node. Since, rreq and rrep messages are sent only to selected trusted neighbor node, there is a decrease in message overhead compared to broadcasting of rreq message in some of the earlier works. Now, selected trusted neighbor node acts as a temporary sender and establishes connection with its trusted neighbor node (towards receiver), and this process is continued till the receiver. The format of rreq message is: $<$ *type, rreq-id, trusted neighbor node's address, originator's address* $>$, where *type* indicates rreq message, *rreq-id* is rreq id number and *originator's address* is sender (or temporary sender) node's address; and the format of rrep message is: $<$ *type, rreq-id, trusted neighbor node's address, originator's address* $>$, where *type* is rrep message. Since, receiver's address is not used in rreq and rrep messages, attacker cannot obtain the information regarding receiver. Here, we assume that

a sender (or temporary sender) knows trusted neighbor node's public key. As, data packet has to be sent only to trusted neighbor node, sender (or temporary sender) sets TTL = 1. The data packet format is $< Trapdoor, data >$, where Trapdoor (TD) information is obtained by encrypting the concatenated information using selected trusted neighbor node's public key. The TD information is given by, $TD = E_{PuK\_k}(S\_Ad||k\_Ad||D\_Ad||Dp)$, where, S_Ad is sender (or temporary sender) node's address, k_Ad is selected trusted neighbor node-k's address, D_Ad is receiver node's address, Dp is receiver node's position and || represents concatenation operation. The data part corresponds to different layer protocols and original data to be sent. The trusted neighbor node decrypts the TD using his private key, whereas other neighbor nodes can only overhear transmission, but cannot decrypt it. The trusted neighbor node compares D_Ad with its own address and realizes that it is not the receiver, and then it acts as a temporary sender and transmits the data packets. In the case, when receiver is 1-hop away, TD information contains concatenation of only node-k's address and receiver node's address. In literature, source routing [6] and sequence numbers [16] are used to avoid loops in a route, but they can disclose communicating nodes location, and thus cannot be used in location privacy scheme. In LPP scheme, data packets are forwarded to only trusted neighbor node, which reduces the distance to receiver in each routing step, and it leads to a loop-free routing. Since, trusted neighbor nodes has knowledge of only previous hop (acting as temporary sender), the original sender node's location privacy is preserved, and we see that the identity of original sender is also preserved. The other neighbor nodes, which cannot decrypt the data packets, are unable to determine receiver, and thus location privacy of receiver is preserved. In the case of receiver, its information is disclosed only to trusted intermediate nodes. To preserve the location privacy, control messages (rreq, rrep etc.) are encrypted, so that they cannot be differentiated from other data packets. We mention that the routing table at each node maintains information on trusted neighbor node towards receiver with their timeout values and rreq-id.

4.6.2 Established Route Is Untraceable

An attacker can overhear the data packets transmitted over wireless links by a node, and identify it as a sender, but cannot determine whether it is the original sender or an trusted intermediate node. The neighbors of a sender which cannot decrypt the TD, confuse the attacker by sending data packets to all their neighbors with an invalid TTL (indicating receiving nodes to discard data packets). Thus, an attacker cannot differentiate between the original sender and other neighbors. Similarly, trusted intermediate nodes and their neighbor nodes confuse the attacker, until receiver node is reached. The neighbor nodes of trusted intermediate nodes are called as participating (or supporting) nodes, because they participate

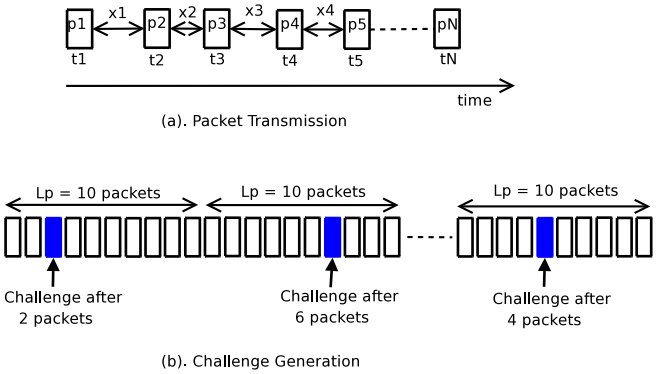


Figure 3: Data transfer scheme for location privacy preserving based routes (DTLPPR)

(or support) in providing an untraceable route. When receiver node receives the data packet, it again transmits the data packet with an invalid TTL to its neighbor nodes, i.e., the receiver acts as a temporary sender, and the neighbor nodes of receiver confuse the attacker by sending data packets to their neighbor nodes with an invalid TTL. Thus, it becomes difficult for an attacker to trace the route.

4.7 Data Transfer Scheme For Location Privacy Preserving Based Routes (DTLPPR)

To ensure that the data packets has reached designated trusted neighbor node, DTLPPR scheme is proposed, where a sender (or temporary sender) randomly generates a challenge for every 'L_p' number of data packets sent to next hop, and in reply, a response is generated by the next hop. Also, to strengthen LPP scheme, time between transmission of each data packet is varied at every hop during data transfer stage, i.e., if packet 'p1' is sent at time 't1', then packet 'p2' is sent at time 't2' (t2 = t1 + x1) and so on. The values of x1, x2, ..., are different (generated randomly), so that it becomes difficult for an attacker to identify sender and receiver based on their packet departure and arrival times, respectively. The Figure 3(a) shows packet transmission in DTLPPR scheme.

4.7.1 Challenge Generation Period

The challenge generation period indicates the number of data packets (L_p) for which, a sender (or temporary sender) node randomly generates a challenge, and it is determined using challenge attribute. By using rough set theory, challenge attribute (denoted as ch) takes value as shown in the Table 7, which is dependent on parameters: 1)*sensitivity of the data packets* (*or data sensitivity*), and 2) *trustworthiness* of selected trusted neighbor node. The *data sensitivity* and *trustworthiness* value is divided into levels - low and high. Original sender node decides *data sensitivity*, and *trustworthiness* is determined

Table 7: Challenge attribute (ch) Values

Data Sensitivity	Trustworthiness	Value
[0, 0.5]	[2, 3]	Low = 1
[0, 0.5]	[1, 2)	Medium = 2
(0.5, 1]	[2, 3]	
(0.5, 1]	[1,2)	High = 3

as described in Section 4.5. The *data sensitivity* value is sent to trusted neighbor node acting as temporary sender (during data transmission). If *data sensitivity* is low and *trustworthiness* of selected trusted neighbor node is high, then challenge attribute takes lowest value (indicating low challenge generation period or L_p). As *data sensitivity* increases and/or *trustworthiness* of selected neighbor node decreases, challenge generation period is increased. We mention that, for simplicity, values of challenge attribute are low (=1), medium (=2) and high (=3). The challenge generation period is determined using, $L_p = L_d * 2^{ch}$, where, L_d is a design parameter, indicating initial number of data packets decided by a sender (or temporary sender) node for generating a challenge at the start of data transfer. Later, sender (or temporary sender) node randomly generates a challenge within 'L_p'. For example, Figure 3(b) shows random generation of a challenge within L_p (= 10), where $L_d = 5$ and $ch = 1$.

4.7.2 Challenge - Response Messages

Sender (or temporary sender) ensures that the data packets has reached designated trusted neighbor node by randomly generating a challenge, and it is given by: $Challenge = [Op_i||n_i||k_i||fr_{flag}]$, where, n_i and k_i are two nonces generated by sender (or temporary sender) for packet-i, Op_i is operation to be done on two nonces for packet-i by the next hop and fr_{flag} is forwarding-rate flag. If fr_{flag} is set to 1, then forwarding-rate of next hop is required in response message, otherwise not required. A sender (or temporary sender) maintains forwarding-rate of next hop, and the counter is incremented for every packet forwarded by next hop. The next hop performs operation (Op_i) on two nonces n_i and k_i, and sends this result back to sender (or temporary sender) along with its forwarding-rate and number of packets received from sender (or temporary sender). The response generated by next hop is given by: $Response = [n_i(Op_i)k_i||fr_{tn}||N_{rx}]$, where, fr_{tn} is forwarding-rate of next hop and N_{rx} is number of packets received from sender (or temporary sender) at the time of response. If the values of 'n_i (Op_i) k_i' and fr_{tn} matches with the values calculated by sender (or temporary sender), then data transfer is continued. Otherwise, it terminates the data transfer and selects another trusted neighbor node or the backup node as next hop. The number of packets received N_{rx} is used by sender (or temporary sender) as a timestamp to obtain forwarding-rate of next hop, i.e, counter value at N_{rx}. We mention that, challenge and response messages are encrypted using next hop's and sender's (or temporary sender's) public key, respectively.

5 Location Privacy Protection Against Attacks

The performance of our proposed scheme against some of the attacks is discussed.

5.1 Timing Analysis Attack

Timing analysis attack [17], considers transmission of the data packets to be observable, and an attacker can locate sender and receiver using packet departure (at sender) and arrival (at receiver) times, respectively. In LPP scheme, neighbor nodes of a sender and receiver sends the data packets (with an invalid TTL) to their neighbors to provide covering feature to original data packets, and thus the attacker finds it difficult to locate the original sender and receiver. The location privacy of communicating nodes can be improved by considering two (or more) hops neighbor nodes, but it may result in high communication overheads. Also, we notice that the location privacy of nodes is strengthen by sending the data packets at different time intervals during data transfer stage (in DTLPPR scheme).

5.2 Packet Tracing Attack

Packet tracing attack [17] leads to a traceable route, i.e., intermediate nodes can be located by the attacker. In the proposed LPP scheme, participating nodes provide an untraceable route by sending data packets (with an invalid TTL) to their neighbor nodes. Notice that, there is an increase in number of participating nodes with increase in number of trusted intermediate nodes, which in turn increases the untraceability of route. The route untraceability is also improved in DTLPPR scheme, where trusted intermediate nodes send data packets at different time interval.

6 Analysis

In this section, we theoretically analyze our proposed schemes. First, we use rough set theory to determine the trusted neighbor node towards receiver. Second, we build a mathematical model for evaluating their trustworthiness. Later, we analyze the achieved location privacy in terms of *sender/receiver location privacy* and *route untraceability*.

6.1 Trusted 1-hop Neighbor Nodes

As explained in Section 3.1, neighbor nodes (from NNIT) or cluster members (from CNIT) in the positive regions

are trusted node(s). First, we consider NNIT (Table 5), with $U_{nnit} = \{A, B, C, D, E, F, G\}$ be a set of neighbor nodes, $X_{nnit} = \{A, B, C, D\}$ to be set of neighbor nodes (towards receiver) and $T = \{TA-1, TA-2, TA-3\}$ to be subset of trust attributes. The lower and upper approximations of X_{nnit} are $T_l(X_{nnit}) = \{A, B, C\}$ and $T_u(X_{nnit}) = \{A, B, C, D, F\}$, respectively. So, from NNIT we obtain positive region as $\text{PosR}_{nnit} = \{A, B, C\}$. Second, we consider CNIT (Table 6), with $U_{cnit} = \{A, B, C, D, I, J, M, N, O, S\}$ is set of nodes within a cluster, $X_{cnit} = \{A, B, C, D\}$ to be set of cluster members (towards receiver) which are 1-hop away from sender (or temporary sender). We mention that, sets X_{nnit} and X_{cnit} have the same elements. From CNIT, we obtain positive region as $\text{PosR}_{cnit} = \{A, B\}$. Now, we take intersection of both the positive regions, i.e., *Required Positive Region* $= \text{PosR}_{nnit} \bigcap \text{PosR}_{cnit} = \{A, B\}$. The trustworthiness of nodes A and B is determined, and node with highest trust value is selected for data transmission, whereas the other node as backup node. When there is only one node in the *Required Positive Region*, then we select that node for data transmission and backup node is selected from PosR_{nnit} or PosR_{cnit}, however higher priority is given to PosR_{nnit} (due to high self-weightage factor). If there are no nodes in *Required Positive Region*, then nodes are selected from PosR_{nnit} or/and PosR_{cnit}, with higher priority given to PosR_{nnit}.

6.2 Trustworthiness Of Neighborhood Nodes

Trustworthiness depends on parameter values of trust attributes, and it may increase or decrease due to change in these parameter values. The change in trustworthiness is modelled as Discrete Time Markov Chain (DTMC) with M states, where state-*1* represents the lowest trustworthiness and state-M represents the highest trustworthiness (see Figure 4). Consider, a random variable $(Y_t)_{t\geq 0}$ representing the current trustworthiness corresponding to a given state of node. Trustworthiness takes value within $[TV_{low},\ TV_{high}]$, where TV_{low} and TV_{high} represents low and high, i.e., state-*1* and state-M (in our scheme $TV_{low} = 1$ and $TV_{high} = 3$), respectively. The trustworthiness range $[TV_{low},\ TV_{high}]$ is divide into M states with a step of δ ($\delta = \frac{1}{|A|}$), where $|A|$ is the cardinality of trust attribute set. The probability of transition from state-i to state-j, i.e., 1-step transition probability is: $P_{i,j}(t) = P(Y_t = j | Y_{t-1} = i); 1 \leq i, j \leq M$.

6.2.1 1-step Forward/Backward Transition Probability

The 1-step transition probabilities are dependent on change in trustworthiness, which in turn depends on change in its parameter values of trust attributes. If the current state is 'i' at time 't', and their is an improvement in parameter values, then trustworthiness transits to the state (*i+1*); otherwise if parameter values declines, then

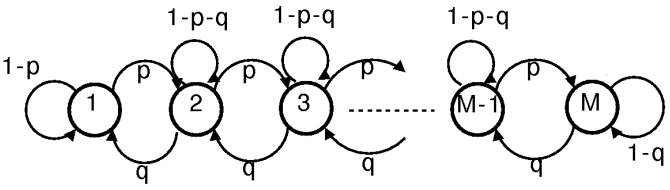


Figure 4: State transition diagram

trustworthiness transits to the state (*i-1*). The trustworthiness can remain in the same state, if there is no change in parameter values. In our model, increase in trustworthiness is related to improvement in any one of the trust attribute parameter values. Assuming that at each instant of time, one of the parameter value is changed, then the forward transition probability (p) and backward transition probability (q) are, $p = p_{i,i+1} = \frac{1}{3}(p_I^{nr} + p_I^{nh} + p_I^{ra})$ and $q = p_{i,i-1} = \frac{1}{3}(p_D^{nr} + p_D^{nh} + p_D^{ra})$, respectively. p_I^{nr}, p_I^{nh} and p_I^{ra} are the probabilities of increase in node reliability, node history (positive behavior) and resource availability, respectively. Similarly, p_D^{nr}, p_D^{nh} and p_D^{ra} are the probabilities of decrease in node reliability, node history (negative behavior) and resource availability, respectively.

Node Reliability

We assume that NNTT parameter values lies within a range $[NNTT^l_{min},\ NNTT^k_{max}]$, where $NNTT^k_{max}$ and $NNTT^l_{min}$ are the maximum NNTT value taken by node-k and minimum NNTT value taken by node-l, respectively. The probability (p_{nt}) with which trustworthiness of node-n (with node traversal time = $NNTT_n$) increases due to NNTT parameter is, $p_{nt} = \frac{NNTT^k_{max} - NNTT_n}{NNTT^k_{max} - NNTT^l_{min}}$. The link stability parameter can be determined using distance between nodes. Assuming that all the nodes have same speed, then the link stability will be high for a neighbor node near to the sender or temporary sender node (as the link will be active for more duration). The probability (p_{ls}) with which trustworthiness of node-n (at a distance D_n from the sender/temporary sender node) increases is, $p_{ls} = 1 - \frac{D_n}{R}$, where R is the transmission range of node. Thus, probabilities with which the trustworthiness increases and decreases (due to node reliability trust attribute) are, $p_I^{nr} = p_{nt} * p_{ls}$ and $p_D^{nr} = (1 - p_{nt}) * (1 - p_{ls})$, respectively.

Node History

We represent parameters of node history trust attribute as forwarding rate (for percentage of packets forwarded) and dropping rate (for percentage of packets dropped). The forwarding rate (f_r) and dropping rate (d_r) is given by $f_r = \frac{N_{pf}}{N_{rx}}$ and $d_r = \frac{N_{pd}}{N_{rx}}$, respectively. N_{pf} is the number of packets forwarded, N_{pd} is the number of packets dropped and N_{rx} is the number of packets received. Thus, probabilities with which the trustworthiness in-

creases and decreases (due to node history trust attribute) are, $p_I^{nh} = f_r*(1-d_r)$ and $p_D^{nh} = (1-f_r)*d_r$, respectively.

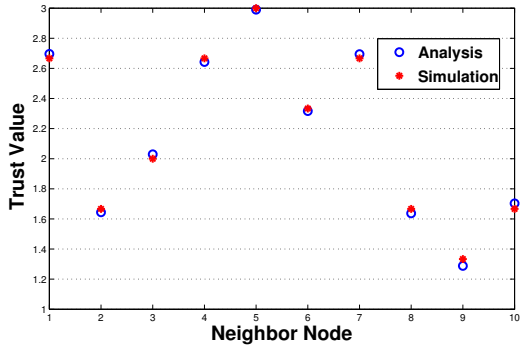
Resource Availability

We assume that, bandwidth availability lies within $[BW^u_{min}, BW^v_{max}]$, where BW^u_{min} is the minimum value at node-u and BW^v_{max} is the maximum value at node-v. Battery power availability lies within $[BP^f_{min}, BP^g_{max}]$, where BP^f_{min} is the minimum value at node-f and BP^g_{max} is the maximum value at node-g, respectively. The probability with which the trustworthiness increases and decreases (due to resource availability) are $p_I^{ra} = p_{bw} * p_{bp}$ and $p_D^{ra} = (1-p_{bw}) * (1-p_{bp})$, respectively. $p_{bw} = 1 - (\frac{BW^v_{max} - BW_n}{BW^v_{max} - BW^u_{min}})$ and $p_{bp} = 1 - (\frac{BP^g_{max} - BP_n}{BP^g_{max} - BP^f_{min}})$ are the probabilities that the trustworthiness increases due to bandwidth and battery power availability, respectively. BW_n and BP_n are bandwidth and battery power availability at node-n, respectively.

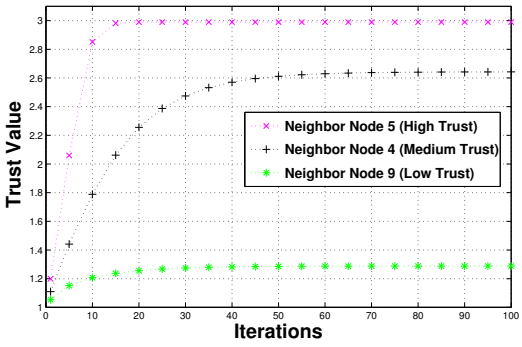
From the transition matrix T_m, we compute steady-state probabilities π_j, $j \in \{1,2,...,M\}$. To validate, we consider a Markov chain as represented in Figure 4 with 7 states, where events are considered to arrive with Poisson process at arrival rate λ to simulate change in parameter values. The analysis and simulation parameters are given in Table 8. T_{bw} and T_{bp} are the total bandwidth and battery power, respectively, and T_{nntt} represents the highest NNTT. Finally, we compare the analytical results with simulation results. First, we evaluate the average trustworthiness, and Figure 5(a), shows the analysis and simulated trustworthiness of 10 neighbor nodes. The average trust values obtained by analysis are very close to simulated results. However, there are some slight differences due to the fact that, during simulations, trust values are calculated using the discretized values. Second, we investigate the speed of convergence (number of iterations) of trust value. We mention that, trust values are recalculated, when any one of the parameter values change. Figure 5(b), shows the number of iteration required for convergence of trust value for low, medium and high trust values. The speed of convergence depends on the state transition probabilities.

Table 8: Analysis and simulation parameters

Parameters	Value(s)
Transmission Range (R)	200m
Number of Neighbor Nodes	10
Mobility Model	Random Way Point
δ	0.33
λ	5 - 10
$[BW_{min}, BW_{max}]$	[30%, 90%] of T_{bw}
$[BP_{min}, BP_{max}]$	[30%, 90%] of T_{bp}
$[NNTT_{min}, NNTT_{max}]$	[30%, 90%] of T_{nntt}



(a) Analysis and simulation results of trustworthiness



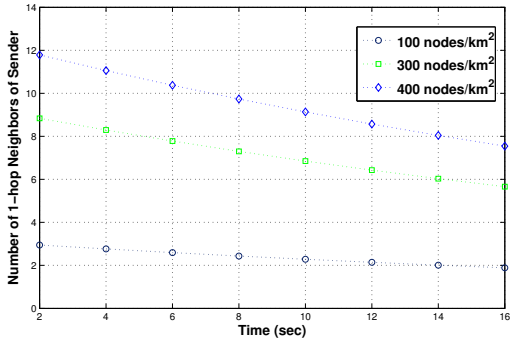
(b) Convergence of analysis trustworthiness

Figure 5: Trustworthiness of neighbor nodes

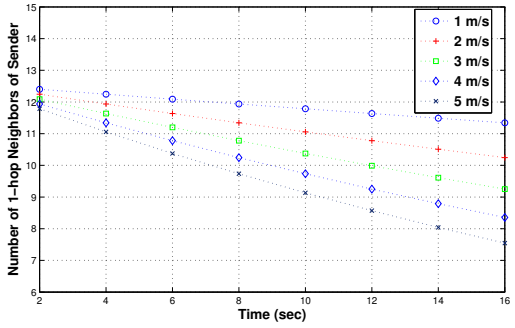
6.3 Sender/Receiver Location Privacy

The neighbor nodes of a sender and receiver confuse the attacker by providing covering feature to original sender's data packets, and also, receiver acts as a temporary sender. The location privacy of a sender or a receiver depends on number of neighbor nodes. From [27], probability ($p_s(t)$) that a node with mobility speed 'm' stays in the region after time 't', is exponentially distributed, $p_s(t) = e^{\frac{-t}{T_s}}$, where $T_s = \frac{\pi * A_r}{L_l * m}$ (A_r and L_l are the area and perimeter, respectively). For circular region with radius R, $T_s = \frac{\pi * R}{2 * m}$. We calculate the number of nodes remaining in sender node's transmission range using node density (n_d) and mobility speed (m). The process of node mobility in sender node's transmission range is assumed to follow exponential distribution [27]. The duration of data transfer indicates elapsed time of nodes communication. The number of nodes remaining ($N_{rem}(t)$) in transmission range of a sender node after a time period 't' is, $N_{rem}(t) = p_s(t) * \pi * R^2 * n_d$. By considering the transmission range to be equal, receiver and sender have same location privacy. Figure 6(a) shows the remaining number of neighbor nodes at mobility speed of 5 m/s for varying node densities with time. We see that, as the node density decreases, the number of neighbor nodes remaining in transmission range drops and hence the location privacy

decreases. We also see that, the remaining neighbor nodes decrease over time. Figure 6(b) shows the number of neighbor nodes remaining at node density 300 nodes/km^2 with varying node mobility speed with time. We see that, the number of neighbor nodes remaining within the transmission range decreases when the node mobility speed increases, so the location privacy decreases. Thus, location privacy is dependent on the node mobility, node density and also on transmission range.



(a) Varying node density



(b) Varying node speed

Figure 6: Estimated sender location privacy

6.4 Route Untraceability

The number of participating nodes determines the strength of untraceability, which is dependent on the number of trusted intermediate nodes (determined using number of hops). From [29], number of hops depends on: (i) The distance (d) between sender and receiver, and (ii) The remaining distance (Z) to the receiver.

To compute the expected number of hops, we assume that a node selects a trusted neighbor node within the link stability *'ls'* ($ls < R$) (see Figure 7). For using [29], circular MANET with radius R_m is approximated by square MANET with side length L_m, where the L_m is equal to ($\sqrt{\pi} * R_m$). Then, expected distance (r) between sender and trusted neighbor node is, $r = (\frac{2n_{des}}{2n_{des}+1} * ls)$. n_{des} is the number of neighbor nodes distributed over the shaded circle (see Figure 7). For simplicity, we consider that the neighbor nodes are uniformly distributed. Therefore, $n_{des} = \frac{N_{ls}}{2}$, where N_{ls} is all the neighbor nodes within

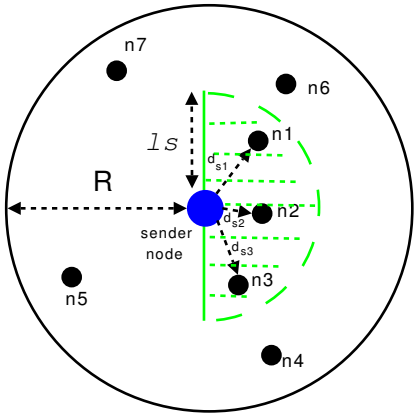


Figure 7: The distances between sender and its neighbor nodes within *ls*

range *ls*, and N_{ls} depends on node density (n_d) and *ls*. We consider that the selected trusted neighbor node may be anywhere on the boundary of semi-circle with radius r. From [29], expected remaining distance (Z) is given by,

$$Z = \int_{d-r}^{\sqrt{d^2+r^2}} Z f_Z(Z) dZ \qquad (1)$$

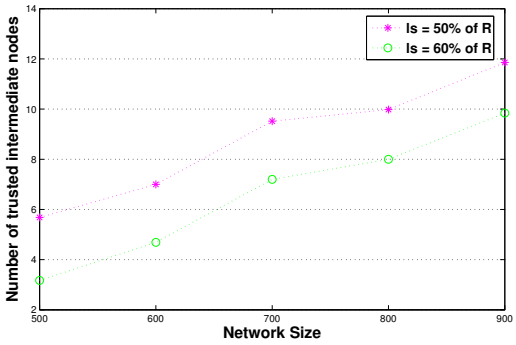
where, $f_Z(Z)$ is the pdf of Z, $f_Z(Z) = \frac{2Z}{\pi dr\sqrt{1-(\frac{d^2+r^2-Z^2}{2dr})^2}}$.

After determining Z for the first hop, 'd' in the next hop is changed to Z (from Equation (1)). Then, by repeating the process and counting the hops until Z falls below *ls*, the number of trusted intermediate nodes can be determined. The *hop count* is dependent on *ls*, thus the *ls* should be chosen such that it minimizes the transmission cost (or hop count). In order to determine the number of participating nodes, number of neighbor nodes of trusted intermediate nodes is calculated. Considering the transmission range of nodes in MANETs to be the same and n_d to be node density, then the number of neighbor nodes (N_{1-hop}) for a node is, $N_{1-hop} = (\pi * R^2) * n_d$. In MANETs, trusted intermediate nodes can have overlapping transmission range and common neighbor nodes. We need to count these common neighbor nodes only once during calculation of participating nodes. The transmission range of two nodes intersect if the distance between them is less than (R). From geometry, area of intersection (A_{ij}) between node-i and node-j is, $A_{ij} = 2R^2 cos^{-1}(\frac{d_{ij}}{2R}) - \frac{1}{2}d_{ij}\sqrt{4R^2-(d_{ij})^2}$. d_{ij} is distance between the two nodes i and j. Then, number of participating nodes (denoted as NP_{1-hop}) are,

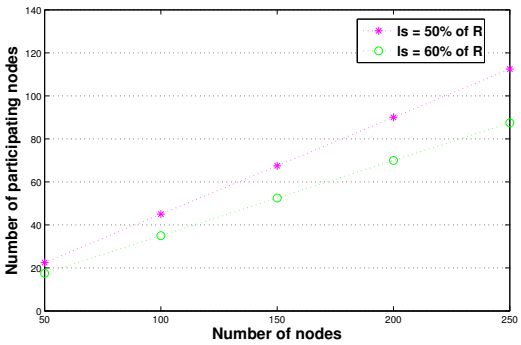
$$NP_{1-hop} = (N_{TN} * N_{1-hop}) - \sum_{i,j,i\neq j} (n_d * A_{ij}) \qquad (2)$$

where N_{TN} is the number of trusted intermediate nodes, and i, j = 1,2,....,N_{TN}. The expected distance (r) is used as the distance d_{ij} between two nodes on the same link. Figures 8(a) and 8(b) shows the number of trusted intermediate nodes and number of participating nodes for varying *ls* (*ls* = 50% and 60% of R), respectively. The

R of the nodes is assumed to be 200m and the network size (circular MANET with radius, R_m) is varied. We see that, with the increase in network size, there is an increase in the number of trusted intermediate nodes. The number of trusted intermediate nodes decrease with increase in *ls*. The Figure 8(a) confirms that transmission cost is determined by the *ls*. The network size is kept constant at 700m and number of nodes is varied. In Figure 8(b), number of participating nodes increases for lower value of *ls*, i.e., route untraceability increases. However, it results in an increase in number of trusted intermediate nodes. The number of participating nodes increases with number of nodes.



(a) Estimated number of trusted intermediate nodes



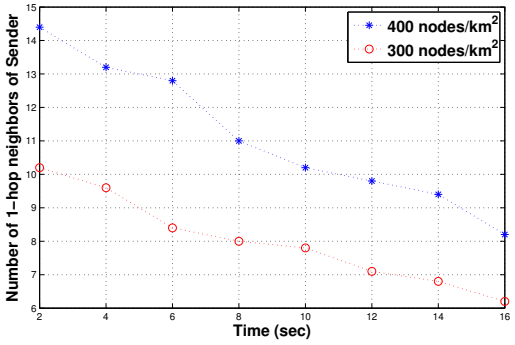
(b) Estimated number of participating nodes

Figure 8: Route untraceability

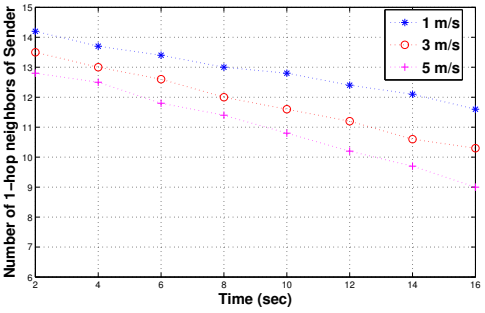
7 Simulation and Results

We provide the performance of proposed scheme using simulations (network simulator NS - 2.34 [14]). We consider bidirectional wireless links with 2Mbps capacity. The number of sender and receiver pairs are kept constant (10 pairs), whereas node mobility, node density and total number of nodes are varied. Each simulation duration was set to be 200s, and the final results were average of 20 simulations. Rough sets are used over the values of trust attributes to maintain NNIT/CNIT. Each node send the parameters values to their neighbor nodes, whenever the parameter values goes below or above the threshold level. Also, each node keeps track of the neighboring node, and whenever the change in received signal strength equals pre-defined value, it updates the NNIT and CNIT. Whenever the change in position is such that the distance between current and previously recorded position is greater than pre-defined value, the node sends the current position to its neighbor nodes. The threshold values of each parameters are varied for each simulation. The following metrics are used to evaluate the performance of proposed scheme in terms of location privacy: (1) *Actual sender location privacy* is the number of neighbor nodes of a sender; and (2) *Actual route untraceability* is the number of participating nodes. Figure 9(a) shows the actual sender location privacy for 300 nodes/km^2 and 400 nodes/km^2 node density. We see that, as the number of neighbors of a sender node move out of its transmission range over time, sender location privacy decreases. Figure 9(b) shows the actual sender location privacy for 1 m/s, 3 m/s and 5m/s node speed. We see that the sender location privacy decreases with increase in node speed over time. In Figure 9(c), average number of participating nodes increases with increasing number of nodes. We compare our proposed scheme with MASK [31] and AODV [16]. The reason behind choosing reactive protocols is that, they are on-demand protocols, so they establish route whenever it is required, and have low processing and computational overhead at node. Reactive routing protocols also provide quick adaptation to dynamic link conditions [16]. For encryption, we use RC6 [18] algorithm. The following metrics are used to evaluate the performance of proposed scheme, in terms of routing efficiency: (1) *Number of hops* is the average number of hop counts; (2) *Delivary rate* is the portion of data packets which are delivered successfully to a receiver; (3) *Latency* is the average time taken by a data packet from a sender to a receiver; and (4) *Normalized control bytes* is the normalized control overhead for sending a single data byte to a receiver. The *ls* is set to be 50% of R (R = 200m) for the proposed scheme, and for others we set *ls* to be equal to R. We see that, LPP has slightly high number of hop counts compared to AODV and MASK (see Figure 10(a)), and the hop count is not much affected when we incorporate DTLPPR scheme. It is expected, as the distance to trusted neighbor selection is dependent on *ls*. We see that, LPP has similar delivery rate as AODV under low mobility (2m/s), but at high mobility the LPP has lower delivery rate compared to AODV (see Figure 10(b)). Also, there is a slight reduction in the delivery rate when DTLPPR scheme is incorporated, however it provides better delivery rates when compared to MASK. The latency in LPP is higher than the AODV, but lower than MASK. This is due to the fact that, in LPP packets are routed through the trusted intermediate nodes only, and also requires time in encryption/decryption. In MASK, node-IDs (pseudonyms) are changed, resulting in high latency and low delivery rates compared to LPP. Figure 10(d) shows that LPP has higher control overhead when compared to AODV, which is expected due to encryption/decryption of data packets and trapdoor; but

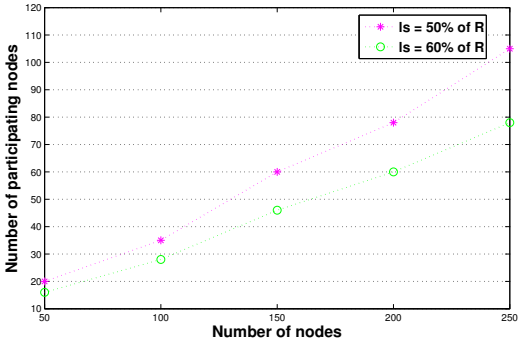
lower control overhead compared to MASK, because in LPP, control messages are sent only to trusted neighbor node. Also, the control packet sizes are less compared to MASK. However, we see that there is a slight increase in control overhead when DTLPPR is incorporated.



(a) Varying node density

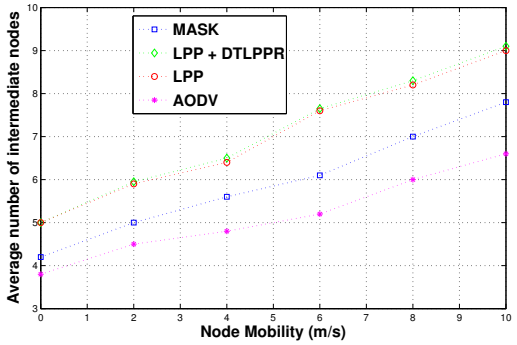


(b) Varying node speed

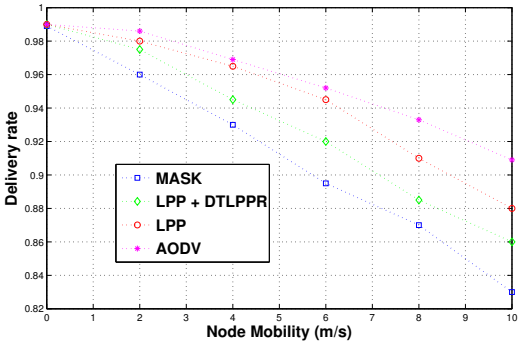


(c) Average number of participating nodes

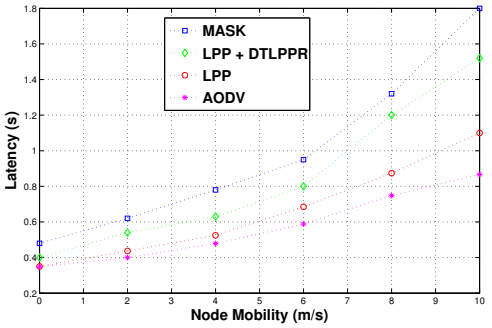
Figure 9: Sender location privacy and route untraceability



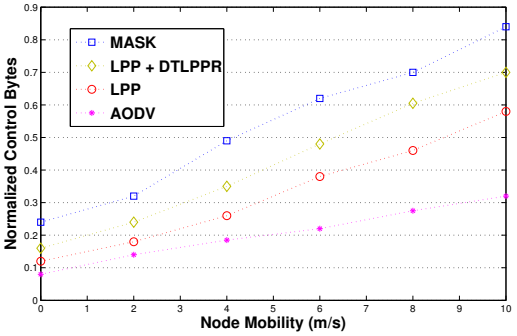
(a) Average hop count



(b) Delivery rate



(c) Latency



(d) Normalized Control Bytes

Figure 10: Comparison of proposed scheme with MASK and AODV

8 Conclusions

To overcome the drawbacks of the earlier approaches, and to preserve location privacy along with route untraceability, a novel LPP and an efficient DTLPPR schemes are proposed in this paper. The scheme uses trusted nodes for routing, which are determined using rough set theory. The analysis of scheme is discussed in terms of *trustworthiness of neighborhood*, *location privacy* and *route untraceability*. The proposed scheme performs better, and the effectiveness is shown through results. Future work, aims at reinforcing the proposed scheme in an attempt to

withstand stronger active attacks.

References

[1] M. S. Bouassida, "Authentication vs. privacy within vehicular adhoc networks," *International Journal of Network Security*, vol. 13, no. 3, pp. 121–134, 2011.

[2] F. Dotzer, "Privacy issues in vehicular ad hoc networks," in *5th International Workshop on PET*, pp. 197–209, 2005.

[3] T. Hayajneh, R. Doomun, P. Krishnamurthy, and D. Tipper, "Source - destination obfuscation in wireless ad hoc networks," *Security and Communication Networks*, vol. 4, no. 8, pp. 888–901, 2011.

[4] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: applications and challenges," *Journal of the Communications Network*, vol. 3, no. 3, pp. 60–66, 2004.

[5] X. Hong, J. Kong, and M. Gerla, "Mobility changes anonymity: new passive threats in mobile ad hoc networks," *Wireless Communication and Mobile Computing*, vol. 6, no. 3, pp. 281–293, 2006.

[6] D. Johnson, Y. Hu, and D. Maltz, *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4*, RFC 4728, 2007.

[7] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *International Conference on Mobile Computing and Networking*, pp. 243–254, 2000.

[8] T. D. S. Keerthi and P. Venkataram, "Locating the attacker of wormhole attack by using the honeypot," in *2012 IEEE 11th International Conference on TrustCom*, pp. 1175–1180, 2012.

[9] J. Kong and X. Hong, "Anodr: Anonymous on demand routing with untraceable routes for mobile adhoc networks," in *Mobile Ad Hoc Networking and Computing*, pp. 291–302, 2003.

[10] J. Kong, X. Hong, and M. Gerla, "A new set of passive routing attacks in mobile ad hoc networks," in *IEEE Military Communications Conference (MILCOM'03)*, pp. 796–801, 2003.

[11] M. Po Kwan, I. Casas and B. C. Schmitz, "Protection of geoprivacy and accuracy of spatial information: How effective are geographical masks?," vol. 39, no. 2, pp. 15–28, 2004.

[12] J. Lim, S. Kim and H. Oh, "A secure location service for ad hoc position-based routing using self-signed locations," in *Proceedings of 6th International Conference on CANS*, pp. 121–132, 2007.

[13] R. Matam and S. Tripathy, "Provably secure routing protocol for wireless mesh networks," *International Journal of Network Security*, vol. 16, no. 3, pp. 182–192, 2014.

[14] Network Simulator, *The Network Simulator ns-2.34*, 2015. (`http://www.isi.edu/nsnam/ns/`)

[15] Z. Pawlak, "Rough sets," *International Journal of Computer and Information Sciences*, vol. 11, no. 5, pp. 341–356, 1982.

[16] C. Perkins, E. Belding-Royer, and S. Das, *Ad Hoc on-demand Distance Vector (AODV) Routing*, RFC 3561, 2003.

[17] J. F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in *International Workshop on Design Issues in Anonymity and Unobservability*, pp. 10–29, 2000.

[18] R. L. Rivest, M. J. B. Robshaw, R. Sidney, Y. L. Yin, "The RC6 block cipher," in *First Advanced Encryption Standard (AES) Conference*, Aug. 1998.

[19] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets," in *Proceedings of ESAS*, pp. 43–57, 2006.

[20] J. H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular adhoc networks," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 160–171, 2010.

[21] W. Wang and C. Cui, "Achieving configurable location privacy in location based routing for manet," in *Military Communications Conference*, pp. 1–7, 2008.

[22] W. Wang and T. Stransky, "Stateless key distribution for secure intra and inter-group multicast in mobile wireless network," *Computer Networks*, vol. 51, no. 15, pp. 4303–4321, 2007.

[23] C. Wu, Y. Yue, M. Li, and O. Adjei, "The rough set theory and applications," *Engineering Computations*, vol. 21, no. 5, pp. 488–511, 2004.

[24] W. Hu, K. Xue, P. Hong and C. Wu, "Atcs: A novel anonymous and traceable communication scheme for vehicular adhoc networks," *International Journal of Network Security*, vol. 13, no. 2, pp. 71–78, 2010.

[25] X. Wu, "Disposer: distributed secure position service in mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 6, no. 3, pp. 357–373, 2006.

[26] X. Wu and B. Bhargava, "AO2P: Ad hoc on-demand position-based private routing protocol," *IEEE Transactions on Mobile Computing*, vol. 4, no. 4, pp. 335–348, 2005.

[27] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous geo-forwarding in manets through location cloaking," *IEEE Transactions on Parallel and Distributed Database Systems*, vol. 19, no. 10, pp. 1297–1309, 2008.

[28] T. Xu and Y. Cai, "Location safety protection in ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1551–1562, 2009.

[29] O. Younes and N. Thomas, "Analysis of the expected number of hops in mobile adhoc network with random waypoint mobility," *Electronic Notes in Theoretical Computer Science (ENTCS)*, vol. 275, pp. 143–158, 2011.

[30] S. Zeng, Y. Huang, and Xingwei Liu, "Privacy-preserving communication for vanets with conditionally anonymous ring signature," *International Journal of Network Security*, vol. 17, no. 2, pp. 135–141, 2015.

[31] Y. Zhang, W. Liu, W. Lou and Y. Fang, "MASK: Anonymous on-demand routing in mobile ad hoc networks," *IEEE Transaction on Wireless Communication*, vol. 5, no. 9, pp. 2376–2385, 2006.

[32] Z. Zhi and Y. K. Choong, "Anonymizing geographic ad hoc routing for preserving location privacy," in *Distributed Computing Systems Workshops*, pp. 646–651, 2005.

Bhawani Shanker Bhati received his B.E. degree from the CMRIT, Bangalore, India in 2009 and M.E. degree from the IISc, Bangalore, India in 2012. He is currently pursuing his Ph.D in the Department of ECE, IISc, Bangalore, India. His research interest are in the areas of Ad hoc Networks, Communication Protocols, Ubiquitous Computing, Security and Privacy in Wireless Networks.

Pallapa Venkataram received his Ph.D. Degree in Information Sciences from the University of Sheffield, England, in 1986. He is currently the chairman for center for continuing education, and also a Professor in the Department of ECE, IISc, Bangalore, India. Dr. Pallapa's research interests are in the areas of Wireless Ubiquitous Networks, Communication Protocols, Computation Intelligence applications in Communication Networks and Multimedia Systems. Dr. Pallapa is the holder of a Distinguished Visitor Diploma from the Orrego University, Trujillo, PERU. He has published over 200 papers in International/national Journals/conferences. He has received best paper awards at GLOBECOM'93 and INM'95 and also CDIL (Communication Devices India Ltd) for a paper published in IETE Journal. He is a Fellow of IEE (England), Fellow of IETE(India) and a Senior member of IEEE Computer Society.

Efficient Pixel Prediction Algorithm for Reversible Data Hiding

K. Bharanitharan[1], Chin-Chen Chang[2,3], Hai-Rui Yang[4], and Zhi-Hui Wang[4]
(Corresponding author: Chin-Chen Chang)

Department of Electrical Engineering, Feng Chia University[1]
Department of Information Engineering and Computer Science, Feng Chia University[2]
Taichung 40724, Taiwan
Department of Computer Science and Information Engineering, Asia University[3]
Taichung 41354, Taiwan
School of Software, Dalian University of Technology[4]
Dalian 116600, P. R. China
(Email: alan3c@gmail.com)
(Received Apr. 9, 2014; revised and accepted Mar. 20 & May 22, 2015)

Abstract

Prediction-error expansion (PEE) is an important reversible data hiding technique, which can hide large messages into digital media with little distortion. In this paper, we propose a nearest neighborhood pixel prediction algorithm (NNP^2) for reversible data hiding algorithms based on Chinese Remainder Theorem (CRT), in which a rhombus prediction is applied in NNP^2, and prediction errors, the difference between pixels and predictions, are modified to embed data. Further, CRT is utilized to adjust the modification size, thus embedding several bits into one embeddable pixel. Laplacian-like distribution of prediction errors is exploited to achieve a trade-off between embedding capacity and visual quality. Experimental results demonstrate that the NNP^2 achieves better embedding capacity with the same stego image quality than the conventional methods.

Keywords: Chinese remainder theorem (CRT), lossless watermarking, reversible data hiding (RDH)

1 Introduction

Reversible data hiding (RDH) techniques embed data into cover media, and, unlike most data hiding, the hidden message, as well as the cover data, can be completely recovered from the output data [3, 7, 16]. Reversibility of RDH offers a solution for lossless embedding in some sensitive media, such as medical images, military images, or artwork images, where even slight modification of these images is unacceptable due to the risk of a wrong explanation.

Generally, the existing RDH schemes are categorized into the following domains: compression domain, histogram shifting (HS) domain, difference expansion (DE) domain, and prediction-error expansion (PEE) domain. For compression domain, Fridrich et al. [6] compressed and encrypted bit-planes to make space for data embedding. However, large payloads would incur a greater level of distortion as a result of this method. Later, proposed generalized LSB (G-LSB) modifies the lowest level of the host image and achieves capacity-distortion control by modifying only a small portion of signal samples [14]. Although RDH schemes in compression domain attain high visual quality, their hiding capacity is relatively limited.

To lower the level of image distortion, the histogram shifting (HS) technique is employed within reversible data hiding. For HS domain, proposed histogram-based RDH scheme that uses pairs of peak points and zero points to lower image distortion, but lower embedding capacity [14]. In 2009, Tsai et al. [7] used linear prediction to calculate a residual image and embed data into the residual values, thus increasing the embedding capacity. Although this scheme achieves a higher embedding capacity, it is suitable only for medical images. Later, the proposed synchronization method solves the problem of communicating peak points for all histogram modification techniques by selecting certain peak points of the pixel difference histogram [17]. Also, the characteristics of the human visual system (HVS) are applied to histogram modifications to improve the visual quality of the embedded images, but this limited overall embedding capacity [11]. Afterwards, Al-Qershi and Khoo proposed a two-dimensional difference expansion (2D-DE) scheme and achieved a high hiding capacity of approximately 1 bit per pixel (bpp) [1]. Hereafter, histogram modification is extended to a pyramidal structure by utilizing global and local characteristics of host images [9]. This method

achieves a higher embedding capacity with acceptable visual quality. Further, Chang and Tai [4] improved histogram modification by sorting the prediction. However, this method of embedding for the White set expanded the prediction error, thus reducing the number of embeddable pixels of the Gray set. Note that histogram-based RDH schemes can achieve good visual quality and adequate embedding capacity, but they need to send pairs of peak and zero points to the receiver.

For DE domain, Tian [10] proposed a lossless DE algorithm based on the 1-D Haar wavelet transformation from 2003. The embedding capacity of this DE algorithm ranges from 0.15 to 1.97 bpp, which is notably higher than other previous schemes. Kamstra et al. [12] improved Tians technique by sorting the discrete wavelet transformation (DWT) coefficients in the low-pass band to make appropriate difference expansion in the high-pass band. These aforementioned DE methods achieve high embedding capacity but result in low image quality.

PEE domain is actually a specific extension of DE domain. In 2007, Thodi and Rodriguez [18] first proposed a PEE method and embedded messages by expanding the difference of pixels and predictions. Due to the Laplacian-like distribution of the prediction-error histogram,

PEE outperforms DE and HS. Afterwards, Hu et al. [8] proposed efficient compression of location map, and thus achieved an overall higher capacity. Sachnev et al. [15] embedded data in prediction errors when sorting by local variance. This method combines predicting and sorting and incurs less distortion compared with previous schemes. Li et al. [13] adaptively embedded one bit in rough pixels and two bits in smooth pixels to increase the hiding capacity. This method avoids large prediction-error expansion, thus achieving better image quality than conventional PEE. Coltuc [5] embedded data into the current pixel as well as its prediction context. This scheme obtains higher visual quality than classical PEE based on median-edge-detector (MED) or gradient-adjusted-predictor (GAP), since modifying four pixels minimizes the distortion introduced by data embedding. Bo et al. [2] generated a sequence consisting of prediction-error pairs and embedded data by expanding or shifting the 2D prediction-error histogram based on the sequence. Embedding in the correlations among prediction-errors rather than individual prediction-errors reduces the distortion.

The prior PEE schemes usually embed one bit, or two bits at most, into an expandable pixel. In this paper, a novel PEE algorithm based on Chinese Remainder Theorem is proposed. Compared with the previous PEE schemes, we first propose to embed six bits at most into one expandable pixel. In addition, we can adaptively achieve a trade-off of embedding capacity and visual quality. Experimental results show that the superiority of NNP^2 over other existing methods.

The rest of this paper is organized as follows. Section 1 introduces the Chinese Remainder Theorem briefly. Section 2 presents the proposed NNP^2 algorithm. Section 4 presents the experimental results and Section 5 concludes the paper.

2 Proposed Nearest Neighborhood Pixel Prediction (NNP^2) Algorithm

In this section we briefly explain the Chinese Remainder Theorem. Following that, our proposed algorithm is explained in detail.

2.1 Brief Introduction to Chinese Remainder Theorem

Chinese Remainder Theorem (CRT) provides a solution for a congruence system. A defined modulus set, $\{n_1, n_2, ..., n_m\}$, where m is a positive integer, and GCD(n_i, n_j) is equal to 1 for $i \neq j, i, j \in [0, m]$. For a positive integer X, there exists equations $x_i = X \bmod n_i$, where $i = 1, 2, ..., m$. The m-tuple $x_1, x_2, ..., x_m$ is unique for any $X \in [0, \prod n_i]$. A simple demonstration of CRT is briefly introduced here.

$$N = n_1 * n_2 * ... * n_m = \prod_{i=1}^{m} n_i \quad (1)$$

$$N_i = N/n_i \quad (2)$$

$$a_i = N_i^{-1} \bmod n_i \quad (3)$$

$$X = (\sum_{i=1}^{m} x_i * N_i * a_i) \bmod N. \quad (4)$$

Equations (1)-(4) above demonstrate the unique solution for the defined congruence system. X in Equation (4) tallies the m-tuple $\{x_1, x_2, ..., x_m\}$. The following example provides the detail implementation of Chinese Reminder Theorem In order to find an integer X for the congruence system, $\{n_1, n_2, n_3\} = \{3, 5, 7\}$ with a 3-tuple $x_1, x_2, x_3 = 2, 3, 2$. The computation process by using CRT is as follows.

$$\begin{aligned} N &= n_1 * n_2 * n_3 = 3 * 5 * 7 = 105. \\ N_1 &= N/n_1 = 105/3 = 35, \\ N_2 &= N/n_2 = 105/5 = 21, \\ N_3 &= N/n_3 = 105/7 = 15. \\ a_1 &= 2, a_2 = 1, a_3 = 1. \\ X &= (\sum_{i=1}^{m} x_i * N_i * a_i) \bmod N \\ &= (2 * 35 * 2 + 3 * 21 * 1 + 2 * 15 * 1) \bmod 105 \\ &= 23. \end{aligned}$$

Verification:

$$\begin{aligned} 23 \bmod 3 &= 2, \\ 23 \bmod 5 &= 3, \\ 23 \bmod 7 &= 2. \end{aligned}$$

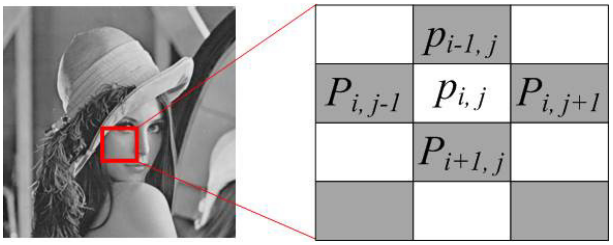


Figure 1: Rhombus prediction

The above example illustrated the Chinese remainder theorem.

2.2 Proposed Nearest Neighborhood Pixel Prediction (NNP^2) Algorithm

In this sub section, we explain the proposed NNP^2 algorithm, which uses CRT to embed data into digital images. NNP^2 can embed six bits, at most, into one expandable pixel by adjusting the modification size, whereas classical PEE schemes can embed a maximum of two bits in an expandable pixel. Laplacian-like distribution of prediction errors is employed to achieve a trade-off of embedding capacity and visual quality. Meanwhile, the rhombus prediction is exploited in order to find more expandable pixels. Simultaneously, we adopt the histogram shifting method to prevent overflow and underflow. In addition, we use a two-phase hiding strategy to transmit the side information to the receiver. Following sections outline the details of NNP^2.

2.2.1 Rhombus Prediction

In NNP^2, we exploit the rhombus prediction to express the high correlation of neighboring pixels. To calculate the prediction value of pixel $p_{i,j}$ in Figure 1, the rhombus prediction considers four neighboring pixels, $p_{i,j-1}$, $p_{i-1,j}$, $p_{i,j+1}$, and $p_{i+1,j}$. In Figure 1, all pixels of the host image are partitioned into two categories: "White" pixels and "Black" pixels. A "White" pixel is predicted by four neighboring "Black" pixels. Note that "White" and "Black" pixels are independent and the modification of "White" pixels do not influence any "Black" pixels, and vice versa. The central pixel, $p_{i,j}$ in Figure 1, can be predicted by its left, upper, right and lower pixels, $p_{i,j-1}$, $p_{i-1,j}$, $p_{i,j+1}$, and $p_{i+1,j}$. The prediction value $p'_{i,j}$ is calculated by Equation (5).

$$p'_{i,j} = \lfloor \frac{p_{i,j-1} + p_{i-1,j} + p_{i,j+1} + p_{i+1,j}}{4} \rfloor \quad (5)$$

2.2.2 Prediction Error Expansion

The data-embedding algorithm for "White" pixels is described as follows. We assume that two primes are p and q, $N = \log_2(q)$, a threshold $T = p*(q-1)$ and the secret file is SF.

The following steps demonstrate the prediction error expansion:

1) Calculate the prediction value $p'_{i,j}$ of "White" pixel $p_{i,j}$ using Equation (6).

2) Calculate the absolute value D of the difference between and using the following equation.

$$D = |p_{i,j} - p'_{i,j}| \quad (6)$$

3) If $0 \le D < p$, read N bits from SF and its decimal value is S, calculate an integer C by using CRT which satisfies that $D = C \bmod p$ and $S = C \bmod q$, and modify $p_{i,j}$ according to those N bits.

$$w_{i,j} = \begin{cases} p'_{i,j} + C \ , \mathrm{p_{i,j}} \ge \mathrm{p'_{i,j}} \\ p'_{i,j} - C \ , \mathrm{p_{i,j}} < \mathrm{p'_{i,j}} \end{cases} \quad (7)$$

where $w_{i,j}$ is the watermarked pixel value of $p_{i,j}$.

4) If $D \ge p$, shift T unit

$$w_{i,j} = \begin{cases} p_{i,j} + T \ , \mathrm{p_{i,j}} \ge \mathrm{p'_{i,j}} \\ p_{i,j} - T \ , \mathrm{p_{i,j}} < \mathrm{p'_{i,j}} \end{cases} \quad (8)$$

where $w_{i,j}$ is the watermarked pixel value of $p_{i,j}$.

The embedding algorithm calculates the prediction value of "White" pixels using "Black" pixels and embeds data into a "White" pixel. Therefore, after embedding in "White" pixels, "Black" pixels are unchanged and "White" pixels are modified as the watermarked pixels. "Black" pixels are considered to embed data by using "White" pixels to calculate their prediction value in the same way. Therefore, the usage of both "White" and "Black" pixels almost double the hiding capacity.

After receiving the watermarked image, the receiver can extract the hidden message by using the same scanning method as used during the embedding algorithm. The receiver calculates the absolute value of the difference C' between the watermarked pixel, $w_{i,j}$, and the prediction value, $p'_{i,j}$. Then, the hidden message can be extracted by

$$S = C' \bmod (q), 0 \le C' < p \times q \quad (9)$$

where S is the decimal value of original N secret bits. Then the original pixel value of $w_{i,j}$ can be recovered by implementing the following equations,

$$D = \begin{cases} C' \bmod (p) \ , 0 \le \mathrm{C'} < \mathrm{p} \times \mathrm{q} \\ C' - T \ , \mathrm{p} \times \mathrm{q} \le \mathrm{C'} \end{cases} \quad (10)$$

$$p_{i,j} = \begin{cases} p'_{i,j} + D \ , \mathrm{w_{i,j}} \ge \mathrm{p'_{i,j}} \\ p'_{i,j} - D \ , \mathrm{w_{i,j}} < \mathrm{p'_{i,j}} \end{cases} \quad (11)$$

Consequently, the receiver can acquire the exact copy of the original image together with the hidden message.

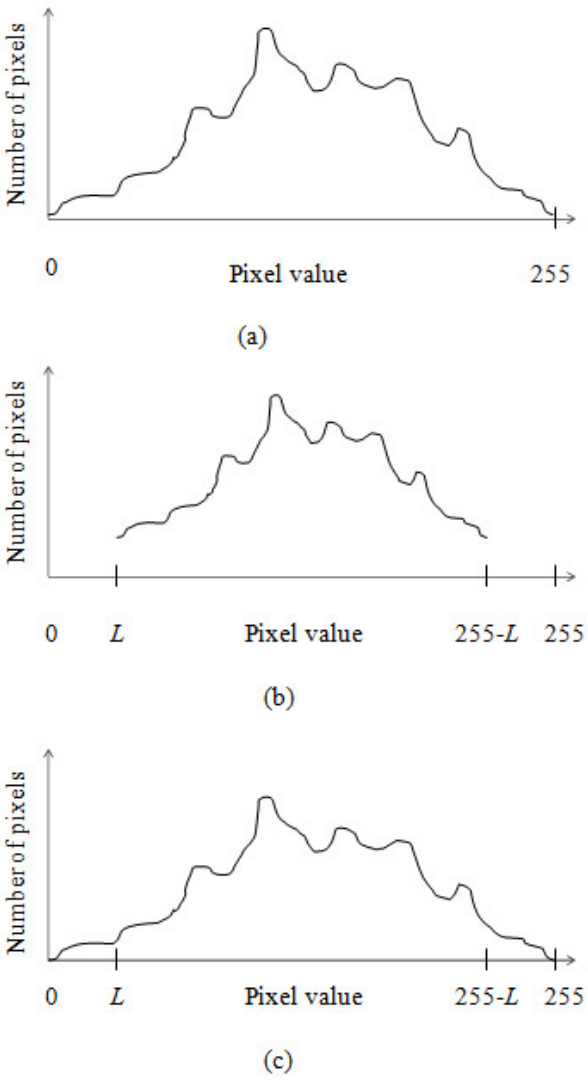


Figure 2: Histograms: (a) histogram of host image, (b) histogram after shifting, and (c) histogram after embedding.

2.2.3 Prevention of Overflow and Underflow

The overflow and underflow problem may occur when watermarked pixels are out of the range of [0, 255]. To prevent these potential issues, we employ a histogram shifting scheme in [8] to shift the histogram from both left and right sides as shown in Figure 2. Assume that two primes used in NNP^2 are p and q, the maximum modification size is $L = p \times q - p$. Therefore, we shift the histogram of host image L units from both left and right sides.

After shifting all potential overflow and underflow pixels, we should construct a one-bit location map to record the histogram shifting information. If a pixel's grayscale value is in the range of [L, 255-L], then we assign a "0" as its location information; otherwise, a "1" is assigned to it. We compress the location map by using the run length-coding algorithm, which can achieve great compression efficiency for overflow and underflow pixels when their numbers are few and consecutive. In NNP^2, the maximum modification size is L. Therefore, shifting the histogram of the host image from both the left and right side by L units can prevent overflow and underflow. Note that the extra information including p, q, and the location map should be transmitted to the receiver to extract the hidden message and recover the host image correctly. For this purpose, we adopt a two-stage embedding strategy to embed extra information together with secret data.

2.2.4 Upper Bound of p and q

NNP^2 uses two primes, p and q, to adjust the range of embeddable pixels and the number of secret bits one embeddable pixel can embed. The larger the p and q values are, the higher the embedding capacity is. However, to prevent overflow and underflow, the histogram of host image is shifted $L = p \times q - p$ units. Pixels with values in [0, L-1] are shifted to [L, 2L-1], and pixels with values in [256-L, 255] are shifted to [256-2L, 255-L]. To distinguish overflow pixels from underflow pixels, p and q must satisfy that $2L - 1 < 256 - 2L$, namely $p \times q - p < 257/4$.

Based on the above condition, while p and q are both integers, we can derive that $p \times q - p < 64$. We set q as a multiple of 2, such as 2, 4, 8, 16, 32 or 64, which means one pixel can embed 6 bits at most.

2.2.5 Two-stage Embedding

Extra information, namely two primes, p and q, and the location map, are sent to the receiver to extract hidden message and recover the host image. Note that $L = p \times q - p$, and there is no need to transmit. Assume that $|LM|$ is the size of the location map. The LSB values of the first $2 \times 6 + |LM|$ pixels of the watermarked image are replaced with $p, q (2 \times 6$ bits) and the location map ($|LM|$ bits). The original $2 \times 6 + |LM|$ LSB values are added to the payload. Therefore, the pure capacity, C, which excludes all extra information, is

$$C = |N_s| - |EI| \tag{12}$$

where $|N_s|$ is the number of secret bits and $|EI|$ is the size of extra information.

3 Experimental Results and Discussion

We have conducted several experiments to evaluate the performance of NNP^2 and compare it with some existing RDH algorithms. Figure 3 shows six typical grayscale images of size 512×512 that were used as test images.

Table 1 shows the pure payload, C, and the PSNR of different test images when p and q are set to be 1 and 2. We can see that the number of expandable pixels, N_e, is highly variable between different images. Smoother images, such as F-16, result in a larger N_e than that of more complex images, like Baboon. We also have observed that

Table 1: Embedding capacity and PSNR for six test images with $p = 1$ and $q = 2$

Host image (512×512)	N_e	**Pure capacity** C **(bits)**	**Extra information** $\|EI\|$ **(bits)**	**PSNR (dB)**	**Bit rate (bpp)**
Lena	34096	34037	32	48.42	0.1298
Baboon	9625	9493	132	48.22	0.0362
Boat	33432	33400	32	48.42	0.1274
F-16	53199	53167	32	48.60	0.2028
Peppers	20250	20218	32	48.30	0.0771
GoldHill	24245	24213	32	48.34	0.0924

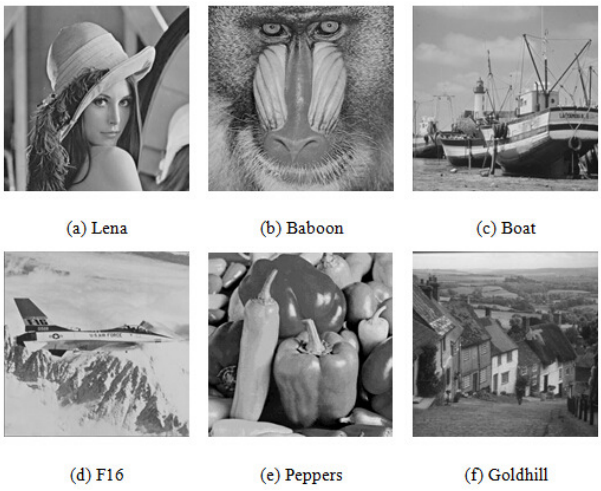


Figure 3: Six test images

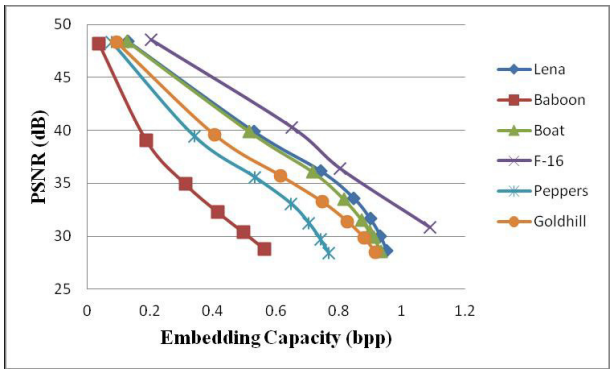


Figure 4: Performance of test images with optimal p and q

all test images except for Baboon have no pixels out of the range [1, 254]. For Lena, the size of location map is $|LM| = 20$ bits when we use the run-length coding algorithm to compress the location map. Thus, the size of extra information is $|EI| = (2 \times 6) + |LM| = 32$ bits.

Table 2 shows several experiments to evaluate the pure embedding capacity versus the PSNR change with different p and same q. An expandable pixel, which can only embed one bit for q, is constantly equal to 2, while p is equal to $2i + 1, i[0, 6]$, which is the threshold of expandable pixels whose absolute value of prediction errors are less than p. We can see that the average PSNR values decrease with increasing p values. However, the growth of the pure embedding capacity is smaller when the size of extra information is growing increasingly larger. In Table 3, we assign p a constant value of 1, and q changes from 2 to 64. This means that only a pixel with a prediction error of 0 is expandable, and one pixel embeds 1 to 6 bits. We observed that the pure embedding capacity will increase and then decrease while q changes from 2 to 64. The embedding capacity increase first for one pixel can embed several bits, but when q is much bigger, the size of extra information increases faster, and the embedding capacity decreases. By adjusting the values of p and q, NNP^2 can adaptively achieve a high embedding capacity with little loss of visual quality.

Figure 4 presents the performance of NNP^2 for test images with optimal p and q values. We can see from the figure that smooth images, like F-16, achieve higher embedding capacity with the same PSNR values, while complex images, like Baboon, will experience severe distortion when the embedding capacity is higher. Therefore, when implementing NNP^2 , images with high correlation perform better than those with low correlation.

We also compare the embedding capacity (bpp) versus image quality (dB) of NNP^2 with that of existing RDH schemes for Lena, as shown in Figure 5. NNP^2 can embed six bits at most, rather than one or two bits, into the prediction error and shift all the non-embeddable pixels. It should be noted that [12] and [8] are histogram-based RDH schemes, which embed data into peak points and just shift the pixels between peak points and zero points rather than all non-embeddable pixels, thus achieving a high embedding capacity while keeping a low distortion rate. Based on the above reasons, the PSNR of NNP^2 is lower than that of the compared methods [12] and [8] when embedding the same number of bits into one expandable pixel. However, proposed algorithm can achieve a trade-off between the embeddable pixels and the number of secret bits that one embeddable pixel can embed. It should be noted that the proposed NNP^2 achieved a higher embedding capacity than those of existing schemes

Table 2: Pure embedding capacity for test images with $q = 2$

Host image (512×512)	$p = 1$	$p = 3$	$p = 5$	$p = 7$	$p = 9$	$p = 11$	$p = 13$
Lena	0.1298	0.5288	0.7424	0.8468	0.8998	0.9316	0.9509
Baboon	0.0362	0.1876	0.3117	0.4140	0.4968	0.5627	0.6151
Boat	0.1247	0.5156	0.7165	0.8152	0.8724	0.9089	0.9332
F-16	0.2028	0.6505	0.8039	0.8729	0.9111	0.9355	0.9522
Peppers	0.0771	0.3405	0.5329	0.6474	0.7045	0.7409	0.7671
GoldHill	0.0924	0.4047	0.6129	0.7461	0.8270	0.8799	0.9143
Average PSNR	48.38	39.69	35.81	33.24	31.30	29.72	28.38

Table 3: Pure embedding capacity for test images with $p = 1$

Host image (512×512)	$q = 2$	$q = 4$	$q = 8$	$q = 16$	$p = 32$	$p = 64$
Lena	0.1298	0.2374	0.3106	0.3680	0.4025	0.0939
Baboon	0.0362	0.0707	0.0914	0.1069	0.0541	-0.8490
Boat	0.1247	0.2298	0.3081	0.3663	0.2778	0.2048
F-16	0.2028	0.3561	0.4536	0.5394	0.5939	0.1090
Peppers	0.0771	0.1347	0.1360	0.0945	0.1098	-0.1639
GoldHill	0.0924	0.1726	0.2338	0.2751	0.1826	-0.1671
Average PSNR	48.38	38.87	31.49	24.84	18.52	12.34

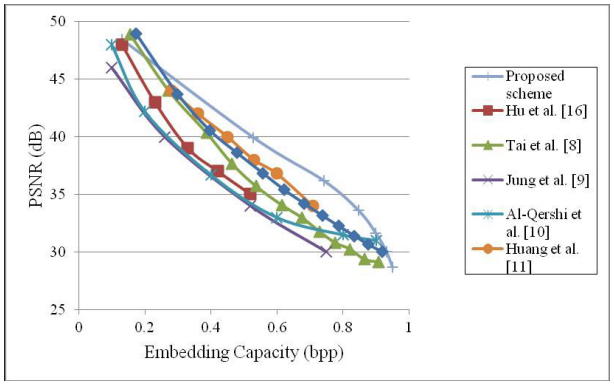


Figure 5: Performance comparison for Lena of NNP^2 and existing RDH schemes

with low distortion. As a result, NNP^2 can obtain better performance in RDH schemes by adjusting the embedding capacity and image quality.

4 Conclusions

In this paper, we proposed NNP^2 to embed data into prediction errors by using CRT to control the modification size. Laplacian-like distribution of prediction errors, which is centered with 0, increases the embedding ability of NNP^2. Also, we control the number of embeddable pixels by adjusting the threshold of prediction errors and embed one to six bits at most into one embeddable pixel that leads to the best performance. We also adopt a two-stage strategy to embed the extra information, rather than sending it to the receiver in an open way. In addition, we use a histogram shifting technique to prevent overflow and underflow. As a result, NNP^2 outperformed the compared algorithms.

Acknowledgments

This work was supported by the National Nature Science Foundation of China under Grant No. 61201385.

References

[1] Q. M. Al-Qershi and B. Ee Khoo, "Two-dimensional difference expansion (2d-de) scheme with a characteristics-based threshold," *Signal Processing*, vol. 93, pp. 154–162, 2013.

[2] Ou Bo, X. Li, et al., "Pairwise prediction-error expansion for efficient reversible data hiding," *IEEE Transactions on Image Processing*, vol. 22, no. 12, pp. 5010–5021, 2013.

[3] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: an overview and a classification," *EURASIP Journal on Information Security*, vol. 2010, pp. 1–19, 2010.

[4] Ya Fen Chang and Wei Liang Tai, "Histogram-based reversible data hiding based on pixel differences with

prediction and sorting," *KSII Transaction on internet and information systems*, vol. 6, no. 12, pp. 3100–3116, 2012.

[5] D. Coltuc, "Low distortion transform for reversible watermarking," *IEEE Transactions on Image Processing*, vol. 21, no. 1, pp. 412–417, 2012.

[6] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for JPEG images," *IEEE Transactions on Image Processing*, vol. 21, no. 1, pp. 412–417, 2001.

[7] Y. Hu and B. Jeon, "Reversible visible watermarking and lossless recovery of original images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 11, pp. 1423–1429, 2006.

[8] Y. Hu, H. K. Lee, et al., "De-based reversible data hiding with improved overflow location map," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 2, pp. 250–260, 2009.

[9] H. C. Huang and F. C. Chang, "Hierarchy-based reversible data hiding," *Expert Systems with Applications*, vol. 40, pp. 34–43, 2013.

[10] T. Jun, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[11] S. W. Jung, S. J. Ko, et al., "A new histogram modification based reversible data hiding algorithm considering the human visual system," *IEEE Signal Processing Letters*, vol. 18, no. 2, pp. 95–98, 2011.

[12] L. Kamstra and J. A. M. H. Henk, "Reversible data embedding into images using wavelet techniques and sorting," *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2082–2090, 2005.

[13] X. Li, B. Yang, et al., "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Transactions on Image Processing*, vol. 20, no. 12, pp. 3524–3533, 2011.

[14] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[15] V. Sachnev, J. K. Hyoung, et al., "Reversible watermarking algorithm using sorting and prediction," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 7, pp. 989–999, 2009.

[16] Y. Q. Shi, Z. Ni, D. Zou, C. Liang, and G. Xuan, "Lossless data hiding: fundamentals, algorithms and applications," in *Proceedings of the 2004 IEEE International Symposium on Circuits and Systems (ISCAS'04)*, vol. 2, pp. II–33, 2004.

[17] W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 6, pp. 906–910, 2009.

[18] D. M. Thodi, J. R. Jeffrey, et al., "Expansion embedding techniques for reversible watermarking," *IEEE Transaction Image Processing*, vol. 16, no. 3, pp. 721–730, 2007.

K. Bharanitharan (S07CM09) received the PhD degree in Electrical Engineering from the National Cheng Kung University, Tainan, Taiwan, in 2009. In 2005, he won outstanding international student fellowship award at National Cheng Kung University. He serves as a reviewer for IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transactions on Very Large Scale Integration Systems, IEEE Transactions on Evolutionary Computation, IEEE Signal processing letter, IEEE Transactions on Very Large Scale Integration Systems since 2009. He has published more than sixteen research papers in highly reputed journals and conferences. His research interests include H.264/AVC video coding, HEVC, scalable video coding, image processing, multiview video coding, and associated VLSI architectures. His research works also include Multi-Core reconfigurable systems, Java based apps development and dynamic power management for advanced video coding.

Chin-Chen Chang obtained his Ph.D. degree in computer engineering from Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in Computer and Decision Sciences. Both were awarded in Tsing Hua University. Dr. Chang served in Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in Chung Hsing University, chair professor in Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan. Professor Chang's specialties include, but not limited to, data engineering, database systems, computer cryptography and information security. A researcher of acclaimed and distinguished services and contributions to his country and advancing human knowledge in the field of information science, Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. He also published more than 1200 papers in Information Sciences. In the meantime, he participates actively in international academic organizations and performs advisory work to government agencies and academic organizations.

Hai-Rui Yang received the BS degree in software engineering in 2012 from the Dalian University of Technology,

Dalian, China. Since September 2012, he has been studying for his MS degree in software engineering in Dalian University of Technology, Dalian, China. His current research interests include information hiding and image processing.

Zhi-Hui Wang received the BS degree in software engineering in 2004 from the North Eastern University, Shenyang, China. She received her MS degree in software engineering in 2007 and the PhD degree in software and theory of computer in 2010, both from the Dalian University of Technology, Dalian, China. Since November 2011, she has been an assistant professor of Dalian University of Technology. Her current research interests include information hiding and image processing.

Secured Genetic Algorithm Based Image Hiding Technique with Boolean Functions

Krishna Bhowal, Debasree Sarkar, S. Biswas, and Partha Pratim Sarkar
(Corresponding author: Krishna Bhowal)

Department of Engineering and Technological Studies, University of Kalyani
Pin - 741235, west Bengal, West Bengal, India (Email: ykbhowal@yahoo.co.in)
(Received Sept. 29, 2014; revised and accepted Jan. 16 & June 21, 2015)

Abstract

Steganography and Watermarking are main parts of the fast developing area of information hiding. Steganography involves hiding of information in a cover media to obtain the stego media, in such a way that the cover media is supposed not to have any embedded image for its unintended recipients. This paper is based on Steganography, Watermarking and Cryptography system where image bits are embedded into higher random LSB layers of audio signals, resulting in increased robustness against noise addition. On the other hand, multi-objective Genetic Algorithm is used to minimize the deviation between original media and embedded media. The basic idea of this paper is to improve security so that probability of detecting the presence of hidden information into cover media is about to zero. For this improvement, image embedding random position numbers are converted to functions and these functions are sent using Symmetric-key encryption algorithm to the receiver end. Key distribution problem is solved by RSA algorithm. We evaluated performance based on imperceptibility, security, robustness, and hiding capacity.

Keywords: Artificial intelligence, genetic algorithm, steganography, watermarking

1 Introduction

Steganography, watermarking and fingerprinting are branches of information hiding. In a computer-based data hiding techniques in audio, secret image is hidden in digital audio signal so that they can be extracted at the receiving end with the help of a secret key and not merely to obscure its presence. The secret image is embedded by slightly altering binary sequence of audio signals.

Multimedia data hiding techniques have developed a strong basis of growing number of applications like copyright protection, authentication, tamper detection, covert communications etc. Following requirements must be satisfied in several applications [5, 6, 31, 32].

Perceptual Transparency: The main focus of this paper is on perceptually undetectable or transparent data-embedding and watermarking techniques. In many applications, such as covert communication, copyright and usage tracking, embedding metadata or additional information, the algorithms must embed data without affecting the perceptual quality of the underlying host signal.

Recovery of Data without Access to Original Signal: In most of the applications such as covert communication, data-embedding algorithms do not have access to the original audio signal while extracting the embedded signal. This inability to access the original signal limits the amount of data that can be embedded in a given host signal.

Bit Rate of Data-Embedding Algorithm: Some applications of data embedding require small amounts of information to be incorporated. On the other hand, many applications of data embedding, e.g., covert communication, require a lot of bandwidth. The ability to embed large quantities of data in a host signal will depend on how the embedding algorithm has been designed. Our algorithm can adapt large amount of information to the underlying host signal.

Robustness: Digital data are modifiable and manipulate-able using computers and widely available software. Operations that damage the host signal also damage the embedded data. Again, third parties may attempt to modify the host signal to detect of the embedded data. Basic requirement of steganography imposes that the presence of hidden information within the stego-cover media should be undetectable. There should be no perceptible difference between the watermarked and original signal, and the watermark should be difficult to remove or alter without damaging the host signal.

Security: A secure data-hiding procedure can only be broken by the authorized user has access to a se-

cret key that controls the insertion of the data in the host signal. This requirement is very important in covert communication scenarios. Hence, a data-hiding scheme is secure if knowing the exact algorithm for embedding the data does not help an unauthorized party to detect the presence of embedded data. An unauthorized user should also be unable to extract the data in a reasonable amount of time. Basic Data hiding process has been shown in Figure 1.

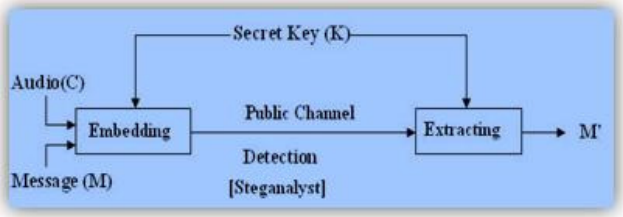


Figure 1: Basic data hiding process

LSB coding is one of the earliest techniques studied in the information hiding area of digital audio. The main advantage of the LSB coding method is a very high channel bit rate and a low computational complexity of the algorithm, while the main disadvantage is considerably low robustness against signal processing modifications. Since substitution techniques usually modify the bits of lower LSB-layers in the samples, it is easy to reveal the hidden image if the low transparency causes suspicious. In order to conceal secret image successfully, a variety of methods for embedding information in digital audio have been introduced [1, 4, 6, 7, 8, 12, 16, 21, 28, 31].

It is well known that LSB-layers bits in samples are more suspicious, so embedding the image bits other than LSB-layers could be helpful to decrease the perceptibility and to increase the robustness. The basic idea of this research work is to provide a novel method to hide the secret data from intruders at high random LSB layers. Then the secret data will be sent to the destination in safer and secure manner. The quality of sounds depends on the length of the image and size of the audio which are selected by the users. Even though it shows changes in bit level deviations in the frequency chart, as a whole we cannot determine the change in the audio. Here the technical challenge is to provide transparency and robustness which are conflicting requirements. The perceptibility and extraction of hidden information of the proposed algorithm is more challenging as well, because there is a significant number of bits flipped in a number in bit layers. On the other hand, image retrieval from random higher LSB layers is still one of the major drawbacks of the modified LSB methods. In this paper, we have been used Boolean functions to extract the hidden information location numbers.

The remainder of the paper is organized as follows: Section 2 discusses related works done by different researchers. Section 3 explains proposed work. Section 4 discusses experimental results. Section 5 highlights advantages of our approach. Section 6 concludes the paper presented here.

2 Related Works

Being a simple method, a very high level of security is not achieved in LSB insertion method. To improve security, different modified-LSB methods are proposed by different researchers. Apart from security, certain other parameters like complexity, computational load, SNR, Bit Error Rate, efficiency, etc are also considered for information hiding techniques.

In [31] a solution of supporting different audio formats and reducing the time for encoding and decoding are discussed. Data is embedded in such a way that each character requires eight 254/255 bytes.

In [6] a two steps method is proposed where data are embedded from the fourth to sixth LSB layers with minimum distortions. First, secret bit is embedded in any higher LSB layer. Second, changes white noise properties by shaping the impulse noise which is caused by the embedding bit. In [7, 8] the hearing threshold in the temporal domain is calculated which is exploited as the embedding threshold, yielding more capacity compared to uniform embedding pattern. Proposed method uses compression of information using lossless compressor, thus increasing total bit rate. In [28] an algorithm is proposed for both image and audio steganography. Regarding audio steganography, it states the technique of echo hiding. Data is embedded in the echo signal varying its parameters like decay rate, offset and amplitude. The original signal is segmented into blocks and each block is given the value 0 or 1 depending upon the secret message. The original signal is echoed and the message is embedded into it. At the receiver end, auto correlation and decoding is done to separate the secret signal and the original signal.

In [21] a robust steganographic method is proposed where data are embedded in the multiple, vague and higher LSB layers. Generally there are two types of attacks namely unintentional attacks and intentional attacks, solutions are suggested for both these type of attacks in this work. The data bits are embedded in the bit other than 1st LSB bit to stop the intentional attack. The bits other than the selected bits for embedding are altered to reduce the distortion. In [12] two LSB methods are proposed. First method is parity coding and the other is XORing of LSB. Initially embedding capability is measured by ensuring that the size of the message to be embedded is less than the cover audio signal. In parity method, the parity bit is considered before directly replacing the LSB. Depending upon the message bit to be embedded, the LSB is either flipped or retained. If the message bit is 0, LSB has to be modified in such a way that parity of the sample is even. If the message bit is 1, LSB is modified in such a way that parity of the sample is odd. In second method, XORed operation be-

tween the LSB and the next bit has to be equivalent to the message bit to be embedded. If equal, the LSB is retained otherwise LSB is flipped. Also they reduce the computational load and the capacity of the cover audio is increased. From experimental results it is found that the encryption with steganography provides better security. Embedding data in the higher LSB layers is prone to less attack than those embedded in the lower layers. But embedding in higher LSB will result in distortion. Therefore further steps have to be included to reduce these distortions.

The idea proposed by [16] is based on psycho acoustic theory of persistence and phase shifting. Persistence of hearing is based on the fact that two sounds successively with a difference of less than one-tenth of a second hit our ears, then the difference between the sounds is imperceptible. It is called the phase shift, the change of which is same as the shift in time. Author used uncompressed audio format (WAV format). In [1] the author has shifted the LSB embedding to the eight bit resulting in slight increase of robustness. However, the hiding capacity will be decreased since some of the samples are to be left unchanged to preserve the audio perceptual quality of the audio signal. In [2, 11, 15, 17, 22, 29, 33, 34], different embedding procedures are followed to hide data in image or audio file. Most of the cases they explained how to hide the information in to medium but how to extract the hidden data from medium at receiver end is not clearly mentioned. It does not raise suspicions that an important message can be possibly carried inside a harmless medium in steganography describes in [14]. Hiding a secret message in order to protect the copyright of a product is the main aims in watermarking are discussed in [3, 18, 25, 26, 30]. To demonstrate its authenticity, namely, its content originality also referred as content verification, or tamper proofing in [2]. An adversary tries to reveal the information carried by a stego-medium. In the case of watermarking, an opponent either tries to remove the watermark in order to violate copyright or to reproduce it after product tampering in order to achieve a false positive content verification.

The easiness of image retrieval is still one of the major drawbacks of the LSB and its variant, knowing by fact that embedded bits are at sixth or eighth position from the stego audio signal. To solve this problem, Boolean functions have been introduced in this paper by which we can easily extract hidden bits embedded in different random LSB positions at the receiving end.

3 Proposed Work

3.1 Best Sample selection using Genetic Algorithm

Genetic Algorithms are adaptive heuristic search algorithm based on the evolutionary ideas of natural selection and genetics. Unlike AI systems, they do not break easily even if the inputs changed slightly, or in the presence of reasonable noise. Also, in searching a large state-space, a genetic algorithm may offer significant benefits over more typical search of optimization techniques.

A population of individuals is maintained within search space for a GA, each representing a possible solution to a given problem. Each individual is coded as a finite length vector of components, or variables, in terms of some alphabet, usually the binary alphabet 0, 1. To continue the genetic analogy these individuals are likened to chromosomes and the variables are analogous to genes. Thus a chromosome (solution) is composed of several genes (variables). A fitness score is assigned to each solution representing the abilities of an individual to 'compete'. The individual with the optimal (or generally near optimal) fitness score is sought. The GA aims to use selective reproduction of the solutions to produce 'offspring' better than the parents by combining information from the chromosomes.

The following points convinced us to use genetic algorithm in this work

1) To maintain the randomness in selection of bit level of audio sample for hiding secret bit.

2) Through GA based crossover and mutation operations on audio sample (chromosome) we may get better set (population) of audio samples than previous generation population.

3) Using the concept of fitness value in GA we may select better or best audio sample from the population of audio samples generated in the previous step.

4) We may consider fitness value is a position number of audio sample where secret bit may be embedded and for which deviation between original audio sample and stego-audio sample is minimized.

5) Using the concept of Multi-objective GA, position number of audio sample where secret bit is embedded may be used

   a. As a Fitness value to select the best chromosome (audio sample).

   b. To extract the hidden secret bit from the stego-audio at the receiving end.

3.2 Steps to Embed Image into Audio File Using Proposed Modified LSB Scheme

1) Read image file and generate byte streams.

2) Read audio file and generate byte streams, convert byte streams to 16 bit audio samples.

3) Obtain n number of chromosomes of 16 genes by inserting two image bits into 16 bits audio sample at n (2 to16) random positions.

4) Apply following GA operator based insertion algorithm to generate better next generation population:

   a. Let pos be the image bit insertion position into the audio sample;

   b. Let $fm(pos)$ be mutation operation on pos position;

   c. Let $fc1(start, end)$ be crossover operation from start to end by 1 and $fc0(start, end)$ be crossover operation from start to end by 0.

   d. If pos = 1, then take no action;

   e. If pos = 2 to 16 then do the following

      i. If image bit is 0 and audio bit is 1 for pos = i;

      ii. If audio bits on 1 to (i-1) positions are holding 0s, then perform $fc1(1, i-1)$ operation;

      iii. If audio bits on 1 to (i-1) positions are holding 1s and on (i+1) position holding 0, then perform $fc0(1, i-1)$ and $fm(i+1)$ operations.

      iv. If image bit is 1 and audio bit is 0 for pos = i;

      v. If audio bits on 1 to (i-1) positions are holding 1s, then perform $fc0(1, i-1)$ operation;

      vi. If audio bits on 1 to (i-1) positions are holding 0s and on (i+1) position holding 1, then perform $fc1(1, i-1)$ and $fm(i+1)$ operations;

      vii. If audio bit on (i+1) and (i-1) positions are holding 0/1 and 1/0 respectively, take no action;

      viii. If audio bit and image bit is same, then no action is to be taken as there will be no deviation between two samples.

5) Now, the best chromosome has been selected, where best one is the chromosome (audio sample) which has the minimum deviation compare to the original 16 bit audio sample.

6) Here fitness value represents the position number for which we get the best chromosome. Again, the position number, best chromosome and distortion are closely related as selection of the best chromosome will reduce the distortion.

7) Fitness value is representing two things here:

   a. Position number which is very important at the receiving end to extract the image.

   b. Distortion which again very important regarding security (distortion can convinced hacker to hack the image).

   So, multi-objective GA is used here.

8) Secret-Bit-Insertion Positions have been stored in Position Arrays during this embedding process.

9) Stego-audio byte streams have been written into audio file.

10) Boolean functions have been generated from the Position Arrays are described in the next section.

Boolean Functions Generation from Position Arrays:

Let S be size of the Position Array.

S_{bin} be binary representation of $S-1$.

N be number of bits required for S_{bin}.

Suppose A_{ij} be a Position Array where i = 0 to S - 1, j = 0 to 1. Here $A_{i,0}$ represents Array index and $A_{i,1}$ represents Position numbers.

$IPA_N(A_{i,0})$ be N bits binary representation of Index i of Position Array, where i = 0 to S - 1;

$IPA_3(A_{i,1})$ be 3 bits binary representation of Index i of Position Array, where i = 0 to S - 1;

Now we get a Matrix $M_{i,N+3}$ by combining $IPA_N(A_{i,0})$ and $IPA_3(A_{i,1})$. Elements of this matrix are 0 or 1.

$$\begin{aligned} MSB(i) &= MSB \quad \text{bit set of Position Array} \\ &= MSB(IPA_3(A_{i,1})) \\ &= M_{i,N+1} \\ MdSB(i) &= \text{Middle bit set of Position Array} \\ &= MdSB(IPA_3(A_{i,1})) \\ &= M_{i,N+2} \\ LSB(i) &= \text{LSB bit set of Position Array} \\ &= LSB(IPA_3(A_{i,1})) \\ &= M_{i,N+3}. \end{aligned}$$

where $i = 0$ to $S-1$. Again,

$$\begin{aligned} MSB(i)_{minterm} &= \text{i's where } M_{i,N+1} = 1 \\ MdSB(i)_{minterm} &= \text{i's where } M_{i,N+2} = 1 \\ LSB(i)_{minterm} &= \text{i's where } M_{i,N+3} = 1 \\ SOP(MSB(i)_{minterm}) &\longrightarrow f_x(a, b, \cdots, N \text{ terms}) \\ SOP(MdSB(i)_{minterm}) &\longrightarrow f_y(a, b, \cdots, N \text{ terms}) \\ SOP(LSB(i)_{minterm}) &\longrightarrow f_z(a, b, \cdots, N \text{ terms}) \end{aligned}$$

Here Size of the Position Array need to be sent to the receiver.

The functions and size of the Position Array has been encrypted using Shared Key AES encryption algorithm.

The Shared Key has been encrypted using Public Key RSA algorithm.

3.3 Steps to Extract Hidden Image from Stego-Audio File

Deviation between audio samples and stego-audio samples has been minimized during the proposed embedding method. So stego-audio is almost equal to the original audio. By getting the image hidden position numbers i.e., Position Array, we can easily extract the hidden image from audio file as follows:

1) Read stego-audio file and generate byte streams, convert byte streams to 16 bit audio samples.

2) Decrypt the Shared Key using the receiver Private Key of RSA.

3) Decrypt the functions and size of the Position Array using Shared Key of AES algorithm.

4) The position numbers of the secret (image) bits have been extracted using the Boolean functions and size of the Position Arrays is described below.

   We have f_x $(a, b, c, \cdots, N$ terms), $f_y(a, b, c, \cdots, N$ terms) & $f_z(a, b, c, \cdots,$ upto N terms) and $IPA_N(A_{i,0})$ for i = 0 to S - 1.

   For index i = x, x has been converted to binary number of N bits like $b_1, b_2, ..., b_N$.

   Assigning $a = b_1, b = b_2, c = b_1, ...$;

   Using f_x(a, b, c,.... upto N terms) we get bit b11;

   Using f_y(a, b, c,.... upto N terms) we get bit b12;

   Using f_z(a, b, c,.... upto N terms) we get bit b13;

   Finally the bit pattern b11b12b13 is generated;

   The secret bit position numbers has been generated by converting this bit pattern to decimal number for index i=x and hidden image bits has been extracted from audio file.

5) The image bits have been converted to bytes and original image has been generated from image bytes.

3.4 Transferring Embedding Position Numbers to the Receiver end in Terms of Boolean Functions: An Example

Following Boolean algebra terms are used to generate Boolean functions: - midterm, Sum of Product, Minimization etc. Let the size of the Position Array is 8 and the corresponding positions of image bits are 2,4,6,1,7,4,6,5.

Here Indexed Position Array and Equivalent Binary Representation are explained in Table 1 and Table 2.

Now MSB bit set X= [0,1,1,0,1,1,1,1]. So, Midterm for MSB is [1,2,4,5,6,7]. And Sum of Product $X = a'b'c + a'bc' + ab'c' + abc' + abc + ab'c$.

Minimization of X:

Table 1: Indexed position array

Index	Position
0	2
1	4
2	6
3	1
4	7
5	4
6	6
7	5

Table 2: Equivalent binary representation

a	**b**	**c**	**X**	**Y**	**Z**
0	0	0	0	1	0
0	0	1	1	0	0
0	1	0	1	1	0
0	1	1	0	0	1
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	1	1	0
1	1	1	1	0	1

Pass 0: $a'b'c + a'bc' + ab'c + abc' + abc + ab'c$;

Pass 1: $a'b'c + ab'c$ reduce to $b'c$; $a'bc' + abc'$ reduce to bc'; $ab'c + ab'c'$ reduce to ab'; $abc' + abc$ reduce to ab;

Pass 2: $ab' + ab$ reduce to a. Finally $X = a + b'c + bc'$. Middle bit set Y=[1,0,1,0,1,0,1,0]. So Midterm of Y is [0,2,4,6].

Sum of Product $Y = a'b'c' + a'bc' + ab'c' + abc'$.

Minimization of Y:

Pass 0: $a'b'c' + a'bc' + ab'c' + abc'$;

Pass 1: $a'b'c' + a'bc'$ reduce to $a'c'$; $ab'c' + abc'$ reduce to ac'; $a'c' + ac'$ reduce to c';

Pass 2: c'; Y = c';

LSB bit set Z=[0,0,0,1,1,0,0,1]. So Midterm of Z is [3,4,7]. Sum of Product $Z = a'bc + ab'c' + abc$.

Minimization of Z:

Pass 0: $a'bc + ab'c' + abc$;

Pass 1: $a'bc + abc$ reduce to bc;

Pass 2: $bc + ab'c'$.

So, the three functions are given below

$$\begin{aligned} X &= a + b'c + bc'; \\ Y &= c'; \\ Z &= bc + ab'c'. \end{aligned}$$

Continuing with the previous example, for the input of the binary of (0-7), we get three outputs from the functions X, Y and Z. Extraction of position number explained in Table 3.

Table 3: Index to position number conversion

a	b	c	X	Y	Z
0	0	0	0	1	0
0	0	1	1	0	0
0	1	0	1	1	0
0	1	1	0	0	1
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	1	1	0
1	1	1	1	0	1

Example 1. *For the Index 7,* $a = 1$, $b = 1$, $c = 1$,

$$\begin{aligned} X &= a + 0.1 + 1.0 = 1 \\ Y &= 0 \\ Z &= 1.1 + 1.0.0 = 1 \end{aligned}$$

So $XYZ = 101$*, i.e., is equal to 5.*

Same way will get the position numbers 2, 4, 6, 1, 7, 4, 6.

4 Experimental Results

Among the various image file format, the image which is smaller in size has been considered in this work. The JPG file is wonderfully small in size, often compressed to perhaps only 1/10 of the size of the original data. JPEG files achieve a smaller file size by compressing the image in a way that retains detail which matters most, while discarding details deemed to be less visually impactful. It supports 8-bit grayscale images and 24-bit color images (8 bits each for red, green, and blue). Here a 24-bit 64 × 64 color JPEG image has been hidden in the audio file. JPEG file have been read in Java as like below:

BufferedImage originalImage = ImageIO.read(new File("rocket.jpg"));

Proposed LSB information hiding algorithm has been tested on 5 audio sequences from different music styles (classic, jazz, country, pop, rock). The audio experts were selected so that they can represent a broad range of music genres, i.e. audio clips with different dynamic and spectral characteristics. The image has been embedded in all music pieces using the proposed and standard LSB algorithm. Clips were 44.1 kHz sampled mono audio.wav files, represented by 16 bits per sample. Duration of the samples ranged from 10 to 15 seconds.

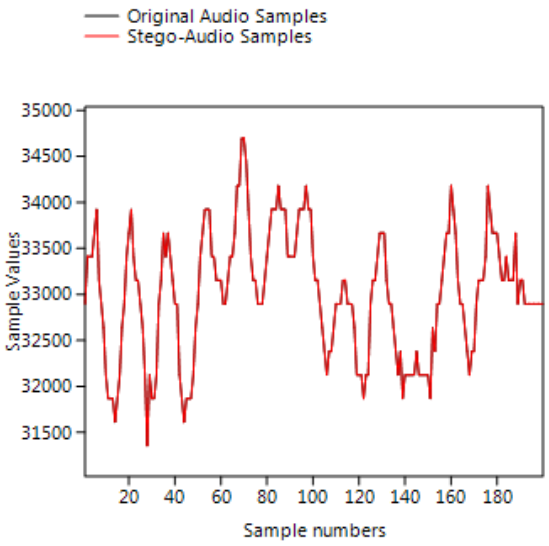


Figure 2: Negligible deviation between host audio samples & watermarked audio samples

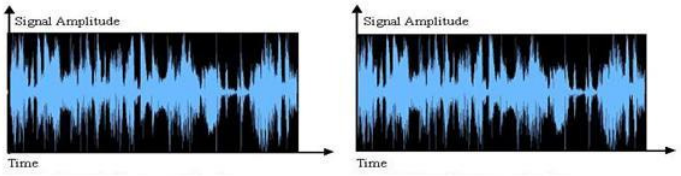


Figure 3: Negligible deviation between host audio wave & watermarked audio wave

4.1 Audio Quality Evaluation

Here 200 audio samples of both original audio and stego-audio has been considered to measure the sample level similarities between these two types of audio samples. From Figure 2, it is clear that statistical signal change (signal amplitude) due to bit embedding is very negligible compare to the original signal.

Figure 3.a shows the waveform of host audio and Figure 3.b shows the waveform of watermarked-audio. From these two Figures it is clear that after increasing the bit level of embedding, the audio signals are not differentiable by the general people.

4.2 Audio Quality Measurements

Here brief descriptions of the quality measures used have been introduced. The original signal (the cover audio) is denoted x(i), i = 1 to N while the distorted signal (the stego-audio) as y(i), i = 1 to N.

Signal-to-Noise Ratio (SNR): The SNR is very sensitive to the time alignment of the original and distorted audio signal [27]. The SNR is measured as equation no. (1), Table 4 and Table 5 showing the experimental result for 5 categories of audio file.

$$SNR = 10log_{10}\frac{\sum_{i=1}^{N} x^2(i)}{\sum_{i=1}^{N}(x(i)-y(i))^2} \quad (1)$$

Table 4: SNR values and capacities comparison with similar works (1 bit per sample)

	Embedding	1 bit per 16 bits sample			
	Music Genre	SNR (dB)		Capacity (%)	
		PM	SW	PM	SW
1	Classic	83.42	33 to 76	6.25	2 -12.5
2	Jazz	82.67	32 to 80	6.25	2 -12
3	Country	82.94	31 to 80	6.25	2 -12.5
4	Pop	83.15	38 to 82	6.25	2 -12.5
5	Rock	83.27	39 to 83	6.25	2 -12.5

Table 5: SNR values and capacities comparison with similar works (2 bits per sample)

	Embedding	2 bits per 16 bits sample			
	Music Genre	SNR (dB)		Capacity (%)	
		PM	SW	PM	SW
1	Classic	71.32	33 to 76	12.5	2 -31
2	Jazz	70.62	32 to 80	12.5	2 -32
3	Country	70.35	31 to 80	12.5	2 -33
4	Pop	71.04	38 to 82	12.5	2 -34
5	Rock	71.14	39 to 83	12.5	2 -34

PM means Proposed Method; SW means Similar Works [1, 4, 6, 7, 8, 12, 16, 21, 28, 31].

4.3 Correlation Based Measures

The similarity between two digital audio samples can also be quantified in terms of the correlation function [9, 27]. These ensure measurement of the similarity between two audios, hence in this sense they are complementary to the difference-based measures: Some correlation based measures are given in Equations (2), (3) and (4). Structural content:

$$C1 = \frac{1}{K}\sum_{k=1}^{K}\frac{\sum_{i=0}^{N-1} x(i)^2}{\sum_{i=0}^{N-1}(y(i))^2} \quad (2)$$

Normalized cross-correlation measure:

$$C1 = \frac{1}{K}\sum_{k=1}^{K}\frac{\sum_{i=0}^{N-1} x(i)*y(i)}{\sum_{i=0}^{N-1} x(i)^2} \quad (3)$$

Czenakowski distance (CZD): A metric that is useful for comparing vectors with strictly non-negative components, like in the case of audio samples, is given by the Czenakowski distance:

$$C = \frac{1}{N}\sum_{i=0}^{N-1}(1 - \frac{2*min(x(i),y(i))}{x(i)+y(i)}) \quad (4)$$

The Czenakowski coefficient (also called the percentage of similarity) measures the similarity among different samples, communities, and quadrates.

Obviously as the difference between two audio samples tends towards zero $\epsilon = x(n) - y(n)$ tends to 0, all the correlation-based measures tend towards 1, while as ϵ^2 tends to G^2 they tend towards 0.

Recall also that distance measures and correlation measure are complementary, so that under certain conditions, minimizing distance measures is tantamount to maximizing the correlation measure. Table 5 is explaining the experimental result for CZD.

Table 6: Correlation based measure of the proposed algorithm

	Music Genre	Sample Size	CZD
1	Classic	16 bits	0.00001888249326
2	Jazz	16 bits	0.00002231742249
3	Country	16 bits	0.00002079240629
4	Pop	16 bits	0.00001666038440
5	Rock	16 bits	0.00001739731132

Experimental results show that the two audio clips (original audio sequence and embedded-audio signal) cannot be discriminated by people. Results of subjective tests showed that perceptual quality of watermarked-audio, if embedding is done using the proposed algorithm, is higher in comparison to standard LSB embedding method. This confirms that described algorithm succeeds in increasing the depth of the embedding layer and also randomizing the bit layer without affecting the perceptual transparency of the watermarked-audio signal.

Therefore, significant improvement in robustness against signal processing manipulation can be obtained, as the hidden bits can be embedded higher LSB layers deeper than in the standard LSB method. The proposed algorithm flips bits in more than one bit layers of the watermarked-audio during the embedding procedure. This property may increase the resistance against Steganalysis that identifies the used LSB layer by analyzing the noise properties of each bit layer.

4.4 Capacity and Detection Probability

The capacity depends on the embedding function, and may also depend on properties of the cover. For example, least-significant-bit (LSB) replacement with one bit per sample in an eight-bit audio achieves a net capacity of 12.5%, or slightly less if one takes into account that each audio is stored with header information which is not available for embedding. If the sample size is 16-bit then

net capacity will be 6.25% or slightly less. It is intuitively clear, often demonstrated and theoretically studied that longer secret images require more embedding changes and thus are statistically better detectable than smaller ones. Hence, capacity and embedding rate are related to security.

The purpose of information hiding is to hide the existence of a secret image and also increasing robustness. Therefore, the security of a data hiding technique is judged by the impossibility of detecting the image content and extracting the hidden image after detection. However, sometimes, Cryptography also is used to increase the level of security. In this paper one image bit and two image bits have been embedded in a 16-bit sample separately and have been compared the result.

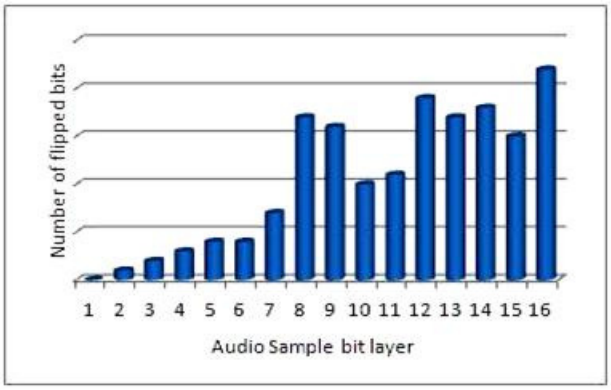


Figure 4: Number of flipped bits per bit layer for the proposed algorithm

4.4.1 Detection Probability (Embedding Location Number-wise)

Here eight (8) 16-bit samples has been used to embed 8 image-bits. The opponent has to detect 8 bits to get 1 byte of information.

Probability to detect an embedded bit position $= \frac{1}{16}$;
Probability to detect 8 embedded bit positions $= \frac{1}{16} \times \frac{1}{16}$ upto 8 terms $= \frac{1}{16^8}$;
If the length of a image is N bytes, then the probability to extract whole image $= (\frac{1}{2} \times \frac{1}{2}$ upto 8 terms)* N terms $= \frac{1}{16^{N*8}}$.

4.4.2 Decoding Probability (bit (0/1)-wise)

Probability to decode an embedded bit $= \frac{1}{2}$;
Probability to decode 8 embedded bits $= \frac{1}{2} \times \frac{1}{2}$ upto 8 terms $= \frac{1}{2^8}$.
If the length of an image is N bytes, then the probability to extract whole image $= (\frac{1}{2} \times \frac{1}{2}$ upto 8 terms) * N terms $= \frac{1}{2^{N*8}}$.

Figure 4 show histogram of the number of modified bit layers in a 10 sec audio sample (116892x16 bits in total) for the proposed LSB algorithm. It is clear that number of flipped bits per bit layers is distributed over all bit layers in the proposed algorithm. In the case of standard LSB algorithm, LSB data hiding techniques can easily detect the bit layer where the data hiding was performed. It is a much more challenging task in the case of the proposed algorithm, because there are a significant number of bits flipped in 16 bit layers and the adversary cannot identify exactly which bit layer is used for the data embedding.

4.5 Security Analysis

Detection, extraction, destruction and manipulation of the hidden data in a watermarked or stego object are the common attacks in Steganography and Watermarking techniques. While there has been quite some effort in the steganalysis of digital images, steganalysis of digital audio is relatively unexplored. Many attacks that are malicious against image Steganography algorithms cannot be implemented against audio Steganography schemes. Consequently, embedding information into audio seems more secure due to the nature of audio signals to be high-capacity data streams necessitates the scientifically challenging statistical analysis.

The attacks to a data hiding technique mainly include passive attack, active attack, and extracting attack. A passive attacker only wants to detect the existence of the embedded image, while an active attacker wants to destroy the embedded image. The purpose of an extracting attacker is to obtain the image hidden in the stego-object. So there are three kinds of security measures for different attackers respectively, i.e., detectability, robustness and difficulty of extraction. Usually the problem of steganography only concerns the detectability so in many literatures delectability is referred to the security of a stegosystem [10]. The problem of Watermarking concerns the detectability and robustness both. In this section the security of our data hiding process is discussed.

Westfeld [35] addressed the steganalysis of the MP3Stego algorithm. Ozer et al. [24] proposed a universal audio steganalysis technique that is effective on both watermarking and steganographic data-embedding methods. The basic idea in [24] rests on the statistical evidence that the distortion measures computed between signals and their de-noised versions have statistically distinguishable distributions for cover-signals and stego-signals. These statistically distinguishable features are used in steganalyzer design to classify cover-signals from stego-signals.

The audio steganalysis algorithm proposed by Liu et. al. [20] uses the Hausdorff distance measure to measure the distortion between a cover audio signal and a stego au-

dio signal. I.Avcibas [13] proposed the use of stream data mining for steganalysis of audio signals of high complexity. Their approach extracts the second order derivative based Markov transition probabilities and high frequency spectrum statistics as the features of the audio streams. The variations in the second order derivative based features are explored to distinguish between the cover and stego audio signals. This approach also uses the Mel-frequency cepstral coefficients [19], widely used in speech recognition, for audio steganalysis.

The above mentioned steganalysis schemes are designed mainly based on the Analysis of Variance (ANOVA), Sequential Floating Search Method (SFS), Regression Analysis Classifier, Support Vector Machine Classifier etc.

By randomizing the embedding approach and choosing the higher LSB layer, the algorithm to estimate the cover statistics can be effectively disabled. The steganalyst cannot make any consistent assumptions about the hiding process even if the embedding algorithm is known to everyone as per the Kerckhoffs principle. Hiding in a randomized manner is quite attractive, and we explore its simplest realization in this paper.

So, most of the technique will not work in our proposed hiding scheme.

According to the experimental result of Signal-to-noise ratio (SNR) and Czenakowski distance (CZD), it is clear that human auditory system will not able to distinguish between original audio and stego-audio.

Here statistical analysis has been performed using [23] on original audio samples and stego audio samples and data have been introduced below and in Tables 7 and 8.

Table 7: Test for equal means (ANOVA)

	Sum of sqrs	df	Mean square
Within groups	1.86199E08	398	467836
Total	1.86199E08	399	
$omega^2$:	-0.002506		
HOV(Levene):	0.9937		
Medians p:	0.9939		

Between groups:

$$\begin{aligned} Sum\_of\_sqrs &= 58.5225; \\ df &= 1; \\ Meansquare &= 58.5225; \\ F &= 0.0001251; \\ p(same) &= 0.9911. \end{aligned}$$

Welch F test in the case of unequal variances: $F = 0.0001251$, $df = 398$, $p = 0.9911$.

Intra-class Correlation statistics: ANOVA

Between raters: Sum of sqrs = 58.5225; $df = 1$; Mean square=58.5225; F=23.96; p(same)=0.9911.

Between cases: Sum of sqrs = 1.86198E08; $df = 199$; Mean square=935670; F=3.831E05.

Within cases: Sum of sqrs = 544.5; $df = 200$; Mean square=2.7225;

Residual: Sum of sqrs = 485.977199; $df = 2.4421$;

Total: Sum of sqrs = 1.86199E08; $df = 399$; 95% confidence has been explain in Table 8.

Table 8: Intra-class correlation statistics(95% confidence)

Model 1	Individual	ICC(1,1)1	[1, 1]
	Mean	ICC(1,k)1	[1, 1]
Model 2	Individual	ICC(2,1)1	[1, 1]
	Mean	ICC(2,k)1	[1, 1]
Model 3	Individual	ICC(3,1)1	[1, 1]
	Mean	ICC(3,k)1	[1, 1]

From the above statistical analysis it is very much clear that statistical attack most of the time will fail to detect the hidden image from the stego-audio.

In our scheme, it is very difficult to detect the embedding information from stego audio. Again, if opposition add any noise with the stego audio randomly, there is a possibility of destroying or modifying information embedded into the audio file. To avoid this type of situation, we may use parity bit error checking like familiar technique or we may use hamming code for error detection and correction in our future work.

5 Advantages of Our Approach

- Embedding position numbers of image bits into audio file are sent to the receiver by converting them to Boolean functions which is more secured.
- Boolean functions are transmitted to receiver using digital signature concept which is very secure and reliable.
- Described algorithm succeeds in not only increasing the depth of the embedding layer but also layers are chosen randomly without affecting the perceptual transparency of the audio signal.
- Two-way robustness (to know the actual position of the image bit) are there, First, insertion positions are randomly chosen, Second, LSB layers are most of the time are high LSB layers.
- Embedding image into audio file causes minimal embedding distortion to the host audio, since optimization is done using GA operators.

- The hidden information detection of the proposed algorithm is more challenging as well, because there is a significant number of bits flipped in random higher LSB bit layers.
- In addition, listening tests showed that perceptual quality of stego-audio is higher in the case of the proposed method than in the standard LSB method.

6 Conclusions

This paper presents a novel bit-modification algorithm for modified LSB data hiding technique where image bit positions are transmitted to the receiver using digital signature concept which is very secure and reliable. The key idea of the algorithm is to embed the image bit which will cause negligible embedding distortion of the host audio. Listening test shows that described algorithm succeeds in increasing the depth of the embedding layer from lower to higher random LSB layers without affecting the perceptual transparency of the audio signal. The detection and extraction of hidden information of the proposed algorithm is more challenging as well, because there is a significant number of bits flipped in random higher LSB bit layers. On the other hand, position numbers are converted to Boolean functions and functions are transmitted using AES and RSA algorithms to the receiver end to make it more secure.

References

[1] M. A. Ahmed, L. M. Kiah, B. B. Zaidan, and A. A. Zaidan, "A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm," *Journal of Applied Sciences*, vol. 10, no. 4, pp. 59–64, 2010.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 45, no. 3, pp. 313–336, 1996.

[3] H. Berghel and L. B. Gorman, "Protecting ownership rights through digital watermarking," *IEEE Computers*, vol. 29, no. 7, p. 101–103, 1996.

[4] K. Bhowal, D. Bhattacharyya, A. J. Pal, and T. H. Kim, "A GA-based audio steganography with enhanced security," *Telecommunication Systems Journal, Springer*, vol. 52, no. 4, pp. 2197–2204, 2013.

[5] L. Boney, A. Tewfik, and K. Hamdy, "Digital watermarks for audio signals," in *Proceedings of the Third IEEE International Conference on Multimedia Computing and Systems*, pp. 473–480, 1996.

[6] N. Cvejic and T. Seppnen, "Reduced distortion bit-modification for LSB audio steganography," *Journal of Universal Computer Science*, vol. 11, no. 1, pp. 56–65, 2005.

[7] D. Ahmad and P. Mohammad, "Adaptive and efficient audio data hiding method in temporal domain," in *7th International Conference on Information, Communications and Signal Processing (ICICS'09)*, pp. 1–4, 2009.

[8] A. Delforouzi and M. Pooyan, "Adaptive digital audio steganography based on integer wavelet transform," *Circuits Systems Signal Processing*, vol. 27, no. 2, pp. 247–259, 2008.

[9] A. M. Eskicioglu and P. S. Fisher, "Image quality measures and their performance," *IEEE Transactions on Communications*, vol. 43, no. 12, pp. 2959–2965, 1995.

[10] J. Fridrich, M. Long, "Steganalysis of LSB encoding in color images," in *Proceedings of IEEE International Conference on Multimedia and Expo (ICME'00)*, pp. 1279–1282, 2000.

[11] K. Gopalan, "Audio steganography using bit modification," in *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 421–424, 2003.

[12] H. B. Kekre, A. Archana, R. Swarnalata, and A. Uttara, "Information hiding in audio signals," *International Journal of Computer Applications*, vol. 7, no. 9, pp. 14–19, 2010.

[13] I. Avcibas, "Audio steganalysis with content-independent distortion measures," *IEEE Signal Processing Letters*, vol. 13, no. 2, p. 92–95, 2006.

[14] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *IEEE Computers*, vol. 31, no. 2, pp. 26–34, 1998.

[15] H. Jouhari and E. M. Souidi, "A novel embedding scheme based on walsh hadamard transform," *Journal of Theoretical and Applied Information Technology*, vol. 32, no. 1, pp. 55–60, 2011.

[16] K. B. Samir, U. P. Tuhin, and Ra. Avishek, "A robust audio steganographic technique based on phase shifting and psycho-acoustic persistence of human hearing ability," *International Journal of Computing and Corporate Research*, vol. 1, no. 1, 2011.

[17] Md. S. Khan, V. V. Bhasker, and V. S. Nagaraju, "An optimized method for concealing data using audio steganography," *International Journal of Computer Applications*, vol. 33, no. 4, pp. 25–30, 2011.

[18] E. Koch and J. Zhao, "Toward robust and hidden image copyright labeling," in *IEEE Workshop Nonlinear Signal and Image Processing*, pp. 452–455, 1995.

[19] Q. Liu, A. H. Sung, and M. Qiao, "Novel stream mining for audio steganalysis," in *Proceedings of the 17th ACM International Conference on Multimedia*, pp. 95–104, 2009.

[20] Y. Liu, K. Chiang, C. Corbett, R. Archibald, B. Mukherjee, and D. Ghosal, "A novel audio steganalysis based on higher-order statistics of a distortion measure with hausdorff distance," *11th International Conference on ISC*, LNCS 5222, pp. 487–501, 2008.

[21] Z. Mazdak, A. M. Azizah, B. A. Rabiah, M. Z. Akram, and A. Shahidan, "A genetic-algorithm-based approach for audio steganography," *World*

Academy of Science, Engineering and Technology, vol. 54, pp. 360–363, 2009.

[22] N. Cvejic and T. Seppanen, "Increasing the capacity of LSB based audio steganography," in *Proceedings of 5th IEEE International Workshop on Multimedia Signal Processing*, pp. 336–338, 2002.

[23] O. Hammer, *Past 3.x - the Past of the Future*, 2013. (`http://folk.uio.no/ohammer/past/`)

[24] H. Ozer, I. Avcibas, B. Sankur, and N. Memon, "Steganalysis of audio based on audio quality metrics," in *Proceedings of SPIE Security Watermarking Multimedia Contents V*, vol. 5020, p. 55–66, 2003.

[25] I. Pitas and T. H. Kaskalis, "Applying signatures on digital images," in *IEEE Workshop Nonlinear Signal and Image Processing*, pp. 460–463, 1995.

[26] J. J. Quisquater, O. Bruyndonckx, and B. Macq, "Spatial method for copyright labeling of digital images," in *IEEE Workshop Nonlinear Signal and Image Processing*, pp. 456–459, 1995.

[27] S. R. Quackenbush, T. P. Barnwell, and M. A. Clements, *Objective Measures of Speech Quality*, Prentice Hall, 1988.

[28] S. Gurvinder, S. K. Dey, S. Dubey, and S. Katiyal, "Increasing the efficiency of echo hiding digital audio steganography," in *4th National Conference on Computing for National Development (INDIACom'10)*, 2010.

[29] S. K. Pal, P. K. Saxena, and S. K. Mutto, "The future of audio steganography," in *Pacific Rim Workshop on Digital Steganography*, 2002.

[30] Van R. G. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proceedings of IEEE International Conference on Image Processing (ICIP'94)*, vol. 2, pp. 86–90, 1994.

[31] R. Sridevi, A. Damodaram, and S. V. L. Narasimham, "Efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security," *Journal of Theoretical and Applied Information Technology*, vol. 5, no. 6, pp. 768–771, 2009.

[32] M. Swanson, B. Zhu, A. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," *Signal Processing. Special Issue on Watermarking*, vol. 66, no. 3, pp. 337–355, 1997.

[33] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," in *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, 1998.

[34] Y. C. Tseng, Y. Y. Chen, and H. K. Pan, "A secure data hiding scheme for binary images," *IEEE Transactions on Communications*, vol. 50, no. 8, pp. 1227–1231, 2002.

[35] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Information Hiding*, LNCS 1768, pp. 61–66, Springer-Verlag, 1999.

Krishna Bhowal obtained his M. Tech from West Bengal University of Technology in 2010. He is a research scholar at the Dept. of Engineering and Technological Studies, University of Kalyani, Kolkata. Currently Mr. Bhowal is working as a Assistant Professor at Academy of Technology, a Degree Engineering College, Kolkata, India. He has about 7 years of experience in teaching. His area of interest includes Audio Steganography, Watermarking, Cryptography; He has published 3 International Journal papers and 2 research papers in International IEEE Conference. He is a member of IEEE.

Debasree (Chanda) Sarkar obtained her Ph.D in Engineering from Jadavpur University in the year 2005. She has obtained her M.E. from Bengal Engineering College (Presently known as Bengal Engineering and Science University, Shibpur) in the year 1994. She earned her B.E. degree in Electronics and Telecommunication Engineering from Bengal Engineering College (Presently known as Bengal Engineering and Science University, Shibpur) in the year 1991. She is presently working as Scientific Officer at the Dept. of Engineering and Technological Studies, University of Kalyani. Her area of research includes Microstrip Antenna, microstrip Filter, Frequency Selective Surfaces. She has contributed to numerous research articles in various journals and conferences of repute.

S. Biswas obtained his Ph.D in engineering from Jadavpur University in the year 2004. He obtained his M.E from Jadavpur University and B.E from Bengal Engineering College (Presently known as Bengal Engineering and Science University, Shibpur) in the year 1994 and 1990 respectively. He is presently working as Scientific Officer at the Dept. of Engineering & Technological Studies, University of Kalyani. He has more than 14 years of teaching experience. His area of interest includes, Artificial Neural Network, Image Processing, Frequency Selective Surfaces, Microstrip Antennas.

Partha Pratim Sarkar obtained his Ph.D in Engineering from Jadavpur University in the year 2002. He has obtained his M.E. from Jadavpur University in the year 1994. He earned his B.E. degree in Electronics and Telecommunication Engineering from Bengal Engineering College (Presently known as Bengal Engineering and Science University, Shibpur) in the year 1991. He is presently working as Senior Scientific Officer at the Dept. of Engineering and Technological Studies, University of Kalyani. His area of research includes Microstrip Antenna, microstrip Filter, Frequency Selective Surfaces and Artificial Neural Network. He has contributed to numerous (more than 110 publications) research articles in various journals and conferences of repute. He is a life fellow of IETE, and fellow of IE (India).

User-to-User Mutual Authentication and Key Agreement Scheme for LTE Cellular System

Mohammed Ramadan[1], Fagen Li[1], ChunXiang Xu[1], Abdeldime Mohamed[2], Hisham Abdalla[1], Ahmed Abdalla[1]

(Corresponding author: Mohammed Ramadan)

School of Computer Science and Engineering, University of Electronic Science and Technology of China[1]
2006 Xiyuan Avenue, Gaoxin West Zone, Chengdu 611731, P.R. China
School of Information Science and Engineering, Southeast University, Nanjing 210096, P.R. China[2]
(Email: nopatia@gmail.com)

(Received July 6, 2015; revised and accepted Aug. 12 & Sept. 29, 2015)

Abstract

Long Term Evolution LTE is the first technology that provides exclusively packet-switched data and modifies the security architecture of the 2G and 3G systems. The LTE security architecture offers confidentiality, access control, a kind of obscurity and mutual authentication. However, numerous types of attacks can be encountered during the mutual authentication process which is a challenge-response based technique. Therefore, a high secure public key algorithm can be implemented to improve the network security services. As the network operator is often considered as not being a highly trusted party and can thus face threats, the communications ends are the only secure parties to provide such security features. This paper proposes a secure mutual authentication and key agreement scheme for LTE cellular system with user-to-user security. The network side in this scheme operates as a proxy and non-trusted party to provide the security architecture with more flexibility and reliability. This is achieved by using designated verifier proxy signature and key agreement protocol based bilinear pairing with some changes in both security algorithms and LTE security architecture within the LTE standardization. Our security and performance analysis demonstrated that the proposed scheme is more secure compared to the basic authentication and key agreements schemes.

Keywords: 4G security, LTE-AKA, LTE proxy signature, mobile communication security

1 Introduction

LTE also referred to as 4G communication system is the next generation of mobile communication system that is being developed by 3GPP for secure and fast communication for 4G mobile communication standards. LTE has high efficiency, and good communication specifications [26]. It provides high communications features, such as bandwidth, data rate and switching techniques. The LTE architecture provides more secure communication than 2G and 3G mobile communication systems by providing mutual authentication between the User Equipment (UE) and Mobility Management Entity (MME). Authentication and Key Agreement protocol for Evolved Packet System EPS-AKA is a technique which executes authentication and session key distribution in LTE security architecture and it is a challenge-response based mechanism that employs symmetric cryptography. The fundamental EPS/LTE architecture is founded on UMTS-AKA and it provides secure network access. When a subscriber attempts to access WLAN, the International Mobile Subscriber Identity (IMSI) is sent through a Network Access Identifier (NAI) to the Access Point (AP). Although the basic EPS-AKA has some advantages, such as larger authentication keys, stronger hash function (SHA-1), support for mutual authentication, support for signaling message data integrity, support for signaling information encryption, support for user data encryption and protection, it has many vulnerabilities as elaborated in [31].

1.1 Motivation

The basic AKA protocol is a challenge-response protocol which it has many vulnerabilities. The primary objectives of this paper is to find a solution to the basic EPS-AKA problems such as false base station attack, IMSI catcher, and to achieve a strong security scheme which can provide user-to-user mutual authentication and key agreement security. By solving these problems, the users gain more trust in their network due to the network operator working only as a proxy. Moreover, the network operator can help the users to implement their security features, and it is considered to be a protected party.

The proposed scheme is based on designated verifier

proxy signature (DVPS) which is a special type of proxy signature in which the designated verifier (UE) alone can check the validity of the proxy (MME) signatures. Our proposed scheme consists of five main algorithms, setup and key generation, signature generation by the users UE's, signature verification and proxy signature generation by the network MME, proxy signature verification by the designated verifiers (users UE's), and session key generation by the users UE's. The original signer (User A) delegates its signing power to the proxy signer (Network operator) to generate proxy signatures for the designated verifier (User B) whereas in the last algorithm, User B checks the validity of the proxy signatures by using its own secret key. Furthermore, in our proposed scheme we made some changes to make DVPS more compatible with the LTE security architecture and to provide user-to-user mutual authentication and key agreement protocol. Designated verifier signature and proxy signature offers many kinds of security levels as proposed in the literature in the field of DVS [15, 17, 24, 30, 33, 36].

The rest of the paper is organized as follows: Section 2 introduces the basic EPS-AKA protocol; Section 3 presents briefly the basic EPS-AKA Vulnerabilities and some threats which are the motivations for this paper; Section 4 discusses the preliminaries of our proposed scheme and we introduce the basic principles of bilinear pairing and designated verifier signature; Section 5 presents our proposed system model and we firstly introduce some assumptions and definitions then present the phases of our proposed scheme; in Sections 6 and 7 we evaluate our proposed scheme by analyzing the security and the performance efficiency respectively; Finally Section 8 concludes this work.

2 The Basic EPS-AKA Protocol

The basic EPS-AKA scheme is a challenge-response based protocol and is quite similar to the UMTS-AKA version [6], except for the key set identifier (eKSI) in the challenge, and for separation indicator process when the user equipment (UE) verifies that the separation bit is set for E-UTRAN access. However, the main purpose of EPS-AKA protocol is the authentication of the user and the establishment of a new local master key KASME between the MME and the UE. EPS-AKA is also used for verification of the freshness of the authentication vector and authentication of its origin (the users home network) by the USIM. KASME is used in subsequent procedures for deriving further keys for the protection of the user plane, Radio Resource Control signalling, and Non-Access Stratum signaling [29].

The EPS-AKA procedure is as follows:

1) Generate EPS authentication vectors (AVs) in the HSS upon request from the MME, and distribute them to the MME. Hence, the MME needs to identify the UE before requesting authentication vectors from the HSS.
2) Mutual authentication and establishing a new shared key between the serving network and the UE.
3) Authentication data distribution between serving networks.

The MME invokes the procedure by requesting EPS authentication vectors from the HSS. The authentication information request shall include the IMSI, the serving network identity 'SN id' of the requesting MME, and an indication that the authentication information is requested for EPS. The SN id is required for the computation of KASME in the HSS. Then the MME invokes the authentication request procedure by selecting the next unused EPS authentication vector from the ordered array of EPS authentication vectors in the MME database (if there is more than one). If the MME has no EPS AV it requests one from the HSS. The MME then sends the random challenge RAND and the authentication token for network authentication AUTN from the selected EPS authentication vector to the mobile equipment, which forwards it to the USIM. The MME also generates a key set identifier eKSI and includes it in the Authentication Request. For the verification process and when the USIM receive RAND and AUTN, then the USIM first computes the anonymity key $AK = f5_K(RAND)$ and retrieves the sequence number $SQN = (SQN \bigoplus AK) \bigoplus AK$, where K is the permanent pre-shared secret key between USIM and AuC, and then the USIM computes $XMAC = f1K(SQN \parallel RAND \parallel AMF)$ and verifies that it equals the MAC included in AUTN. For the authentication response process and upon receipt of the Authentication Response message the MME checks whether the received RES matches the expected response XRES from the selected authentication vector. If it does then the authentication of the user has been successful [10]. Figure 1 illustrates the handshaking procedures of the basic EPS-AKA protocol.

3 Vulnerabilities of the Basic EPS-AKA

For network access security, 2G mobile systems such as GSM and CDMA were designed to be protected against external attacks. However, these designs have led to numerous interception attacks [27, 35]. In 3G network, a mobile station is connected to a visited network by means of a radio link to a particular base station (Node B). Multiple base stations of the network are connected to a Radio Network Controller (RNC) and multiple RNCs are controlled by a GPRS2 Support Node (GSN) in the packet-switched case or a Mobile Switching Center (MSC) in the circuit-switched case. The Visitor Location Register (VLR) and the serving GSN keep track of all mobile stations that are currently connected to the network. Every subscriber can be identified by its International Mobile Subscriber Identity (IMSI). In order to protect against profiling attacks, this permanent identifier is sent over the air interface as infrequently as possible. Instead, locally valid

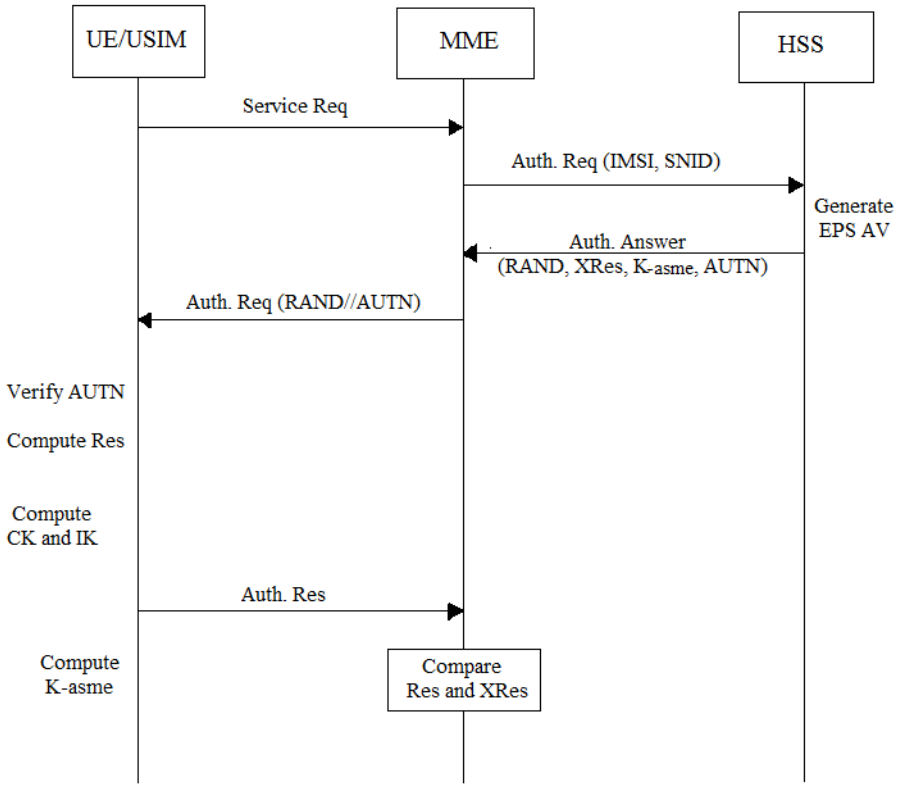


Figure 1: The basic EPS-AKA scheme

Temporary Mobile Subscriber Identity (TMSI) is used to identify a subscriber whenever possible. Every UMTS subscriber has a dedicated home network with which he shares a long term secret key Ki. The Home Location Register (HLR) keeps track of the current location of all subscribers of the home network. Mutual authentication between a mobile station and a visited network is carried out with the support of the current Serving GSN (SGSN) or the MSC/VLR respectively. UMTS supports encryption of the radio interface as well as integrity protection of the signaling messages. For a detailed description we refer to [1, 2].

Wireless cellular networks were originally designed to provide ubiquitous access for communication. Although the 2G network was designed with some security aspects in mind, GSM just featured cryptographic algorithms to guarantee privacy and authentication. The GSM security architecture, proposed two decades ago, is nowadays known to be insufficient given current computational power. UMTS-based 3G networks enhanced the system by implementing stronger encryption and a two-way authentication scheme. Both encryption and authentication are further enhanced in LTE. However, with the current threat landscape and the increasing sophistication of attacks, such security architecture is not enough to guarantee the availability of mobility networks.

The Authentication and Key Agreement protocol in EPS has a known vulnerability that can be exploited to breach the privacy of the user's identity and even his location [3, 4, 5]. However, many works tried to solve this problem by proposing alternative protocols [25]. The vulnerability, (i.e. sending the International Mobile Subscriber Identity in plaintext when no temporary identifier is valid) which was inherited from UMTS, can be used for tracking the user and/or detecting the user's presence. One of the latest proposed alternative protocols noted as Security Enhanced Authentication and Key Agreement (SE-AKA) was Cryptanalyzed in [1] and it was found vulnerable to brute force and intelligent brute force attacks when no padding is used.

There are several other types of attacks that could be threats to the LTE mobile network such as malware spreading, phishing, and DoS/DDoS attacks. DoS/DDoS is classified, based on the traffic load maliciously generated, into low and high traffics for DoS and DDoS respectively. We note that a special class of attack is defined for the case of the attacker being already within the network perimeter and not requiring a charge of malicious traffic. This is the case of an insider attack. Furthermore, some attacks have a local scope, disrupting service at the RAN level and blocking service for a single cell or sector. And other types of attacks can have a much wider scope, and are capable of disrupting a large portion of the mobility network. Local attack is a radio jamming and saturation of the wireless interface and such attacks can be launched from a single device or radio transmitter [20]. However,

the proposed scheme is secure against such attacks and particularly against the common attack, false base station and IMSI catcher attack.

4 Preliminaries

Our scheme relies on designated verifier proxy signature DVPS and key agreement protocol based bilinear pairing. We will briefly introduce the basic principles and some properties related to these techniques.

4.1 Bilinear Pairing

Let G_1 be a group of the order of a large prime number q and G_2 be a multiplicative subgroup of a finite field $\mathbb{F}$ of the same order and P be a generator of G_1. A map $e : G_1 \times G_1 \longrightarrow G_2$ is called a bilinear map if it has the following properties [21]:

Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ where $P, Q \in G_1$ and $a, b \in Z_q^*$;

Non-degeneracy: $P, Q \in G_1$, such that $e(P, Q) \neq 1$;

Computability: $P, Q \in G_1$ there is an efficient algorithm to compute $e(P, Q)$.

4.2 DVS

There exist three participants in the system, namely Alice, Bob and Cindy, who act as the original signer, the proxy signer and the receiver (or the designated verifier), respectively. We denote (xi, P_i) as a pair of private key and public key for user i, where $i \in \{A, B, C\}$ indicating Alice, Bob, and Cindy, respectively. A designated verifier proxy signature scheme (DVPS) consists of following algorithms [13]:

Parameters Generation: It takes as input the system security parameter l and outputs the system parameters.

Key Generation: It takes as input the security parameter l and outputs the key set: (xi, P_i) for $i = A, B, C$.

Proxy Key Generation: A deterministic algorithm that takes as input the original signer's secret key, the proxy signer's secret key, the identity of the proxy signer and the warrant m_w to generate the proxy key. That is Proxy Key Gen (x_A, x_B, ID_B, m_w), where X_A and X_B are the secret keys of the original signer and the proxy signer respectively and ID_B is the identity of the proxy signer.

Sign: A deterministic algorithm that takes as input the proxy key, the designated verifier's public key and a message m to generate a signature (σ), where proxy key is generated by the above Proxy Key Generation algorithm.

Verify: A deterministic algorithm that accepts a message m, a signature (σ), the original signer's public key, the proxy signer's public key, the proxy signer's identity and the receiver's secret key and then returns Valid if the signature is correct, and otherwise outputs invalid.

5 Proposed System Model

The proposed design provides user-to-user mutual authentication and key agreement technique for LTE cellular system which we termed as LTE-AKA. The basic LTE-AKA scheme does not provide end-to-end security and it has many vulnerabilities as shown in Section 3. We seek to address these vulnerabilities in our proposed scheme with more flexibility and security than the basic EPS-AKA scheme. We achieve this by using the system parameters in our model and distribute them between the entities during the communication modes. For example the system parameters will be distributed in advance and stored in both USIM card and HSS/AuC and for the security parameters and public keys will be distributed in the synchronization mode.

5.1 System Model Assumptions

The following assumptions are made with regard to our proposed scheme:

1) Assume user A and user B belongs to the same serving network and here we used the serving network identity SNID.

2) Using the home network identity HNID in case user A and B are not using the same serving network.

3) The identifier IMEI is assumed to be the message to be signed.

4) The identifiers IMSI, GUTI, SNID are assumed to be the identities to be hashed.

5) The pre-shared key (K) is used as a secret value during the session key phase.

5.2 Definitions of System Model Key Terms

5.2.1 Definitions

The major parties are the Home Network which is signified by (HSS), and the Visited/Serving Network which is signified by (MME). However, the subsequent definitions and terms are vital for our proposed scheme [23].

Home Service Server (HSS): The fundamental subscriber database at the home network (HPLMN). It is the definitive database of mobile subscriber information for a wireless carrier's network. It is also the real-time list that links phones, phone numbers, user accounts and service plan information.

Mobility Management Entity (MME): The MME is situated in the visited network (VPLMN). It is the network termination for the challenge-response part of the EPS-AKA protocol. It is also the host for the Access Security Management Entity (ASME), which is responsible of access security.

User Equipment (UE): The user/subscriber equipment is made up of the mobile equipment (ME) and the subscriber module (UICC/USIM).

Base station or eNodeB (eNB): The radio access point in LTE. It belongs to the visited network (VPLMN).

Serving Network Identity (SNID): SNID refers to the network accessed by the user and it is made up of PLMN ID (MCC+MNC). However, it classifies the specific serving network to UE's while in their roaming mode.

Authentication Center (AuC): It is a security database and it recommends any security information management; which (SIM) card is trying a network connection when a phone has a live network signal, and it provides security to ensure that third parties are incapable of exploiting network subscriber services.

International Mobile Station Equipment Identity (IMEI): It is a type of serial number that solely recognizes the mobile equipment internationally. The IMEI is allocated by the equipment manufacturer and registered by the network operator.

International Mobile Subscriber Identity (IMSI): IMSI is a permanent identity. Each registered user is solely recognized by its (IMSI) which is saved in the subscriber identity module (USIM).

Globally Unique Temporary UE Identity (GUTI): GUTI is a temporary identity that is transferred between UE and the network. It is arbitrarily allotted by the MME to every mobile in the region, when it is switched on. It consists of two major components:

1) GUMMEI which identifies the MME that assigned the GUTI.
2) M-TMSI which identifies the UE within the MME that assigned the GUTI.

5.2.2 Notations and Terms

Table 1 illustrates the notations used in the proposed LTE-AKA scheme.

Table 1: The notations and terms of the proposed scheme

Notations	Description
Subscript A	User A
Subscript B	User B
Subscript A/B	User A and user B
UE	User equipment
K	Pre-shared key
X	User's secret key
A	Public key for UE_A
B	Public key for UE_B
H/SNID	Home/Serving network identity
SK	Session key
Req	Authentication request
Res	Authentication response
XRes	Expected authentication response

5.3 The Proposed LTE-AKA Scheme

The proposed scheme is based on designated verifier signature and pairing based key agreement protocol to provide AKA scheme for the LTE cellular communication system [13, 21]. As we presented in Section 3, the basic EPS-AKA scheme is challenge-response algorithm which has many security weaknesses such as false base station attack and IMSI catcher attack (See Section 6). However, our proposed scheme solves such weaknesses with the same bandwidth consumption and handshaking process. And it only needs two handshaking processes for both authentication and key agreement processes. However, the network operator entities MME and HSS/AuC in our proposed scheme are only as a proxy signer and it is responsible for the system parameters and then assigns the GUTI for the visited network and for the users who belong to this location area. Hence, the session key will be changeable according to the current location. It will be computable only for the communication ends of the UE. Therefore, we assume two cases for our proposed scheme according to the security based mobility mode. Figure 2 illustrates the handshaking process for both cases.

Case 1: The two subscribers belong to the same visiting network, i.e. same MME and in this case the MME request the system parameters from the home network (HSS) which are computed by the AuC in advance. However, the same SNID will be used for the AKA protocol.

Case 2: Here we assume the two subscribers wishing to connect each other are on different visited networks i.e. different MME's (roaming mode) and the LTE-AKA will be achieved separately and some parameters exchange via home network HSS and some system parameters will be exchanged via the secured link between MME's. In this case the home network identity PLMN ID will be used for the AKA protocol.

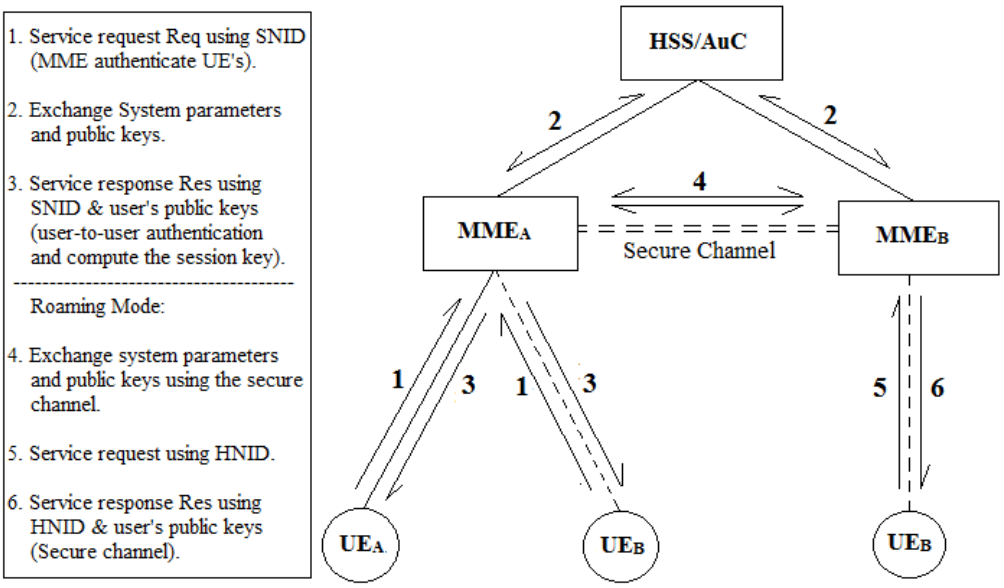


Figure 2: The proposed LTE-AKA handshaking process

The main objective of our scheme is to provide user-to-user AKA security scheme by let the MME's works as a proxy and use the user's identifier IMEI's as a message and the subscriber's GUTI or use the specific IMSI as identifiers with the network identifier SNID, and later for the session key. The AuC uses the same parameters to verify the UE, and then sends another signature which we called RES to the UE, then when the UE received the RES's it will compute the changeable session key depending on the current GUTI identifiers which is allocated in advance by MME. The UE's is continuously listening to the broadcast messages from MME through the base station (eNB) to determine the tracking area by using the parameter Tracking Area Identity (TAI). The ME is comparing the TAI which is received with that stored in the USIM and if not equal, UE requests a new TAI. This case occurs when the mobile is switched on or when the specific UE moved from one location area to another. Hence, the system parameters and keys will be distributed in the paging/synchronization processes before the call setup process. The proposed LTE-AKA scheme consists of the following four phases.

Phase 1: Setup and Key Generation.

Setup: This phase calculates the system parameters in the synchronization mode, when the UE connecting to the base station (eNB) which is in the idle, i.e. NAS security context. This phase works as follows:

1) UEA want to get access to the network services and connect to UEB, so we have four entities such as: UEA, UEB, visited network MME, and the home network HSS.
2) The setup algorithm will be done by the HSS/AuC, and it takes as input the system security parameter, and outputs the system parameters $\{G_1, G_2, P, q, e, H_1, H_2\}$, where

G_1**:** Cyclic additive group of order q;

G_2**:** Multiplicative group of order q;

P**:** Generator of G_1;

e**:** Bilinear map $e : G_1 \times G_1 \longrightarrow G_2$;

H_1**:** One way hash function: $\{0,1\}^* \longrightarrow G_1$;

H_2**:** One way hash function: $\{0,1\}^* \longrightarrow Z_q^*$.

Key Generation: This algorithm will be achieved by the users, and it computes the public/private keys, and we assume there are two users A and B which are willing to contact each other, this algorithm works as follows:

For UE_A**:**
Pick a secret key $xA \in Z_q^*$ and calculate the corresponding public key

$$A = x_A P.$$

Then using its own public key and identifications $(IMSI_A/GUTI_A)$ calculates:

$$\begin{aligned} Q_A &= H_1(IMSI_A \parallel GUTI_A, A) \\ D_A &= x_A Q_A, A. \end{aligned}$$

For UE_B**:**
Pick a secret key $xB \in Z_q^*$ and calculate the corresponding public key

$$B = x_B P.$$

Then using its own public key and identifications ($IMSI_B/GUTI_B$) calculates:

$$\begin{aligned} Q_B &= H_1(IMSI_B \parallel GUTI_B, B) \\ D_B &= x_B Q_B, B. \end{aligned}$$

For MME:

Pick a secret key $x_N \in Z_P^*$ and calculate the corresponding public key

$$N = x_N P.$$

Then using the public key and home / serving network identification (H / SNID) calculates:

$$Q_N = H_1(H/SNID, N).$$

These keys $\{D_A, D_B, N, Q_N\}$ will be distributed between entities in the synchronization mode and it will be used in the further phases. However, when the mobile user ME enter the specific serving network, and start to send location update messages including its own public key, and it can get the parameters for the specific serving network.

Phase 2: MME authenticate the users UE_A and UE_B

When the user A wants to get access to user B, Then it will start to compute the following parameters and send them to MME:

For UE_A:

Using MME's parameters N and Q_N, and its own secret key compute the corresponding request Req_A and send it to MME as follows:

$$Req_A = x_A Q_N.$$

For UE_B:

User B uses its own secret key and the network parameters as follows to compute Req_B and send it to MME as follows:

$$Req_B = x_B Q_N.$$

For MME:

When MME receives the service requests Req_A, Req_B it will start to authenticate UE_A and UE_B using the system parameters and the user's public keys as follows.

MME check $e(Req_A, P) = e(Q_N, A)$ for UE_A, if not equal abort the request. If equal, then using Req_A and B compute Res_B response and send it to UE_B:

$$Res_B = H_2(IMEI_B, e(Req_A, x_N Q_N, B)).$$

Then For UE_B MME check $e(Req_B, P) = e(Q_N, B)$, if not equal abort the request. If equal, then by the same way compute Res_A and send it to UE_A:

$$Res_A = H_2(IMEI_A, e(Req_B, x_N Q_N, A)).$$

Phase 3: User-to-User authentication.

As the subscriber authentication and network operator processes are bedeviled with security problems as outlined in Section 6, we proposed scheme that can achieve user-to-user authentication and the MME act as a proxy, and $UE_{A/B}$ as a designated verifiers. The algorithm for achieving this purpose as follows:

For UE_A:

When receive Res_A from MME then compute $XRes_A$:

$$XRes_A = H_2(IMEI_A, e(Req_A, B + N)).$$

And check and validate the equality $Res_A = XRes_A$ holds, if not outputs invalid and abort access.

For UE_B:

When receive Res_B from MME then compute $XRes_B$:

$$XRes_B = H_2(IMEI_B, e(Req_B, A + N)).$$

And check the equality $Res_B = XRes_B$ holds, if not outputs invalid and abort access. Figure 3 illustrates this phase at the UE/USIM side when the users authenticate each other.

Correctness:

This correctness for UE_A and it is the same process for UE_B: When the UE_A receives the

$$Res_A = H_2(IMEI_A, e(Req_B, x_N Q_N, A)).$$

It starts to compute:

$$XRes_A = H_2(IMEI_A, e(Req_A, B + N)).$$

Where,

$$\begin{aligned} A &= x_A P \\ Req_B &= x_B Q_N. \end{aligned}$$

Then,

$$Res_A = H_2(IMEI_A, e(x_B Q_N, x_N Q_N, x_A P)).$$

From the bilinear properties we get:

$$\begin{aligned} Res_A &= H_2(IMEI_A, e(x_A P, x_B Q_N) \\ &\quad \cdot e(x_A P, x_N Q_N)) \\ &= H_2(IMEI_A, e(x_A Q_N, x_B P) \\ &\quad \cdot e(x_A Q_N, x_N P)) \\ &= H_2(IMEI_A, e(Req_A, B) \\ &\quad \cdot e(Req_A, N)) \end{aligned}$$

Then,

$$\begin{aligned} Res_A &= H_2(IMEI_A, e(Req_A, B + N)) \\ &= XRes_A. \end{aligned}$$

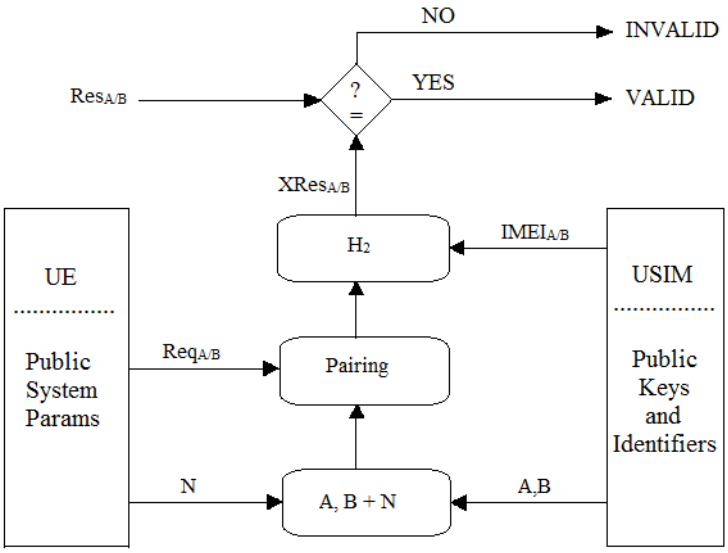


Figure 3: User-to-User authentication

Phase 4: Establish a shared secret key between UE_A and UE_B.

In our proposed scheme we assume that the network operator is not highly trusted, and the UE can only share a secret key. The proposed scheme can provide User-to-User security as well as mutual authentication between the two entities. Users A and B used the pre-shared key K which is distributed in advance and store in SIM card and AuC, this key comes from the standard security architecture in the LTE system, and the parameters $Q_{A/B}$ and $D_{A/B}$ which is distributed in advance during the setup and key generation phase, and this value depends on the identifiers (temporary or permanent) which in turn depends on the current location for the specific mobile station, i.e. the current serving network MME. Then users $UE_{A/B}$ can compute the session key as follows:

For UE_A:

Using the pre-shared key (K) the user UE_A can calculate the following parameters which are distributed during the Setup and key generation phase.

$$\begin{aligned} Q_A &= H_1(IMSI_A/GUTI_A, A) \\ D_B &= x_B Q_B, B. \\ T_A &= KQ_A. \end{aligned}$$

Then compute the shared secret session key

$$SK_A = e(T_A, D_B + x_A Q_B).$$

For UE_B:

By the same way UE_B calculate the following parameters:

$$\begin{aligned} Q_B &= H_1(IMSI_B/GUTI_B, B) \\ D_A &= x_A Q_A, A \\ T_B &= KQ_B. \end{aligned}$$

Then compute the shared secret session key:

$$SK_B = e(T_B, D_A + x_B Q_A).$$

UE_A and UE_B will compute the same shared secret key:

$$\begin{aligned} SK &= SK_A \\ &= SK_B \\ &= e(Q_A, Q_B)^{K(XA+XB)} x_A x_B P. \end{aligned}$$

6 Security Analysis of the Proposed Scheme

This section provides the security analysis of the proposed scheme. The proposed LTE-AKA scheme is more secure than the regular EPS-AKA which has a plethora of flaws as discussed in Section 3. The security analysis for LTE security architecture develops from UE's until the core network HSS/AuC. As the most common security features for mobile communication are discretion (location and data), authentication, access security, and imitation, the LTE security mechanisms should be able to attain these security features. Moreover, all these security features derived from the access level because the access level is the first line of defense against attacks. That means, the proposed LTE-AKA scheme offers a strong user-to-user mutual authentication and key agreement mechanism compared to that of [34]. The security necessities and analysis are as follows.

6.1 Security of the User-to-User Mutual Authentication Scheme

The entity MME has to utilize his secret key x_N to create the signatures and transfer them to the precise users, and UE_A and UE_B cannot create the signature without the knowledge of the MME's secret key, so this feature makes the proposed scheme unforgeable and somehow offers fortification to the network operator side. Furthermore, MME is the lone entity that can verify the legitimacy of the user's signatures; hence no snooping can happen due to the MME's secret key even if the user's secret keys are revealed.

6.2 Security of the Secret Session Key Scheme

The session key attacker can obtain the system parameters and the public keys which are conveyed in public during setup and key generation phase. However, it is difficult for an attacker to work out the session key SK because the attacker does not know the secret keys and the pre-shared key K which are saved securely in both the SIM card and AuC. Furthermore, the attacker can get some information for example one side secret key, but cannot compute the session key. Without knowing all the secret keys x_A, x_B, x_N, which belongs to CDH and it's a hard and difficult problem.

6.3 False Base Station Attack

False base station also referred to as IMSI catcher attack [3, 4, 5], it is a widespread attack in the field of mobile communication security, generally known as man-in-the-middle attack. In this attack, the user's identifiers can put a false base station between the mobile station and base station to act as a real base station. However, our proposed scheme is secure against such attack due to the identifiers protection by using the hash. Therefore, there is no way to try this attack by sending the fake message because the permanent identifier IMEI is used as a message to be signed. Moreover, to compute the SK, the attacker needs to get the secret parameters and they are not known and are not published in public. Furthermore, the proposed scheme provides obscurity to the users somehow by using temporary identifiers (GUTI) instead of (IMSI) when the user is in the roaming mode.

6.4 Known Key Attack and Forward/Backward Secrecy

By obtaining the secret keys of UE_A and UE_B, it still cannot be realistic for the attacker to recover the previous session keys. The reason is that the session key entails the temporary identifiers and the secret keys. Thus, it is impossible to obtain any secret keys or the session key from the public parameters as well as GUTI work as a temporary key for every session. On the other hand, it is also unfeasible to compute the value (x_A, x_B, P) due to the CDH hard problem. The basic EPS-AKA has many flaws as we presented in Section 3, and the most common problem in this context is that the privacy of the user's identities and even their locations by sending the IMSI identifier in clear as we know it as IMSI catcher attack, and many proposed works tried to solve such problems. In general, the proposed scheme is considered to be more secure since it provides user's privacy and access security, achieves user-to-user mutual authentication and key agreement scheme, and the third party (the network side) work as proxy and we consider it as untrusted third party.

6.5 End-to-end Security

Many research works focus on the security between the mobile user and the base station due to the insecure air interface, and it is easy for an attacker to eavesdrop this particular link [8]. However, our proposed scheme provide end-to-end security and only users can compute the session key, and they can authenticate each other as well as the network operator can authenticate the users.

6.6 Replay Attack

The proposed scheme is secure against the replay attack due to the changeable session keys:

$$\begin{aligned} SK &= SK_A = SK_B \\ &= e(Q_A, Q_B)^{K(XA+XB)} x_A x_B P. \end{aligned}$$

The session key derived from the hash value of the temporary identities and the public keys. The temporary identity GUTI is changeable according to the user's location area, and hence when the attacker replays with the previous security parameters, then the request will be rejected because the users UE's will know that this request is invalid.

7 Performance Evaluation

Since 4G cellular systems offer a high specification performance as mentioned in the introduction section, the security feature can be enhanced using the new network utilities as much as a strong security is needed. However, the proposed scheme makes use of these advantages and evaluates the performance of the proposed LTE-AKA protocol.

The performance of our proposed scheme is evaluated using the existing experimental setup of [11, 12] for a variety of cryptographic operations using MIRACLE [32] in PIV 3 GHZ processor with Windows XP operating system and 512 MB memory. From [11, 12] the relative running time for the operations we employed in our proposed model and we define some terms for the running time calculation as follows:

T_p = Pairing operation: 20.01 (ms).

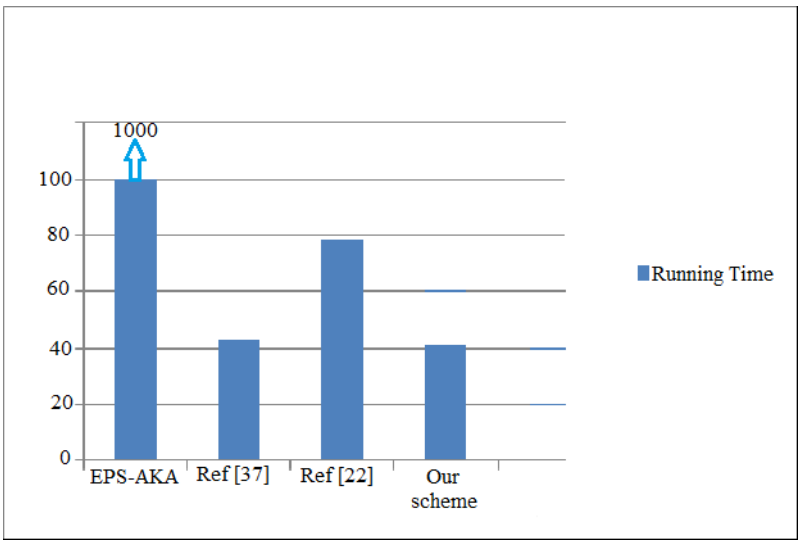


Figure 4: Running time-based efficiency comparison

T_m = Pairing-based scalar multiplication: 6.38 (ms).

T_e = ECC-based scalar multiplication: 0.83 (ms).

T_h = Hash function: 3.04 (ms).

We observe that the implementation of the proposed model required three pairing operations and one exponential operation on the user side and four pairing operations and one exponential operation on the network side, and for the other operations we assumed that the running time is omitted. Table 2 shows the performance efficiency based running time of the proposed model.

According to the computational cost we clearly can note that the total running time in both UE side and MME side is 109.11 (ms). That means, the proposed model scheme is quite reliable to be implemented in the real field of the LTE mobile communication systems comparing with the standard EPS-AKA scheme. Generally, from the above analysis and results it can be noted that the proposed scheme has reasonable computational complexity when it is compared to the basic protocols such as EPS-AKA and Extensible Authentication Protocol (EAP-AKA) which it takes about 1000 ms [28].

In the mobile communication field, computation cost is very important. When a user requests a service to a provider with payment way, the users will care about the transmission and computational cost [16].

Many research works have been proposed schemes in the field of mobile communication security, particularly in authentication and key agreement protocol such as [7, 9, 14, 18, 19, 22, 37, 38], here we give a reasonable computational cost comparison (UE's side) for our proposed scheme with [22, 37]. This comparison will be calculated based on the operation's computational cost for each reference. Table 3 shows comparison of the computational cost efficiency, Figure 4 illustrates comparisons of the performance efficiency based running time and Table 4 shows comparison of the security-based performance efficiency for our proposed scheme with the basic scheme EPS-AKA and [7, 9, 18].

From the above comparisons we can observe that the proposed scheme can be applied in the practical field of LTE cellular system according to the relatively accepted performance efficiency comparing with the call setup process in LTE cellular system, EAP-AKA, and the previous research works.

8 Conclusion

The LTE cellular system possesses considerable communication flexibility, and the agreement of mobile phone manufacturers is also required. However, the improvement of the deployed public key cryptographic algorithms can be very useful. The LTE security architecture is a mature evolved architecture, with both strengths and weaknesses, and therefore, the PKI infrastructure is more secure and it can be modified as well as the LTE security architecture. In this paper, we proposed a secure LTE-AKA scheme which is based on user-to-user security. The proposed scheme is performed at the end-entities, therefore it is more flexible and there is no need to make any change within the core network. Furthermore, we have analyzed the security and the performance of our scheme and realized that the proposed scheme is more flexible and secure than the basic EPS-AKA scheme which has many weaknesses.

References

[1] 3GPP Technical Specification, 3GPP TS 33.102, V5.3.0, Third Generation Partnership Project; Tech-

Table 2: The performance efficiency Time of the proposed scheme

Entities/Phases	UE Side(ms)	MME Side(ms)
Phase 1	$2T_e + T_h$= 4.7	$T_e + T_h$= 3.87
Phase 2	T_e= 0.83	$2T_p + T_m + T_h$= 49.44
Phase 3	$T_p + T_h$= 23.05	None
Phase 4	$T_p + T_e + T_m$= 27.22	None
Total	55.8	53.31

Table 3: Comparison of computational cost efficiency in (ms)

Computational cost	EPS-AKA	[37]	[22]	Our scheme
UE side	1000	43	78.360	42.695

Table 4: Comparison of security-based efficiency

Security Parameters	**EPS-AKA**	**[7]**	**[9]**	**[18]**	**Our scheme**
Mutual authentication	Y	Y	Y	Y	Y
End-to-end security	N	N	N	N	Y
Privacy preserving	N	Y	N	Y	Y
Replay attack	Y	Y	Y	Y	Y
Forward/Backward secrecy	N	Y	N	Y	Y

nical Specifications Group Services and System Aspects; 3G Security; Security Architecture, Sept.2003.

[2] 3GPP Technical Report, 3GPP TR 31.900, V5.3.0., Third Generation Partnership Project; SIM/USIM Internal and External Interworking Aspects, 2003.

[3] 3rd Generation Partnership Project, 3GPP TR 33.821 V9.0.0 (2009-06), Rationale and Track of Security Decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE), Release 9, June 2009.

[4] 3rd Generation Partnership Project, 3GPP TS 33.401 V11.2.0 (2011-12), 3GPP System Architecture Evolution (SAE); Security Architecture, Release 11, Dec. 2011.

[5] 3rd Generation Partnership Project, 3GPP TS 33.401 V8.8.0 (2011-06), 3GPP System Architecture Evolution (SAE); Security Architecture, Release 8, June 2011.

[6] S. Antipolis, *3GPP, TS 33.102, 3G Security; Security Architecture*, 3rd Generation Partnership Project, Technical Report v3.11.0, 2002.

[7] J. Cao, H. Li, M. D. Ma, Y. Y. Zhang, C. Z. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks", *Computer Networks*, vol. 56, no. 8, pp. 2119-2131, 2012.

[8] C. C. Chang, K. L. Chen, M. S. Hwang, "End-to-end security protocol for mobile communications with end-user identification/authentication", *Wireless Personal Communications*, vol. 28, no. 2, pp. 95–106, Jan. 2004.

[9] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing", *IEEE Communication Letters*, vol. 14, no. 1, pp. 54–56, Jan. 2010.

[10] D. Forsberg, G. Horn, W. D. Moeller and V. Niemi, *LTE Security*, John Wiley and Sons, 2010.

[11] D. He and J. Chen, "An efficient certificate-less designated verifier signature scheme", *The International Arab Journal of Information Technology*, vol. 10, no. 4, pp. 389–396, 2013.

[12] D. Hea, J. Chen and R. Zhang, "An efficient identity-based blind signature scheme without bilinear pairings," *Computers & Electrical Engineering*, vol. 37, no. 4, pp. 444–450, July 2011.

[13] X. Huang, Y. Mu, W. Susilo, and F. Zhang, "Short designated verifier proxy signature from pairings", in *Embedded and Ubiquitous Computing (EUC'05)*, LNCS 3823, pp. 835–844, Springer, 2005.

[14] Y. L. Huang, C. Y. Shen, S. W. Shieh, "S-AKA: A provable and secure authentication key agreement protocol for UMTS networks", *IEEE Transactions on Vehicular Technology*, vol. 60, no. 9, pp. 4509-4519, 2011.

[15] M. S. Hwang, C. C. Lee, S. F. Tzeng,"A new proxy signature scheme for a specified group of verifiers", *Information Sciences*, vol. 227, pp. 102–115, Apr. 2013.

[16] M. S. Hwang, C. Y. Liu, "Authenticated encryption schemes: Current status and key issues", *International Journal of Network Security*, vol. 1, no. 2, PP.61–73, Sep. 2005.

[17] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *Advances in Cryptology (EUROCRYPT'96)*, LNCS 1070, pp. 143–154, Springer-Verlag, 1996.

[18] Q. Jing, Y. Zhang, A. Fu and X. Liu, "A privacy preserving handover authentication schemes for EAP-based wireless networks", *IEEE Global Telecommunications Conference (GLOBECOM'11)*, pp. 1–6, Dec. 2011.

[19] Q. Jinga, Y. Zhang, X. Liua and A. Fuc, "An efficient handover authentication scheme with location privacy preserving for EAP-based wireless networks", in *IEEE International Conference on Communications (ICC'12)*, pp. 857–862, 2012.

[20] R. P. Jover and P. Giura, "How vulnerabilities in wireless networks can enable advanced persistent threats", *International Journal on Information Technology*, 2013.

[21] B. Kanga, C. Boydb, Ed Dawsonb, "Identity-based strong designated verifier signature schemes: Attacks and new construction", *Computers & Electrical Engineering*, vol. 35, no. 1, Jpp. 49–53, 2009.

[22] Y. Kim, W. Ren, J. Jo, M. Yang, Y. Jiang, J. Zheng, "SFRIC: A secure fast roaming scheme in wireless LAN using ID-based cryptography", in *Proceedings of IEEE International Conference on Communications (ICC'07)*, pp. 1570-1575, June 2007.

[23] G. M. Koien, "Mutual entity authentication for LTE", in *7th International Wireless Communications and Mobile Computing Conference (IWCMC'11)*, pp. 689–694, July 2011.

[24] F. Laguillaumie and D. Vergnaud, "Designated verifiers signature: Anonymity and efficient construction from any bilinear map", in *Fourth Conference on Security in Communication Networks (SCN'04)*, LNCS 3352, pp. 107–121, Springer-Verlag, 2004.

[25] C. Lai, H. Li, R. Lu, X. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks", *Computer Networks*, vol. 57, no. 17, pp. 3492-3510, Dec. 2013.

[26] P. Lescuyer, T. Lucidarme, *Evolved Packet System (EPS): The LTE and SAE Evolution of 3G UMTS*, John Wiley and Sons Ltd, 2012.

[27] W. Millan, P. Gauravaram, "Cryptanalysis of the cellular authentication and voice encryption algorithm", *IEICE Electronics Express*, vol. 1, no. 15, pp. 453–459, 2004.

[28] C. Politis, K. A. Chew and N. Akhtar, "Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks", *IEEE Wireless Communications*, vol. 11, no. 4, pp. 76–88, Aug. 2004.

[29] M. Purkhiabani, A. Salahi, "Enhanced authentication and key agreement procedure of next generation 3GPP mobile networks", *International Journal of Information and Electronics Engineering*, vol. 2, no. 1, pp. 69–77, Jan. 2012.

[30] S. Saeednia, S. Kramer, and O. Markovitch, "An efficient strong designated verifier signature scheme", in *The 6th International Conference on Information Security and Cryptology (ICISC'03)*, LNCS 2971, pp. 40–54, Springer-Verlag, 2003.

[31] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A tutorial," *IEEE Communications Magazine*, vol. 47, no. 2, pp. 84–91, 2009.

[32] M. Scott, *MIRACLE – Multiprecision Integer and Rational Arithmetic C/C++ Library*, Shamus Software Ltd, Dublin, Ireland, 2003. (`http://www.shamus.ie`)

[33] W. Susilo, F. Zhang, and Y. Mu."Identity-based strong designated verifier signature schemes", in *Proceedings of the 9th Australasian Conference on Information Security and Privacy (ACISP'04)*, LNCS 3108, pp. 313–324, SpringerVerlag, 2004.

[34] C. E. Vintila, V. V. Patriciu, I. Bica, "Security analysis of LTE access network", in *The Tenth International Conference on Networks (ICN'11)*, pp. 29–34, Jan. 2011.

[35] D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm", in *Advances in Cryptology (CRYPTO'97)*, LNCS 1294, pp. 526–537, Springer, 1997.

[36] H. Xiong, Z. Qin, and Fagen Li, "A certificateless proxy ring signature scheme with provable security", *International Journal of Network Security*, vol. 12, no. 2, pp.92–106, Mar. 2011.

[37] C. Zhang, R. Lu, P. Ho and A. Chen, "A location privacy preserving authentication scheme in vehicular networks", in *IEEE Wireless Communications and Networking Conference (WCNC'08)*, pp. 2543–2548, 2008.

[38] Y. Zhang, X. F. Chen, J. Li, H. Li, "Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks", *Computer Networks*, vol. 75, pp. 192-211, 2014.

Mohammed Ramadan He received his B.S. degree in communications engineering from Karary University in 2007, Khartoum, Sudan, and M.S. degree in computer engineering, information security (GSM security) from University of Electronic Science and Technology of China in 2013, Chengdu, China. He is currently working toward the Ph.D. degree in Information Security, Mobile Communications Security from University of Electronic Science and Technology of China. His current research interests include mobile communications security (LTE security).

Fagen Li received his B.S. degree from Luoyang Institute of Technology, Luoyang, China, in 2001, M.S. degree from Hebei University of Technology, Tianjin, China in 2004 and Ph.D. degree in cryptography from Xidian University, Xi'an, China in 2007. From 2008 to 2009, he was a postdoctoral fellow in Future University Hakodate, Hokkaido, Japan, which is supported by the

Japan Society for the Promotion of Science. He worked as a research fellow in the Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan, from 2010 to 2012. He is now an associate professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. His recent research interests include cryptography and network security. He has published more than 70 papers in the international journals and conferences.

ChunXiang Xu is a professor at University of Electronic Science and Technology of China (UESTC). Her research interests include information security, cloud computing security and cryptography. She received her PhD, M.Sc. and B.Sc. degrees at Xidian University, in 2004, 1988 and 1985 respectively, PR China.

Abdeldime Mohamed Salih is a lecture with Karary University, Khartoum-Sudan, now he is a Ph.D. student with Southeast University, School of Information Science and Communication Engineering, Nanjing.

Hisham Abdalla is a doctoral student at University of Electronic Science and Technology of China (UESTC). He received his M.Sc. degree from UESTC and BE degree in computer engineering from Karary University in 2006. His research interests include cloud computing security, cryptography and digital right management.

Ahmed Abdalla He received the B.S. Degree in Electrical Engineering from Karary university in 2005, Khartoum Sudan and the M.S. Degree in M.Sc. in Electronic Engineering, Information and signal processing form University of Electronic Science and Technology of China in 2013, Chengdu, China. He is currently working toward the PhD. Degree Electronic Engineering from University of Electronic Science and Technology of China. His current research interests include radar counter countermeasure and radar signal processing.

Secure and Efficient Smart Card Based Remote User Password Authentication Scheme

Jianghong Wei, Wenfen Liu and Xuexian Hu
(Corresponding author: Jianghong Wei)

State Key Laboratory of Mathematical Engineering and Advanced Computing
Zhengzhou, Henan Province 450002, China
(Email: jianghong.wei.xxgc@gmail.com)
(Received Dec. 6, 2014; revised and accepted Feb. 10 & Mar. 23, 2015)

Abstract

In distributed systems, the smart card based password authentication, as one of the most convenient and efficient two-factor authentication mechanisms, is widely used to ensure that the protected services are not available to unauthorized users. Recently, Li et al. demonstrated that the smart card based password authentication scheme proposed by Chen et al. cannot provide perfect forward secrecy as they claimed. In addition, the password change phase of the scheme is unfriendly and inefficient. Subsequently, Li et al. presented an enhanced smart card based password authentication scheme to overcome the above flaws existing in Chen et al.'s scheme. Furthermore, Kumari and Khan, and Jiang et al. demonstrated that Chen et al.'s scheme cannot resist off-line password guessing attacks, and also proposed an improved scheme, respectively. In this study, we first illustrate that Li et al.'s scheme, and Kumari and Khan's scheme both fail to achieve the basic security requirement of the smart card based password authentication, namely, once the private information stored in the smart card has been extracted, the schemes would be vulnerable to off-line password guessing attacks. We also point out that Jiang et al.'s scheme, as well as Kumari and Khan's scheme cannot provide perfect forward secrecy. Then, we introduce a new smart card based password authentication scheme. By presenting concrete analysis of security and performance, we show that the proposed scheme cannot only resist various well-known attacks, but also is more efficient than other related works, and thus is feasible for practical applications.

Keywords: Password, remote access, smart card, two-factor authentication

1 Introduction

Owing to information technology rapid progression, more and more resources are distributed in the form of network services provided and managed by servers in distributed systems. Remote user authentication schemes are used to ensure that these protected services are not available to unauthorized users. Most of early authentication mechanisms [1, 15, 18, 23] are solely based on the password. In these schemes, the remote server maintains a table to record the information about each user's password, and exploits it to verify the privilege of the corresponding user. However, while widely implemented in many real life applications (e.g., private corporations, banking systems, database management systems), password authentication schemes will inescapably suffer from several attacks, such as dictionary attacks, password table tampering, etc.

To conquer these attacks and improve the system security, Chang and Wu [2] introduced smart card based password authentication scheme, which has become one of the most convenient and commonly used two-factor authentication mechanisms. In the context of the smart card based password authentication scheme, each user possesses a password easy to remember and a smart card, which is issued by the remote server, and used to store some private data. The password and smart card of each user are bonded together by the remote server, that is, once successful mutual authentication requires the user to provide the correct password and corresponding smart card simultaneously. In order to evaluate the security of smart card based password authentication scheme, Xu et al. [24] suggested that there should be two assumptions of the adversary's capabilities explicitly made in this kind of authentication scheme:

1) The adversary has total control over the communication channel between the users and the remote server in the authentication phase, which means the adversary can intercept, insert, delete, or modify any message transmitted in the channel.

2) The adversary may either steal a user's smart card and then extract the information from it by the method introduced by Kocher et al. [13] and

Messerges et al. [19], or obtain a user's password, but not the both.

In fact, the first assumption is exactly the Dolev-Yao Threat Model [6], which has been widely accepted as the standard threat model for cryptographic protocols. The second assumption characters the basic security requirement of two-factor authentication scheme, that is, as long as the private information of the two authentication factors have not been disclosed simultaneously, the scheme should be still secure. This is also why the two-factor authentication scheme is more secure than the single-factor authentication scheme. The above two assumptions, which can also be considered as a security model for the smart card based password authentication scheme, have been widely approved, and the security analyses of the authentication schemes [3, 4, 5, 7, 8, 9, 10, 11, 12, 14, 16, 17, 20, 21, 22, 24] are all based on them.

Since the introduction of smart card based password authentication, it has attracted many researcher's attention, and a lot of such schemes have been presented. However, most of them are flawed. Such examples are that, Xu et al.'s [24] scheme suffers from impersonation attacks, Das's [5] scheme is vulnerable to gateway node by-passing attack and privileged-insider attack.

Most recently, Chen et al. [4] illustrated that the schemes proposed by Song [20] and Sood et al. [21] still have various security flaws being ignored, and then proposed a robust smart card based remote user password authentication scheme. They claimed that their scheme can resist various attacks and provide perfect forward secrecy. However, Li et al. [17] pointed out that Chen et al.'s [4] scheme fails to ensure forward secrecy, and the password change phase of the scheme is unfriendly and inefficient. To overcome the problems mentioned above, Li et al. also introduced an enhanced smart card based remote user password authentication scheme. Furthermore, Kumari and Khan[14], as well as Jiang et al. [11] demonstrated that Chen et al.'s [4] scheme is even insecure against off-line password guessing attacks, and provided an improved scheme, respectively.

In this paper, we will demonstrate that Li et al.'s [17] scheme, and Kumari and Khan's [14] scheme are not secure under the assumptions (1) and (2). Specifically, the adversary can launch off-line password guessing attacks once the private data stored in the smart card have been extracted by the adversary. In addition, we point out that Kumari and Khan's [14] scheme is not correct in some case, and cannot provide perfect forward secrecy. We also note that Jiang et al.'s [11] scheme cannot provide perfect forward secrecy and friendly password change, since it inherits the main body of Chen et al.'s [4] scheme. Furthermore, to conquer these attacks and drawbacks, we propose a new smart card based password authentication scheme. Our scheme is not only secure against various well-known attacks (e.g., off-line password guessing attack, impersonation attack, replay attack, etc.) under the assumptions (1) and (2), but also is more efficient than previous schemes without loosing necessary security properties (e.g., forward secrecy, mutual authentication etc.).

The remainder of the paper is structured as follows: we provide review and cryptanalysis of Li et al.'s [17] scheme and Kumari and Khan's [14] scheme in Section 2 and Section 3, respectively. And then a secure and efficient smart card based remote user password authentication scheme is proposed in Section 4. Section 5 discusses the performance and security of our proposal. Finally, we conclude in Section 6.

2 Review and Cryptanalysis of Li et al.'s Scheme

In this section, we first briefly review the remote user authentication scheme proposed by Li et al. [17], and then demonstrate that their scheme is vulnerable to off-line password guessing attack by presenting the concrete attack process. For convenience, we summarize the notations used throughout this paper in Table 1.

2.1 Review of Li et al.'s Scheme

Li et al.'s [17] scheme consists of four phases: initialization, registration, authentication, password change. The details of the scheme are given as follows.

2.1.1 Initialization Phase

To initialize, the remote server S selects large prim numbers p and q such that $p = 2q + 1$. S also chooses a random number $x \in Z_q^*$ as its master secret key, as well as a secure one-way hash function $h(\cdot) : \{0,1\}^* \rightarrow Z_p^*$.

2.1.2 Registration Phase

When a user U_i wants to register to become a legal user, he/she first selects a password PW_i and unique identity ID_i. Then, the registration procedure proceeds as follows:

1) U_i submits the registration request message $\{ID_i, PW_i\}$ to the remote server via a secure channel.

2) Upon receiving the request message, S computes $A_i = h(ID_i||PW_i)^{PW_i} \bmod p$ and $B_i = h(ID_i)^{x+PW_i} \bmod p$.

3) S stores $\{A_i, B_i, p, q, h(\cdot)\}$ into a smart card, and issues the smart card to U_i via a secure channel.

2.1.3 Authentication Phase

When a legal user U_i wants to login into the server for acquiring some services, he/she first attaches the smart card to a device reader, and inputs his/her identity ID_i and password PW_i. Then, the authentication mechanism performs as follows:

Table 1: The notations used throughout this paper

Symbol	Description
U_i	The ith user
S	The remote server
$\mathcal{A}$	The adversary
ID_i	The user U_i's identity
PW_i	The user U_i's password
x	The master secret key of the remote server
p and q	Two large prime numbers such that $p = 2q + 1$
T	The tiemstamp
ΔT	The maximum transmission delay
T_e	The running time for once modular exponentiation operation
T_m	The running time for once modular multiplication/inverse operation
T_h	The running time for once hash operation
T_s	The running time for once symmetric encryption/decryption operation
$h(\cdot)$	A secure one-way hash function
Z_q	The ring of integers modulo q
Z_q^*	The multiplicative group of Z_q
$\|\|$	The concatenation operation

1) The smart card computes $A_i' = h(ID_i||PW_i)^{PW_i} \bmod p$, and checks that whether A_i' is equal to A_i stored in the smart card. If not, the smart card terminates the session. Otherwise, the smart card performs the following steps.

2) The smart card chooses a random number $\alpha \in Z_q^*$, and then computes:

$$\begin{aligned} C_i &= B_i/h(ID_i)^{PW_i} \bmod p, \\ D_i &= h(ID_i)^{\alpha} \bmod p, \\ M_i &= h(ID_i||C_i||D_i||T_i), \end{aligned}$$

where T_i is the current timestamp. Finally, the smart card sends the authentication request message $\{ID_i, D_i, M_i, T_i\}$ to the remote server S.

3) Upon receiving the authentication request message, S checks if the identity ID_i is valid and $T_i' - T_i \leq \Delta T$, where T_i' is the current timestamp. If either or both are invalid, S rejects the authentication request.

4) By use of the received authentication request message, S first computes:

$$C_i' = h(ID_i)^x, \text{ and } M_i' = h(ID_i||C_i'||D_i||T_i).$$

Then, S compares M_i' with M_i. If they are equal, the user U_i is authenticated by the remote server S. Otherwise, S rejects the authentication request.

5) If the user is authenticated by the remote server S, the server first chooses a random number $\beta \in Z_q^*$, and computes $V_i = h(ID_i)^{\beta} \bmod p$. Then S sets the shared session key as $sk = D_i^{\beta} \bmod p$. Finally, S gets the current timestamp T_S, computes $M_S = h(ID_i||V_i||sk||T_S)$, and then sends the response message $\{ID_i, V_i, M_S, T_S\}$ to U_i.

6) On receiving the response message, U_i checks ID_i and compares T_S' with T_S, where T_S' is the time that the response message is received. If ID_i is valid and $T_S' - T_S \leq \Delta T$, U_i computes:

$$sk' = V_i^{\alpha} \bmod p,\ M_S' = h(ID_i||V_i||sk'||T_S).$$

Then, U_i checks that whether M_S' is equivalent to the received M_S. If not, the session is terminated. Otherwise, the remote server S is authenticated by the user U_i, and an agreed session key $sk = h(ID_i)^{\alpha\beta} \bmod p$ is shared between them.

2.1.4 Password Change Phase

When the user U_i wants to replace his/her password PW_i with a new password PW_i^{new}, he/she first inputs ID_i and PW_i into the smart card. Then, the smart card carries out the following steps:

1) The smart card computes $A_i' = h(ID_i||PW_i)^{PW_i} \bmod p$, and compares A_i' with the stored value A_i. If they are not equal, the request is rejected. Otherwise, the user is asked to input a new password PW_i^{new}.

2) After receiving the new password, the smart card computes:

$$\begin{aligned} A_i^{new} &= h(ID_i||PW_i^{new})^{PW_i^{new}} \bmod p, \\ B_i^{new} &= B_i \cdot h(ID_i)^{PW_i^{new}}/h(ID_i)^{PW_i} \bmod p. \end{aligned}$$

The smart card replaces A_i, B_i with A_i^{new}, B_i^{new}, respectively.

2.2 Cryptanalysis of Li et al.'s Scheme

Now, focus on Li et al.'s scheme [17], we present two kinds of off-line password guessing attacks once the private information stored in the smart card had been disclosed. To begin with the following discussions, by the assumption (1), we first suppose that the adversary $\mathcal{A}$ has recorded the messages $\{ID_i, D_i, M_i, T_i\}$ and $\{ID_i, V_i, M_S, T_S\}$, which are involved in some successful authentication completed between the user U_i and the server S. Then, by the assumption (2), the adversary $\mathcal{A}$ can obtain U_i's smart card, and extract the private data $\{A_i, B_i, p, q, h(\cdot)\}$ stored in the smart card by the method introduced by Kocher et al. [13] and Messerges et al. [19].

The adversary $\mathcal{A}$ launches the first kind of off-line guessing attacks as follows:

Step 1. $\mathcal{A}$ selects a candidate password PW_i^* from the dictionary space $\mathcal{D}$.

Step 2. $\mathcal{A}$ computes $A_i^* = h(ID_i||PW_i^*)^{PW_i^*} \bmod p$.

Step 3. $\mathcal{A}$ checks that whether A_i^* is equal to A_i. If yes, $\mathcal{A}$ can conclude that PW_i^* is correct. Otherwise, $\mathcal{A}$ repeats the above procedure until the correct password PW_i is yielded.

Furthermore, $\mathcal{A}$ can launch the second kind of off-line guessing attacks as follows:

Step 1. $\mathcal{A}$ selects a candidate password PW_i^* from the dictionary space $\mathcal{D}$.

Step 2. $\mathcal{A}$ computes $C_i^* = B_i/h(ID_i)^{PW_i^*} \bmod p$.

Step 3. $\mathcal{A}$ computes $M_i^* = h(ID_i||C_i^*||D_i||T_i)$. Note that if $PW_i = PW_i^*$ holds, so does $C_i = C_i^*$ and $M_i = M_i^*$.

Step 4. $\mathcal{A}$ checks that whether M_i^* is equal to M_i. If yes, $\mathcal{A}$ can conclude that PW_i^* is correct. Otherwise, $\mathcal{A}$ repeats the above procedure until the correct password PW_i is yielded.

Denote by $|\mathcal{D}|$ the number of passwords in the dictionary space $\mathcal{D}$. Then, the running time of the first attack procedure is $\mathcal{O}(T_e + T_h)$, and the running time of the second attack procedure is $\mathcal{O}(T_e + T_m + 2T_h)$. That means, regardless of which method to use, the time for the adversary to recover U_i's password is proportional to the size of the password space $\mathcal{D}$. Consequently, in practise, for a restricted password space, the adversary may recover the password in seconds on a PC.

3 Review and Cryptanalysis of Kumari and Khan's Scheme

In this section, we first briefly review the smart card based remote user password authentication scheme proposed by Kumari and Khan [14], and then provide a cryptanalysis of the scheme to demonstrate that the scheme is not correct in some case, suffers from off-line password guessing attack, and can not provide perfect forward secrecy.

3.1 Review of Kumari and Khan's Scheme

Similarly, Kumari and Khan's [14] scheme also consists of four phases, i.e., initialization phase, registration phase, authentication phase and password change phase. We briefly introduce the concrete scheme as follows.

3.1.1 Initialization Phase

For initialization, the remote server S chooses two large primes p and q such that $p = 2q+1$ and $n = pq$, and keeps p and q secret. S selects a random number $x \in Z_q^*$ as its long-term private key. S also picks up a secure one-way hash function $h(\cdot)$. In addition, S preserves a registration table R_GR to record registration information about all legal users, i.e., an unique tuple $(ID_i, T_r, x \cdot p \oplus (ID_i||T_r))$ for each registered user U_i, where T_r is the registration time of U_i.

3.1.2 Registration Phase

To become a legal user and obtain services provided by the remote server, one needs to register at S to get the corresponding privilege. The detailed registration procedure performs as follows:

1) A user U_i selects his/her identity ID_i, and submits the registration request message $\{ID_i\}$ to the remote server S through a secure channel.

2) After receiving the request message, S checks whether the received identity ID_i is in the table R_GR or not. If yes, S rejects the request; otherwise, S generates a tuple $(ID_i, T_r, x \cdot p \oplus (ID_i||T_r))$, and adds it into R_GR. Here, T_r is the timestamp that the user U_i registered to S, $\oplus$ is bitwise XOR operation.

3) S sets $A_i = h(ID_i)^{x+T_r+PW_0} \bmod n$, $B_i = (h(ID_i)^{x+T_r} \bmod n) \otimes PW_0 \otimes ID_i$, and generates a temporary identity $EID_i = E_{x+p}(ID_i||T_r)$ by encrypting ID_i and T_r with the private key $x + p$. Here, $\otimes$ is bitwise NOR operation. Then S stores $\{A_i, B_i, EID_i, n, h(\cdot), E_{key}(\cdot), D_{key}(\cdot)\}$ into a smart card, and issues the smart card to U_i through a secure channel.

4) Upon receiving the smart card, U_i chooses a new password PW_i, and replace the default password PW_0 with PW_i as described in Section 3.1.4.

3.1.3 Authentication Phase

If a registered user U_i wants to obtain the corresponding services provided by a legal remote server S, he/she needs to accomplish mutual authentication described as follows:

1) The user U_i first inserts his/her smart card to a device reader, and keys in ID_i and PW_i. Then, the smart card computes $C_i = (A_i/h(ID_i)^{PW_i}) \mod n$, $B_i^* = C_i \otimes PW_i \otimes ID_i$. The smart card checks whether B_i^* is equal to B_i. If not, the smart card terminates the authentication process; otherwise, the smart card chooses $\alpha \in Z_n^*$, and computes:

$$\begin{aligned} D_i &= h(ID_i)^{\alpha} \bmod n, \\ W_i &= C_i \cdot D_i \bmod n, \\ M_i &= h(ID_i||C_i||D_i||T_i), \end{aligned}$$

where T_i is the current timestamp. Finally, the smart card sends the authentication request message $\{EID_i, D_i, M_i, T_i\}$ to the server S through a public channel.

2) After receiving the authentication request message from U_i, the server S first gets the current timestamp T_{S1}, and checks if $(T_i - T_{S1}) > \Delta T$. If yes, S terminates the authentication process; otherwise, S gets a tuple $(ID_i||T_r)$ through decrypting EID_i with its private key $x + p$.

3) If there exists a record corresponding to the tuple $(ID_i||T_r)$ in the table R_GR, S first computes:

$$\begin{aligned} C_i^* &= h(ID_i)^{x+T_r} \bmod n, \\ W_i^* &= C_i^* \cdot D_i \bmod n, \\ M_i^* &= h(ID_i||C_i^*||D_i||W_i^*||T_i). \end{aligned}$$

Then, S checks if $M_i^* = M_i$. If not, S rejects the authentication request; otherwise, S authenticates the user U_i.

4) S acquires the current timestamp T_{S2}, and computes the session key:

$$\begin{aligned} sk &= h(W_i^*||T_{S2}), \\ EID_i^* &= E_{x+p}(ID_i||T_r||T_{S2}), \\ M_S &= E_{C_i^*}(ID_i||EID_i^*||W_i^*||T_{S2}). \end{aligned}$$

Then S sends the response message $\{M_S\}$ to the user U_i, and replaces the value $x \cdot p \oplus h(ID_i||T_r)$ with $x \cdot p \oplus h(ID_i||T_r||T_{S2})$ in R_GR.

5) After receiving the response message from the server S, the smart card first obtains the tuple $(ID_i||EID_i^*||W_i^*||T_{S2})$ by decrypting M_S with its private key C_i^*. Then, the smart card checks the validity of ID_i, the freshness of T_{S2}, and verifies if $W_i^* = W_i$, $EID_i^* = EID_i$. If all of tests are passed, the smart card authenticates the remote server S; otherwise, it puts an end to the authentication process.

6) The smart card generates the session key $sk = h(W_i||T_{S2})$, and replaces the value EID_i with EID_i^*.

3.1.4 Password Change Phase

When a user U_i wants to update his/her password, (s)he inputs ID_i and PW_i followed with a new password PW_i^{new}. Then, the smart card proceeds as follows:

1) Compute $C_i = (A_i/h(ID_i)^{PW_i}) \mod n$, $B_i^* = C_i \otimes PW_i \otimes ID_i$, and check if $B_i^* = B_i$. If not, reject the request; otherwise, compute $A_i^{new} = C_i \cdot h(ID_i)^{PW_i^{new}} \mod n$, $B_i^{new} = C_i \otimes PW_i^{new} \otimes ID_i$.

2) Replace A_i and B_i with A_i^{new} and B_i^{new}, respectively.

3.2 Cryptanalysis of Kumari and Khan's Scheme

In this section, by presenting concrete analysis and attacks, we demonstrate that Kumari and Khan's [14] scheme is not correct in some case, suffers from off-line password guessing attack once the private information stored in the smart card has been extracted by the adversary by the method introduced by Kocher et al. [13] and Messerges et al. [19], and can not provide perfect forward secrecy.

3.2.1 Correctness

In the authentication phase of Kumari and Khan's scheme, we notice that the smart card need to compute $C_i = A_i \cdot 1/h(ID_i)^{PW_i} \mod n$. However, since $n = pq$ is a composite number, in some case (i.e., $gcd(n, h(ID_i)^{PW_i}) \neq 1$), $1/h(ID_i)^{PW_i} \mod n$ does not exist, and thus the smart card can not compute C_i. Although the probability that the aforementioned case occurs is less than $1 - \frac{\varphi(n)}{n} = \frac{p+q-1}{n}$, where $\varphi(\cdot)$ is Euler function, and is negligible when p and q are large enough, the essential point is that the correctness of Kumari and Khan's scheme is not perfect.

3.2.2 Off-line Password Guessing Attack

By the assumption (1), we first suppose that the adversary $\mathcal{A}$ has intercepted an authentication request message $\{EID_i^*, D_i, M_i, T_i\}$ and the associated response message $\{M_S = E_{C_i^*}(ID_i||EID_i^*||W_i^*||T_{S2})\}$ exchanged between the user U_i and the server S. Then, by the assumption (2), the adversary $\mathcal{A}$ can obtain U_i's smart card, and extracts the data $(A_i, B_i, h(\cdot), n)$. Subsequently, $\mathcal{A}$ can launch off-line password guessing attacks as follows:

Step 1. $\mathcal{A}$ picks up a candidate identity ID_i^* and a candidate password PW_i^* from two different dictionaries $\mathcal{D}_{id}$ and $\mathcal{D}_{pw}$, respectively.

Step 2. $\mathcal{A}$ computes $C_i^* = A_i/h(ID_i^*)^{PW_i^*} \mod n$, $B_i^* = C_i^* \otimes PW_i^* \otimes ID_i^*$. Note that if $ID_i^* = ID_i$ and $PW_i^* = PW_i$, then it holds that $C_i^* = C_i$ and $B_i^* = B_i$, which means that the adversary $\mathcal{A}$ can verify the validity of ID_i^* and PW_i^* by checking if $B_i^* = B_i$.

Step 3. If $B_i^* = B_i$, $\mathcal{A}$ concludes that ID_i^* and PW_i^* are correct identity and password, respectively. Otherwise, $\mathcal{A}$ repeats the above procedure until the correct identity and password are found.

In addition, similar to the above procedure, not only B_i, but also the recorded messages M_i and M_S can be used to verify the validity of candidate password and identity. We omit the details here.

In Kumari and Khan's scheme, we notice that the identity and password are both selected by the user him/hefself, which indicates that they are values easy to remember and guess, rather than random values with high entropy. The following analysis will show that the above attack can be finished in polynomial time, which is contrary to Kumari and Khan's [14] claim that "it is not possible to guess two correct values ID_i and PW_i simultaneously in polynomial time", and thus the attack is feasible in practice.

Denote by $|\mathcal{D}_{id}|$ and $|\mathcal{D}_{pw}|$ the sizes of dictionary space $\mathcal{D}_{id}$ and $\mathcal{D}_{pw}$, respectively. Since the identity and password are human-remember and guessable, we can suppose that $|\mathcal{D}_{id}| = f_{id}(\lambda)$ and $|\mathcal{D}_{pw}| = f_{pw}(\lambda)$, where $f_{id}(\cdot)$ and $f_{pw}(\cdot)$ are polynomials, and λ is some fixed parameter. Roughly evaluating, the running time of the above attack is $\mathcal{O}(T_e + 2T_m + T_h)$. Thus, the time that the adversary gets the correct identity and password is at most $f_{id}(\lambda)f_{pw}(\lambda)\cdot\mathcal{O}(T_e+2T_m+T_h) = g(\lambda)\cdot\mathcal{O}(T_e+2T_m+T_h)$, where $g(\lambda) = f_{id}(\lambda)\cdot f_{pw}(\lambda)$, and is still a polynomial. That is, the adversary can recover the identity and password in polynomial time.

3.2.3 Perfect Forward Secrecy

Perfect forward secrecy ensures that previously established session keys are still secure even if the secret values of any participant involved in an authentication scheme are disclosed. Kumari and Khan [14] assumed that the secret value p could not be disclosed, and then claimed that their scheme could provide perfect forward secrecy. In fact, to complete once authentication process of their scheme, the server is required to possess the secret values x and $x + p$ simultaneously, where $x + p$ is used to generate a new temporary identity for the user by calling a symmetric encryption scheme. This suggests that the role of $x + p$ is the same with x. Thus, when considering perfect forward secrecy of their scheme, as well as x, $x+p$ should also be revealed.

Now, we illustrate that Kumari and Khan's [14] scheme can not provide perfect secrecy when the server's secret values x and $x + p$ are allowed to disclose. Suppose the adversary $\mathcal{A}$ has recorded an authentication request message $\{EID_i, D_i, M_i, T_i\}$ and the associated response message $\{M_S\}$, then $\mathcal{A}$ obtains (ID_i, T_r) by decrypting EID_i with $x + p$, and computes $C_i^* = h(ID_i)^{p+T_r}$. Furthermore, $\mathcal{A}$ can get $(ID_i, EID_i^*, W_i^*, T_{S2})$ by decrypting M_S with C_i^*, and retrieve the corresponding session key $sk = h(W_i^*||T_{S2})$. Thus, Kumari and Khan's [14] scheme can not provide perfect forward secrecy.

4 The Proposed Scheme

To conquer the security flaws existing in the schemes of Li et al. [17] and Kumari and Khan [14], we now propose a new smart card based remote user password authentication scheme. Our proposal also makes up of four phases, i.e., initialization phase, registration phase, authentication phase and password change phase.

4.1 Initialization Phase

Initially, the remote server S selects large prime numbers p and q such that $p = 2q + 1$. S also chooses its master secret key $x \in Z_q^*$, and a secure hash function $h(\cdot) : \{0,1\}^* \rightarrow Z_p^*$.

4.2 Registration Phase

As showed in Fig.1, when a user U_i wants to register to become a new legal user, the registration procedure is performed as follows:

1) U_i selects his/her identity ID_i and password PW_i, then submits the registration request message $\{ID_i, PW_i\}$ to the server S via a secure channel.

2) Upon receiving the registration request message, S checks that whether ID_i is valid or not. If not, S rejects the demand. Otherwise, S computes $B_i = h(x||ID_i)$, $A_i = B_i + h(PW_i||ID_i)$.

3) S stores $\{A_i, p, q, h(\cdot)\}$ into a smart card, and then issues the smart card to U_i via a secure channel.

4.3 Authentication Phase

When a user wishes to login into the server S for obtaining some services, he/she first attaches his/her smart card to a device reader, and inputs ID_i and PW_i. Then the authentication procedure, as illustrated in Fig.2, proceeds as follows:

1) The smart card first computes $B_i = A_i - h(PW_i||ID_i)$, and then selects a random number $\alpha \in Z_q^*$, and computes:

$$\begin{aligned} D_i &= h(ID_i)^{\alpha} \bmod p, \\ D_i^* &= D_i + B_i, \\ M_i &= h(ID_i||D_i^*||T_i), \end{aligned}$$

where T_i is the current time. Finally, the smart card sends the authentication request message $\{ID_i, D_i^*, M_i, T_i\}$ to the server.

2) On receiving the authentication request message, S checks if ID_i is valid and $T_i' - T_i \leq \Delta T$, where T_i' is the time that the message is received. If either or both are invalid, the request is rejected. Furthermore, S checks that whether $M_i' = h(ID_i||D_i^*||T_i)$ is equal to M_i or not. If not, the request is also rejected.

Registration phase

User U_i		Server S
Chooses ID_i and PW_i.	$\{ID_i, PW_i\}$ $\longrightarrow$	Computes: $B_i = h(x\|\|ID_i)$, $A_i = B_i + h(PW_i\|\|ID_i)$.
	$\longleftarrow$ Smart card	Smart card $\leftarrow \{A_i, p, q, h(\cdot)\}$.

Figure 1: Registration phase of the proposed scheme

Authentication phase

$U_i(ID_i, PW_i,$ Smart card)		$S(x)$
Inputs ID_i, PW_i, $B_i = A_i - h(ID_i\|\|PW_i)$. Selects $\alpha \in_R Z_q^*$, computes: $D_i = h(ID_i)^\alpha \bmod p$, $D_i^* = D_i + B_i$, $M_i = h(ID_i\|\|D_i^*\|\|T_i)$.	$\{ID_i, D_i^*, M_i, T_i\}$ $\longrightarrow$	Verifies ID_i and T_i. $M_i' = h(ID_i\|\|D_i^*\|\|T_i)$?= M_i. Selects $\beta \in_R Z_q^*$, computes: $V_i = h(ID_i)^\beta$, $B_i' = h(x\|\|ID_i)$, $D_i' = D_i^* - B_i'$, $Z_i = (D_i')^\beta \bmod p$, $M_S = h(ID_i\|\|D_i'\|\|V_i\|\|Z_i\|\|T_S)$.
	$\longleftarrow$ $\{ID_i, V_i.M_S, T_S\}$	
Checks ID_i and T_S. $Z_i' = V_i^\alpha \bmod p$, $M_S' = h(ID_i\|\|D_i\|\|V_i\|\|Z_i'\|\|T_S)$?= M_S. $sk = h(ID_i\|\|D_i\|\|V_i\|\|Z_i')$ $R_i = h(ID_i\|\|D_i^*\|\|V_i\|\|Z_i'\|\|T_i^{new})$	$\{ID_i, R_i, T_i^{new}\}$ $\longrightarrow$	Verifies ID_i and T_i^{new} $R_i' = h(ID_i\|\|D_i^*\|\|V_i\|\|Z_i'\|\|T_i^{new})$?= R_i $sk' = h(ID_i\|\|D_i'\|\|V_i\|\|Z_i)$

Figure 2: Authentication phase of the proposed scheme

3) S selects a random $\beta \in Z_q^*$, and first computes $V_i = h(ID_i)^\beta \bmod p$, $Z_i = (D_i^*)^\beta \bmod p$, and then sets:

$$\begin{aligned} B_i' &= h(x||ID_i), \\ D_i' &= D_i^* - B_i', \\ M_S &= h(ID_i||D_i'||V_i||Z_i||T_S), \end{aligned}$$

where T_S is the current time. Finally, S sends the message $\{ID_i, V_i, M_S, T_S\}$ to U_i.

4) After receiving the message, the smart card checks ID_i and compares T_S with T_S', where T_S' is the time that the message is received. If ID_i is valid and $T_S' - T_S \leq \Delta T$, S computes $Z_i' = V_i^\alpha \bmod p$, $M_S' = h(ID_i||D_i||V_i||Z_i'||T_S)$. If $M_S' \neq M_S$, the session is terminated. Otherwise, the server S is authenticated by the user U_i, and the shared session key is set as $sk = h(ID_i||D_i||V_i||Z_i')$. Furthermore, U_i gets the current time T_i^{new}, and generates a response message $R_i = h(ID_i||D_i||V_i||Z_i'||T_i^{new})$, and then sends the message $\{ID_i, R_i, T_i^{new}\}$ to S.

5) Upon receiving the response message, S checks ID_i and T_i^{new}. If they are valid, S computes $R_i' = h(ID_i||D_i'||V_i||Z_i||T_i^{new})$. If $R_i' \neq R_i$, S terminates the session. Otherwise, U_i is authenticated by S, and the shared session key is set as $sk' = h(ID_i||D_i'||V_i||Z_i)$. Finally, an agreed session key $sk = sk'$ is established between the user and the server.

4.4 Password Change Phase

This phase is invoked whenever a user U_i wants to replace his/her password PW_i with a new password PW_i^{new}. The specified procedure is performed as follows:

1) U_i attaches his/her smart card to a device reader, and inputs ID_i and PW_i, followed with the new password PW_i^{new}.

2) The smart card computes $A_i^* = A_i - h(PW_i||ID_i) + h(PW_i^{new}||ID_i)$. Then the smart card replaces A_i with A_i^*.

5 Security Analysis and Performance Comparisons

In this section, we present the security and performance analysis of our proposal, and compare it with other related schemes.

5.1 Resist Off-line Password Guessing Attacks

In this kind of attack, an adversary $\mathcal{A}$ is supposed to be able to get the private data $\{A_i, p, q, h(\cdot)\}$ stored in the user U_i's smart card, where $A_i = h(x||ID_i) + h(PW_i||ID_i)$. The adversary $\mathcal{A}$ may select a candidate password PW_i^* and compute $h(PW_i^*||ID_i)$, but he/she can not exploit A_i to verify the correctness of PW_i^* if he/she does not have the master secret key x. Furthermore, $\mathcal{A}$ can get the transmitted messages $\{ID_i, D_i^*, M_i, T_i\}$, $\{ID_i, V_i, M_S, T_S\}$, $\{ID_i, R_i, T_i^{new}\}$. Note that $\mathcal{A}$ can also not exploit D_i^* and R_i, which contain the information about the password PW_i, to verify the correctness of PW_i^*, since he/she does not know the values of $D_i = h(ID_i)^\alpha \bmod p$ and $Z_i' = h(ID_i)^{\alpha\beta} \bmod p$. This also makes off-line password guessing attacks impossible for a passive attacker, who can only obtain the exchanged messages. Therefore, our scheme is secure against off-line password guessing attacks, even the private data stored in the smart card are disclosed.

5.2 Resist Replay Attacks

Replay attacks mean that the adversary interferes with a protocol run by the insertion of a message, or part of a message, that has been sent previously in any protocol run. Our scheme exploits timestamp and secure one-way hash function to guard against replay attacks during the authentication phase. Suppose that the adversary has recorded the messages $\{ID_i, D_i', M_i, T_i\}$, $\{ID_i, V_i, M_S, T_S\}$ and $\{ID_i, R_i, T_i^{new}\}$, which would be used to replay. However, note that the timestamps T_i, T_S and T_i^{new} are contained in these messages, thus the replayed messages can be quickly detected by checking these timestamps. Furthermore, if the adversary replaces the timestamps T_S and T_i^{mew} with the current timestamps, the messages cannot pass the verification of the hash function. Therefore, our proposal is secure against replay attacks.

5.3 Resist Impersonation Attacks

If the adversary wants to launch the impersonation attacks, he/she has to generate a correct value R_i, which is difficult without the knowledge of D_i and Z_i. In order to get the values D_i and Z_i, the adversary must either hold the server's secret key x (i.e., the adversary has impersonated the server), or possess the private data A_i stored in U_i's smart card and the password PW_i simultaneously. It is obvious that such impersonation attack is trivial in the above two settings. Hence, our proposal is free from impersonation attacks.

5.4 Resist Parallel Attacks

To launch this kind of attack, the adversary $\mathcal{A}$ is required to create a valid authentication message by use of these intercepted authentication messages. However, we note that the authentication request message and the corresponding response message in our scheme are different in terms of structure and associated with timestamps. In addition, our scheme exploits hash values to ensure the

Table 2: Performance comparisons with previous related works

	User side	Server side	Total
Song [20]	T_s+4T_h	T_e+T_m+4T_h	T_e+2T_s+8T_h
Sood et al. [21]	3T_e+2T_m+3T_h	2T_e+T_m+3T_h	5T_e+3T_m+6T_h
Chen et al. [4]	2T_e+2T_m+4T_h	T_e+T_m+4T_h	3T_e+3T_m+8T_h
Li et al. [17]	4T_e+T_m+4T_h	3T_e+3T_h	7T_e+T_m+7T_h
Kumari and Khan [14]	2T_e+3T_m+2T_h+T_s	T_e+T_m+2T_h+3T_s	3T_e+4T_m+4T_h+4T_s
Jiang et al. [11]	3T_e+T_m+3T_h	2T_e+3T_h	5T_e+T_m+6T_h
Ours	2T_e+6T_h	2T_e+6T_h	4T_e+12T_h

authenticity. Thus, our scheme is secure against parallel attacks.

5.5 Perfect Forward Secrecy

Similar to Li et al.'s [17] scheme, by means of the intractability of the discrete logarithm problem, our scheme can also provide perfect forward secrecy. Specifically, in the case that both the user's password and the server's master secret key are disclosed, if the adversary wants to recover a previous session key $sk = h(ID_i||D_i'||V_i||Z_i)$ which is independent of the password and the master secret key, he/she must compute $Z_i = h(ID_i)^{\alpha\beta} \bmod p$. This means that the adversary has to compute α from $D_i' = h(ID_i)^{\alpha} \bmod p$ or β from $V_i = h(ID_i)^{\beta} \bmod p$. However, the discrete logarithm problem is widely believed to be difficult. Therefore, our proposal can ensure perfect forward secrecy.

5.6 Known-key Security

Known-key security means that the corrupted session keys have no effect on the security of those uncorrupted session keys. In our proposal, the shared session key is derived from $D_i = h(ID_i)^{\alpha} \bmod p$, $V_i = h(ID_i)^{\beta} \bmod p$ and $Z_i = h(ID_i)^{\alpha\beta} \bmod p$, where α and β are *randomly* chosen from Z_q^*. Thus, for another session of which session key is derived from $D_i' = h(ID_i)^{\alpha'} \bmod p$, $V_i' = h(ID_i)^{\beta'} \bmod p$ and $Z_i' = h(ID_i)^{\alpha'\beta'} \bmod p$, α' and β' are independent of α and β, which means that $h(ID_i||D_i||V_i||Z_i)$ is also independent of $h(ID_i||D_i'||V_i'||Z_i')$. Therefore, our scheme can provide known-key security.

5.7 Mutual Authentication and Key Agreement

To achieve mutual authentication, our scheme provides a mechanism that allows the user to verify the server in Step 4 of the authentication phase, and that allows the server to verify the user by Step 5 of the authentication phase. Furthermore, after they authenticated each other correctly, a shared session key, which is derived by the user and server as a function of information contributed by each of them such that no party can predetermine the resulting value, is established among the user and server, and then is used to provide a secure channel for subsequent communications.

5.8 Performance and Functionality Comparisons

In this section, we evaluate our scheme in terms of performance and functionality, and compare it with other related schemes as summarized in Table 5.1 and Table 5.7.

Typically, time complexity associated with these cryptographic operations, i.e., modular exponentiation operation, modular multiplication/inverse operation, hash operation and symmetric encryption/decryption, can be roughly expressed as $T_e \gg T_m \gg T_s \approx T_h$. Thus, the running time of all modular exponentiation operations, which are executed by the smart card and the remote server simultaneously, accounts for the major part of the running time of the entire authentication phase. In addition, computation ability of the smart card is usually limited. Therefore, to reduce the authentication delay, the smart card (i.e., user side) should execute as few modular exponentiation operations as possible, while the essential security properties of smart card based password authentication scheme are not compromised. From this perspective, Table 5.1 shows that our scheme is more efficient than these schemes [21], [4], [17], [14] and [11], since we have

$$\begin{aligned} 2T_e + 6T_h \text{ (Ours)} &< 2T_e + 2T_m + 4T_h \text{ ([4])} \\ &< 3T_e + T_m + 3T_h \text{ ([11])} \\ &< 2T_e + 3T_m + 2T_h + T_s \text{ ([14])} \\ &< 3T_e + 2T_m + 3T_h \text{ ([21])} \\ &< 4T_e + T_m + 4T_h \text{ ([17])}. \end{aligned}$$

Besides, in the aspect of the total computation cost, our scheme is also more efficient than schemes of Sood et al. [21], Li et al. [17] and Jiang et al. [11]. Although the remote server involved in our scheme needs once additional modular exponentiation operation when compared with Chen et al.'s [4] scheme and Kumari and Khan's [14] scheme respectively, we can consider the total computation cost of our scheme to be nearly the same with the two schemes, since the remote server possesses powerful

Table 3: Functionality comparisons with previous related works

	Song [20]	Sood [21]	Chen [4]	Li [17]	Kumari [14]	Jiang [11]	Ours
Off-line password guessing attacks	No	Yes	No	No	No	Yes	Yes
Impersonation attacks	No	Yes	No	Yes	Yes	Yes	Yes
Replay attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Parallel attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Forgery attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Man-in-the-middle attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Known-key security	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Perfect forward secrecy	No	No	No	Yes	No	No	Yes
Mutual authentication	Yes	No	Yea	Yes	Yes	Yes	Yes
Session key agreement	Yes	No	Yes	Yes	Yes	Yes	Yes
Quickly detect wrong password	No	No	No	Yes	Yes	No	No
Friendly password change	No	No	No	Yes	Yes	No	Yes
Perfect correctness	Yes	Yes	Yes	Yes	No	Yes	Yes

capacity of computation and storage, and then the time difference of once modular exponentiation operation may be ignored.

Smart card based password authentication should enjoy two-factor security, namely, even when either the private data stored in the smart card or the corresponding password are compromised (not the both), the scheme should be still secure. As illustrated in Table 3, when compared with the schemes of Song [20], Sood et al. [21], Chen et al. [4], Kumari and Khan [14], and Li et al. [17], only our scheme can resist password guessing attacks when the private data stored in the smart card is disclosed. Although schemes of Sood et al. [21] and Jiang et al. [11] are also free from off-line password guessing attacks, nevertheless they cannot provide perfect forward secrecy and friendly password change. We also note that when compared with other schemes, only the correctness of Kumari and Khan's scheme is not perfect, since a composite number is used as the modular number in their scheme.

The essential point is that Li et al.'s [17] scheme and Kumari and Khan's [14] scheme enjoy the functionality of quickly detecting wrong password through storing the verification information about the corresponding password into the smart card. However, as indicated by off-line password guessing attacks presented in Section 2.2 and Section 3.2, once the private information stored in the smart card has been disclosed, the adversary would exploit the verification information to check the validity of each candidate password, and launch off-line password guessing attacks. Thus, we suggest that the smart card should not contain any information that can be directly used to verify the validity of the corresponding password. Nevertheless, when the smart card can not detect the wrong password, which is the case in our scheme, inputting wrong password will produce one round additional communication between the user and the remote server, since only the remote server can check the correctness of the password.

6 Conclusions

In this study, we first examined the smart card based password authentication schemes proposed by Li et al. [17] and Kumari and Khan [14], respectively. Our cryptanalysis showed that the schemes would be vulnerable to off-line password guessing attacks once the private information stored in the smart card has been disclosed. In addition, we also pointed out that Kumari and Khan's [14] scheme cannot provide perfect forward secrecy and perfect correctness. Subsequently, to overcome the defects existing in the above two schemes, we proposed a new smart card based password authentication scheme. By presenting the concrete analysis of security and performance, we demonstrated that our proposal is not only free from various well-known attacks, but also is more efficient than other previous related works. Thus, our scheme is more feasible for practical applications.

Acknowledgements

This work was supported in part by the National Key Basic Research Program (973 program) under Grant 2012CB315905, in part by the National Nature Science Foundation of China under Grant 61379150, and in part by Foundation of Science and Technology on Information Assurance Laboratory under Grant KJ-14-004.

References

[1] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in Cryptology (Eurocrypt'00)*, pp. 139–155, Springer, 2000.

[2] C. C. Chang and C. S. Laih, "Remote password authentication with smart cards," *IEE Proceedings E: Computers and Digital Techniques*, vol. 138, no. 3, pp. 165-168, 1992.

[3] K. Chatterjee, A. De, and D. Gupta, "Mutual authentication protocol using hyperelliptic curve cryptosystem in constrained devices," *International Journal of Network Security*, vol. 15, no. 1, pp. 9–15, 2013.

[4] B. L. Chen, W. C. Kuo, and L. C. Wuu, "Robust smart-card-based remote user password authentication scheme," *International Journal of Communication Systems*, vol. 27, no. 2, pp. 377–389, 2014.

[5] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[6] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[7] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments," *International Journal of Network Security*, vol. 16, no. 4, pp. 318–321, 2014.

[8] D. Giri, T. Maitra, R. Amin, and P. D. Srivastava, "An efficient and robust rsa-based remote user authentication for telecare medical information systems," *Journal of Medical Systems*, vol. 39, no. 1, pp. 1–9, 2015.

[9] M. S. Hwang, S. K. Chong, and Te-Yu Chen, "Dos-resistant id-based password authentication scheme using smart cards," *Journal of Systems and Software*, vol. 83, no. 1, pp. 163–172, 2010.

[10] M. S. Hwang and Li H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[11] Qi Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card-based password authentication scheme," *International Journal of Communication Systems*, vol. 28, no. 2, pp. 383–393, 2015.

[12] W. S. Juang and J. L. Wu, "Two efficient two-factor authenticated key exchange protocols in public wireless lans," *Computers & Electrical Engineering*, vol. 35, no. 1, pp. 33–40, 2009.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology (CRYPTO'99)*, pp. 388–397, Springer, 1999.

[14] S. Kumari and M. K. Khan, "Cryptanalysis and improvement of a robust smart-card-based remote user password authentication scheme," *International Journal of Communication Systems*, vol. 27, no. 12, pp. 3939–3955, 2014.

[15] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[16] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol.," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[17] X. Li, J. Niu, M. K. Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1365–1371, 2013.

[18] I-En Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727–740, 2006.

[19] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[20] R. Song, "Advanced smart card based password authentication protocol," *Computer Standards & Interfaces*, vol. 32, no. 5, pp. 321–325, 2010.

[21] S. K. Sood, A. K. Sarje, and K. Singh, "An improvement of Xu et al.'s authentication scheme using smart cards," in *Proceedings of the Third Annual ACM Bangalore Conference*, p. 15, 2010.

[22] S. K. Sood, A. K. Sarje, and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 609–618, 2011.

[23] T. D. Wu, "The secure remote password protocol," in *Network & Distributed System Security*, vol. 98, pp. 97–111, 1998.

[24] J. Xu, W. T. Zhu, and D. G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

Jianghong Wei received the B.S. degree in Information Security from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2009. He is currently a PhD student in State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China. His research interests include applied cryptography and network security.

Wenfen Liu received the PhD degree in Mathematics from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 1995. She is a full professor in the State Key Laboratory of Mathematical Engineering and Advanced Computing, and severs as head of probability statistics. Her research interests include probability statistics, network communications and information security.

Xuexian Hu is a lecturer in the State Key Laboratory of Mathematical Engineering and Advanced Computing. He received the PhD degree in Information Security from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2009. His current research interests include applied cryptography, network security.

Cryptanalysis of a Compact Certificateless Aggregate Signature Scheme

Chih-Cheng Chen[1], Hanmin Chien[2], and Gwoboa Horng[1]
(Corresponding author: Gwoboa Horng)
Department of Computer Science and Engineering, National Chung Hsing University[1]
250 Kuo Kuang Road, Taichung, Taiwan 402 (R.O.C.)
Department of Digital Multimedia Design, China University of Technology[2]
No. 56, Sec. 3, Xinglong Rd., Wunshan District, Taipei City 116, Taiwan (R.O.C.)
(Email: gbhorng@cs.nchu.edu.tw)
(Received July 31, 2014; revised and accepted Sept. 24 & Oct. 6, 2014)

Abstract

In this paper, we cryptanalyze a recently proposed compact certificateless aggregate signature scheme (CCLAS) and show that it is in fact insecure against a Type-I attack. We also point out that the success of the attack is due to the inappropriate security model used to prove that CCLAS is secure.

Keywords: Aggregate signature, certificateless cryptography, cryptanalysis

1 Introduction

The most important contribution of modern cryptography is the invention of a way to create digital signatures. A digital signature is an electronic analogue of a written signature to be used by the recipient or a third party to identity of the signatory or to verify the integrity of the data. To deal with specific application scenarios, digital signature schemes have evolved into many different variants. Among them, aggregate signature schemes, which allow a collection of individual signatures to be compressed into a single short signature, are most useful for reducing the size of certificate verification chains and for reducing message size in secure routing protocols [2].

Certificateless public key cryptography (CL-PKC) [1] was proposed in 2003. Since then many cryptographic schemes have been proposed based on CL-PKC. CL-PKC solves the key escrow problem of the identity-based cryptography in a way that the full private key of a user is divided into two parts. The first part, called partial private key, is controlled by a key generator center (KGC). The second part is chosen by the user himself and remains secret to the KGC. Therefore, to discuss the security issues of CL-PKC, there are two types of attacks, depending on which part of the private key is compromised.

In 2014, Zhou et al. proposed a compact certificateless aggregate signature scheme (CCLAS) [15]. They also defined security models and showed that CCLAS is existentially unforgeable under adaptive chosen-message attacks and chosen-identity attacks. In this paper, we cryptanalyze CCLAS and show that it is in fact insecure against a Type-I attack.

The organization of this paper is as follows. Section 2 consists of some preliminaries, including a generic construction of a certificateless aggregate signature scheme and security models. Review of CCLAS is given in Section 3. The cryptanalysis of CCLAS is presented in Section 4. Finally, we give conclusions in Section 5.

2 Preliminaries

2.1 Generic Construction of a Certificateless Aggregate Signature Scheme

A certificateless aggregate signature (CLAS) scheme consists of three parts, initial setup **InitSetup**, signature generation and aggregation **CL-Sign**, and signature verification **CL-Verify**:

InitSetup. This part consists of the following algorithms:

- **Setup:** This algorithm, run by the KGC, takes a security parameter as input, then outputs master-key and system parameter params.
- **Partial-Private-Key-Extract:** This algorithm, run by the KGC, takes params, master-key and a user's identity ID as inputs, then outputs a partial-private-key D_{ID} to that user.
- **Set-Secret-Value:** This algorithm, run by a user, returns a secret value x.
- **Set-Private-Key:** This algorithm, run by a user, takes the user's partial-private-key D_{ID} and his

secret value as inputs, and outputs the full private key.

Set-Public-Key: This algorithm, run by a user, takes params and the user's full private key as inputs, and outputs a public key pk_{ID} for that user.

CL-Sign. This part consists of an individual signature generation algorithm and a signature aggregation algorithm.

IndiSign: The individual signature generation algorithm, run by a signer, takes params, a message m, and the user's full private key as inputs, and outputs σ as the signature for the message m.

SignAggr: The signature aggregation algorithm, run by any user or a third party, takes n individual signatures σ_i on messages m_i generated by users of identities ID_i where $i = 1, \cdots, n$, as input and returns an aggregate signature σ.

CL-Verify. This part consists of an individual signature verification algorithm and an aggregate signature verification algorithm.

IndiVeri: The individual signature verification algorithm, run by a verifier, takes params, a public key pk_{ID}, a message m, a user's identity ID, and a signature S as inputs. The verifier accepts signature S if and only if S is the signature of the message m for the public key pk_{ID} of the user with identity ID.

SignVeri: The aggregate signature verification algorithm, run by a verifier, takes an aggregate signatures σ_i on messages m_i generated by users of identities ID_i and public key pk_{ID_i} where $i = 1, \cdots, n$, as input and accepts the aggregate signature σ if it is valid.

2.2 Security Models

Traditionally, a digital signature scheme is secure if it is existentially unforgeable against adaptive chosen message attacks. The attack methods are centered on querying signatures for adaptive chosen messages. For a CLS scheme, the situation is more complicated since the attackers can do a lot more than merely querying signatures. For example, they can query for the partial private key of any user.

Therefore, when discussing the security issues of a certificateless signature scheme, there are two types of adversaries, A_I and A_{II} corresponding to two types of attack models Type-I and Type-II respectively. A Type-I attack model is used to model the case when an adversary A_I has compromised the user secret value or replace the user public key. However, he cannot compromise the master-key nor access the user partial key. Whereas a Type-II attack model is used to model the case when an adversary A_{II} (the malicious-but-passive KGC) has gained access to the master key but cannot perform public key replacement of the user being attacked. Since our attack is of Type-I, we describe the attack model in more detail. We refer the readers to [15] for the Type-II attack model.

The type-I attack model is defined in terms of a game played between a challenger C and the Type-I adversary A_I as follows.

Initialization. C runs Setup algorithm to generate the master key and public parameters to A_I.

Queries. A_I can adaptively perform the following polynomially bounded queries.

Partial-Private-Key query: $\mathcal{A}_1$ can query for the partial private key of any user with identity ID. $\mathcal{C}$ will return the partial private key D_{ID} to $\mathcal{A}_1$.

Public-Key query: $\mathcal{A}_1$ can query for the public key of any user with identity ID. $\mathcal{C}$ will return the public key pk_{ID} of that user.

Secret-Value query: $\mathcal{A}_1$ can query for the secret value of any user with identity ID. $\mathcal{C}$ will return the secret value x_{ID} of that user to $\mathcal{A}_1$.

Public-Key-Replacement: For any user with identity ID and public key pk, $\mathcal{A}$ can set a new public key pk', and then $\mathcal{C}$ replaces pk with pk'.

IndiSign query: $\mathcal{A}_1$ can query for the signature σ_i corresponding to a message m_i, a user with identity ID_i and public key pk_i. $\mathcal{C}$ will generate σ_i, and return it to $\mathcal{A}_1$.

SignAggr query: $\mathcal{A}_1$ can query aggregate signature for multiple signatures, $\mathcal{C}$ will return an aggregate signature σ by the **SignAggr** algorithm and return it to $\mathcal{A}_1$.

Forgery. $\mathcal{A}_1$ outputs an aggregate signature $\sigma^* = (R^*, S^*)$ of n individual signatures σ_i on messages m_i generated by users of identities ID_i^* where $i = 1, \cdots, n$. $\mathcal{A}_1$ wins the game if and only if the following conditions hold.

1) The forged aggregate signature σ^* is valid.
2) For each i, $1 \leq i \leq n$, at least one of the secret value or the partial private key of ID_i^* has not been queried.
3) σ^* has never been queried by the *IndiSign* and *SignAggr* oracles.

3 CCLAS

Most certificateless signature schemes are based on bilinear pairing [10, 11, 12, 13]. A bilinear map is a mapping $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, where $\mathbb{G}_1$ is an additive cyclic group of prime order q, and $\mathbb{G}_2$ is a multiplicative cyclic group of the same order q. We are interested in bilinear maps with the following properties:

1) Computable: given $P, Q \in \mathbb{G}_1$, there exists a polynomial time algorithm to compute $\hat{e}(P, Q) \in \mathbb{G}_2$.

2) Bilinear: for any $x, y \in \mathbb{Z}_q^*$, we have $\hat{e}(xP, yP) = \hat{e}(P, P)^{xy}$ for any $P \in \mathbb{G}_1$.

3) Non-degenerate: if P is a generator of $\mathbb{G}_1$, then $\hat{e}(P, P)$ is a generator of $\mathbb{G}_2$.

The CCLAS scheme consists of eight probabilistic-polynomial time algorithms, namely Setup, PartialKeyGen, UserKeyGen, IndiSign, IndiVeri, SignAggr, SignVeri and ExtAggr.

Setup: The KGC determines a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ where $\mathbb{G}_1$ is a cyclic additive group of prime order q with a generator P, $\mathbb{G}_2$ is a cyclic multiplicative group of the same order, and three hash functions $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*, H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$, and $H_3 : \{0,1\}^* \to \mathbb{G}_1$. Then it randomly chooses $s \in \mathbb{Z}_q^*$ as master-key, and then sets P_{pub} as the master-public-key where $P_{pub} = sP$. Finally, it publishes the system parameter params $= \langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, P, P_{pub}, H_1, H_2, H_3 \rangle$.

Partial-Private-Key-Extract: The KGC, based on params, master-key s and user's identity ID_i, computes and returns a partial-private-key $D_i = sQ_i$ to the user with identity ID_i where $Q_i = H_1(ID_i)$.

UserKeyGen: A user with identity ID_i, sets a random value $x_i \in \mathbb{Z}_q^*$ as his secret value and public key $P_i = x_i P$. The pair (D_i, x_i) is the user's full secret key SK_i.

IndiSign: To facilitate the aggregation of individual signatures, a random string ω, called state string, is chosen by the first signer. Each subsequent signer checks that it has not used the string ω before. To sign a message m_i using the full secret key (x_i, D_i), the signer with identity ID_i should perform the following steps:

1) Compute $P_\omega = H_2(\omega)$;
2) Pick a random number from r_i $\mathbb{Z}_q^*$ and compute $R_i = r_i P$;
3) Compute $h_i = H_3(\omega)$;
4) Compute $P_\omega = H_2(m_i, ID_i, \omega)$;
5) Compute $S_i = r_i P_\omega + D_i + x_i h_i$;
6) Output $\sigma_i =< R_i, S_i >$.

IndiVeri: To verify a signature $\sigma_i =< R_i, S_i >$ on the state string ω and the message m_i, the verifier should perform the following steps:

1) Compute $P_\omega = H_2(\omega)$;
2) Compute $h_i = H_3(m_i, ID_i, \omega)$;
3) Accept the signature if and only if $\hat{e}(P, S_i) = \hat{e}(R_i, P_\omega)\hat{e}(P_{pub}, Q_i)\hat{e}(P_i, h_i)$.

SignAggr: For $i = 1, \cdots, n$, to aggregate signatures $\sigma_i =< R_i, S_i >$ on state string ω and messages m_i signed by users with identities ID_i, one should perform the following:

1) Compute $S = \Sigma_{i=1}^n S_i$ and $R = \Sigma_{i=1}^n R_i$;
2) Output the aggregate signature $\sigma =< R, S >$.

SignVeri: To verify a signature $\sigma_i =< R_i, S_i >$ on the state string ω and the message m_i, the verifier should perform the following steps:

1) Compute $P_\omega = H_2(\omega)$;
2) Compute $Q_i = H_1(ID_i)$ and $h_i = H_3(m_i, ID_i, \omega)$ for $i = 1, \cdots, n$;
3) Accept the aggregate signature if and only if

$$\hat{e}(P, S) = \hat{e}(R, P_\omega)\hat{e}(P_{pub}, \Sigma_{i=1}^n Q_i)\hat{e}(\Pi_{i=1}^n P_i, h_i).$$

The aggregate signature is compact in a sense that its length is the same as that of an individual signatures. Furthermore, CCLAS scheme introduces another algorithm called ExtAggr which can be used to extract a valid individual signature. When an individual signature is be extracted from the aggregate signature the remaining part is also a valid aggregate signature.

4 Cryptanalysis of CCLAS

4.1 A Type I Attack

In this section we will show that is in fact forgeable under Type I attack. The attack goes as follows.

Suppose an adversary, say Alice, knows the secret value x_i of a user with identity ID_i through the *Public-Key-Replacement* query or the *Secret-Value query* query.

Then Alice can issue an IndiSign query to obtain a signature σ_i on a message m_i and a state string ω such that $\sigma_i = (R_i, S_i)$ where $R_i = r_i P$, $S_i = r_i P_\omega + D_i + x_i h_i$, and $h_i = H_3(m_i, ID_i, \omega)$. Note that Alice cannot compute the partial private key D_i directly. However, from σ_i, Alice can compute $T = r_i P_\omega + D_i = S_i - x_i h_i$ since x_i is known.

Now it is very simple for Alice to forge a signature $\sigma' = (R', S')$ for any message m' under the same state string ω. She only needs to set $R' = R$ and $S' = T + x_i h'$ where $h' = H_3(m', ID_i, \omega)$. Since $\hat{e}(P, S') = \hat{e}(P, T + x_i h') = \hat{e}(P, r_i P_\omega + D_i + x_i h') = \hat{e}(R', P_\omega)\hat{e}(P_{pub}, Q_i)\hat{e}(P_i, h')$, $\sigma' = (R', S')$ is indeed a valid signature for message m'.

Hence, given an aggregate signature σ which includes σ_i, Alice can use ExtAggr algorithm to extract σ_i from σ followed by adding σ' to it to obtain a forged aggregate signature σ^*.

4.2 Discussion

The linear equation used to construct the second part of a signature in CCLAS is similar to that of the CLS short signature scheme proposed in [5] and attacked by

Shim in [7]. Therefore, the same attack can also be used to attack CCLAS. In [6], three kinds of adversaries are introduced, namely normal, strong, and super. They are distinguished by their attack power. A strong Type I adversary can make a strong-sign query which takes as input (ID, m, sv), where ID denotes the identity that has been created, m denotes the message to be signed and sv is the secret value. In the above attack, Alice is a strong Type-I adversary. Therefore, CCLAS is insecure against strong Type-I attacks.

Over the years, many provably secure certificateless signature schemes have been proposed under certain security models. However, they are shown to be insecure [3, 4, 8, 9, 14]. Therefore, the security models for certificateless signature schemes are quite subtle. Based on the security models of CCLAS, to existentially forge a signature is equivalent to derive the partial private key of a user. However, as mention in the attack, our attack cannot derive the partial key but instead forge a signature based on an existent state string. Therefore, the security model used to prove that CCLAS is secure is inappropriate.

5 Conclusions

The integration of certificateless public key cryptography and aggregate signature has many potential applications. However, for a certificateless aggregate signature scheme to be used in application environments, we must make sure that it is secure against attacks. Therefore cryptanalysis plays a vital role for a cryptographic protocol to be successfully applied in the real world. In this paper, we have analyzed CCLAS scheme and showed that it is not secure against strong Type-I attacks.

Acknowledgement

This work was partially supported by the National Science Council of the Republic of China under contract No. NSC102-2221-E-005-051.

References

[1] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," *Proceedings of Advances in Cryptography (ASIACRYPT'03)*, LNCS 2894, pp. 452–473, Springer-Verlag, 2003.

[2] D. Boneh, D. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," *Proceedings of Advances in Cryptography (EUROCRYPT'03)*, LNCS 2656, pp. 416–432, Springer-Verlag, 2003.

[3] D. He, M. Khan, and S. Wu, "On the Security of a RSA-based Certificateless Signature Scheme," *International Journal of Network Security*, vol. 16, pp. 78–80, 2014.

[4] D. He, M. Tian, and J. Chen, "Insecurity of an efficient certificateless aggregate signature with constant pairing computations." *Information Sciences*, vol. 268, pp. 458–462, 2014.

[5] X. Huang, Yi Mu, W. Susilo, D.S. Wong, and W. Wu, "Certificateless signature revisited," in *Information Security and Privacy*, LNCS 4586, pp. 308–322, Springer-Verlag, 2007.

[6] X. Huang, Y. Mu, W. Susilo, D. Wong, and W. Wu, "Certificateless signatures: new schemes and security models," *The Computer Journal*, vol. 55, pp. 457–474, 2012.

[7] K. Shim, "Breaking the short certificateless signature scheme," *Information Sciences*, vol. 179, pp. 303–306, 2009.

[8] K. Shim, "On the security of a certificateless aggregate signature scheme," *Communications Letters*, vol. 15, pp. 1136–1138, 2011.

[9] H. Tu, D. He, and B. Huang, "Reattack of a certificateless aggregate signature scheme with constant pairing computations," *The Scientific World Journal*, Article ID 343715, 10 pages, 2014.

[10] C. Wang, D. Long, and Y. Tang, "An Efficient Certificateless Signature from Pairings," *International Journal of Network Security*, vol. 8, pp. 96–100, 2009.

[11] H. Xiong, Z. Guan, Z. Chen, F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Information Science*, vol. 219, pp. 225–235, 2013.

[12] H. Xiong, Z. Qin, and F. Li, "A certificateless proxy ring signature scheme with provable security," *International Journal of Network Security*, vol. 12, pp. 92–106, 2011.

[13] L. Zhang and F. Zhang, "A new certificateless aggregate signature scheme," *Computer Communications*, vol. 32, pp. 1079–1085, 2009.

[14] M. Zhang, J. Yao, C. Wang, and T. Takagi, "Public key replacement and universal forgery of a SCLS scheme," *International Journal of Network Security*, vol. 15, pp. 133–138, 2013.

[15] M. Zhou, M. Zhang, C. Wang, and B. Yang, "CCLAS: A practical and compact certificateless aggregate signature with share extraction," *International Journal of Network Security*, vol. 16, pp. 174–181, 2014.

Chih-Cheng Chen received the M.S. degree in graduate school of computer science and information technology from National Taichung Institute of Technology, Taiwan. He is currently pursuing the Ph.D. degree in computer science and engineering from National Chung Hsing University. His research interests include data hiding, secret sharing, watermarking and image processing.

Han-min Chien was born in Taipei, Taiwan, in 1971. He received the Ph.D. degree in electronics & electrical engineering from the Queens University of Belfast, N. Ireland, U.K., in 2005. In 2006, he joined the Department of Computer Science & Information Engineering,

China University of Technology, Taiwan, as an Assistant Professor, and transferred to the Department of Digital Multimedia Design in 2011. His current research interests include image processing, virtual reality, medical instruments, and Ergonomics. He was the recipient of Young Investigator Applicants Encouragement Award from the commit of 6th Asian-Pacific Conference on Medical and Biological Engineering, Japan, 2005, the SPUR-VEC Research Funding of the Queens University of Belfast & Parliament of Northern Ireland, from 2001 to 2005.

Gwoboa Horng received the B.S. degree in Electrical Engineering from National Taiwan University in 1981 and the M.S. and Ph.D. degrees from University of Southern California in 1987 and 1992, respectively, all in Computer Science. Since 1992, he has been on the faculty of the Department of Computer Science and Engineering at National Chung-Hsing University, Taichung, Taiwan, R.O.C. His current research interests include artificial intelligence, cryptography, and information security.

Weaknesses of Password Authentication Scheme Based on Geometric Hashing

Martin Stanek
Department of Computer Science, Comenius University
Mlynská Dolina, 842 48 Bratislava, Slovak
(Email: stanek@dcs.fmph.uniba.sk)
(Received May 9, 2014; revised and accepted Jan. 16 & May 5, 2015)

Abstract

We show that a recently proposed password authentication scheme based on geometric hashing has several security weaknesses, and that the use of this scheme should be avoided in practice.

Keywords: Authentication, geometric hashing, password

1 Introduction

Password authentication schemes are an important class of cryptographic protocols. They provide a mechanism that allows a user to authenticate to a server by using his/her password. Various protocols were proposed, e.g. [6, 9, 10, 12, 13, 14, 15], and many attacks on such schemes appeared, e.g. [2, 4, 5, 7, 8, 11, 13]. A survey on password authentication schemes can be found in [16].

Recently, a new password authentication scheme was proposed in [17]. The scheme is based on geometric hashing. The authors claim the security of the scheme, namely a resilience against replay attack, off-line guessing, stolen-verifier, denial of service, and man-in-the-middle attacks.

For brevity, we will call the scheme from [17] "the geometric scheme". We show several weaknesses of the geometric scheme:

- Contrary to the claim stated in [17] the geometric scheme is not resistant against stolen-verifier attack. We show how an attacker can authenticate using user's stolen verifier. Moreover the verifier can also be used to recover user's identity and password.
- The performance of the geometric scheme can be easily degraded by a malicious user. First, the attacker can cause a significant grow of the internal data structure (a hash table) used for storing users' verifiers. Second, the attacker is able to cause a large number of collisions in the hash table, thus increasing the complexity of lookups performed during authentication.
- The scheme allows a substantial reduction of potential identity/password pairs.

The paper is organized as follows. We briefly introduce the geometric scheme in Section 2. The weaknesses are presented in Section 3.

2 The Geometric Scheme

We present the geometric scheme in sufficient detail to make our paper self-contained and to allow the reader to understand the findings.

2.1 Preliminaries

The geometric scheme is based on problem of geometric hashing [3]; for more recent work on bucketing problems, see [1].

Let S be the set of points in two-dimensional space $\mathbb{R}^2$: $S = \{(x_i, y_i)\}_{i=1}^n$. Let $\theta \in \langle 0, \pi)$ be an angle of projection – it uniquely determines the line going through the origin point $(0, 0)$ such that the angle between the line and x-axis is θ. A projection of point $s = (x, y)$ at angle θ is defined as a value $|s|_\theta = x \cos\theta + y \sin\theta$. For given S and θ the following notions are defined:

- The span of the projection:

$$\mathrm{span}_\theta(S) = \max\{||s_i|_\theta - |s_j|_\theta| \,;\; s_i, s_j \in S\}.$$

- The resolution of the projection:

$$\mathrm{res}_\theta(S) = \min\{||s_i|_\theta - |s_j|_\theta| \,;\; s_i, s_j \in S \text{ and } i \neq j\}.$$

- The length of the projection:

$$\mathrm{len}_\theta(S) = \mathrm{span}_\theta(S) / \mathrm{res}_\theta(S).$$

In order to have the smallest projection value starting at zero, the value C is computed as $C = \min\{|s|_\theta;\ s \in S\}$. Then an adjusted projection is a shifted version of the projection: $P_\theta(s) = |s|_\theta - C$.

2.2 Initial Configuration

User's identity id and password pw represent a point $(\mathsf{id}, \mathsf{pw}) \in \mathbb{R}^2$. The server computes an angle θ^* that minimizes the length of the projection for initial set of n users S_U, e.g. using an $O(n^2 \log n)$ algorithm from [3]. The idea is to create even-sized buckets and place each $(\mathsf{id}, \mathsf{pw})$ pair into a corresponding bucket according its adjusted projection. Let C^* be the value calculated for shifting the projection, and let res_{θ^*} be the resolution of the projection computed for S_U and θ^*.

The server builds a hash table with entries $(\mathrm{idx}_{\theta^*}(\mathsf{id}, \mathsf{pw}), P_{\theta^*}(\mathsf{id}, \mathsf{pw}))$, where the index value $\mathrm{idx}_{\theta^*}(\mathsf{id}, \mathsf{pw}) = \lfloor P_{\theta^*}(\mathsf{id}, \mathsf{pw}) / \mathrm{res}_{\theta^*} \rfloor$ serves as a key for the hash table. Possible collision are treated in a standard way by linked list of colliding values.

The length of the projection is minimized to make the size of the hash table reasonable small. The use of adjusted projection ensures that the hash table index starts at zero. The server publishes the values θ^*, C^* and res^*_θ computed for the initial set of users, and stores the hash table. Note that the server stores neither passwords, nor user identities in clear.

2.3 Authentication

Authentication involves two parties – client (user) and server. The protocol consists of a single message prepared by the client and sent to the server, and a verification performed by the server.

The client knows his/her own identity id, password pw, and public values published by the server – θ^*, C^* and res^*_θ. Let H be a cryptographic hash function, and let t_c be a fresh time stamp. The client computes values $m_1 = P_{\theta^*}(\mathsf{id}, \mathsf{pw})$, $m_2 = H(\mathsf{pw} \oplus \mathsf{id})$, $M_1 = \mathrm{idx}_{\theta^*}(\mathsf{id}, \mathsf{pw})$, $M_2 = H(m_1 \oplus t_c)$, $M_3 = \mathsf{pw} \oplus m_1$, and $M_4 = P_{\theta^*}(m_2, \mathsf{pw})$. The client sends to the server the 5-tuple: M_1, M_2, M_3, M_4, t_c.

The server performs the following verification steps after receiving the values M_1, M_2, M_3, M_4, t_c:

1) If time stamp t_c is not recent enough or M_1 if out range of the hash table, the server rejects the authentication.

2) Index M_1 is used to get all $P_{\theta^*}(\mathsf{id}', \mathsf{pw}')$ values from the hash table that share this index. The sever searches through these values for $m'_1 = P_{\theta^*}(\mathsf{id}', \mathsf{pw}')$ such that $H(m'_1 \oplus t_c) = M_2$. If the m'_1 is not found, the server rejects.

3) The server extracts $\mathsf{pw}' = M_3 \oplus m'_1$ and $\mathsf{id}' = (m'_1 - \mathsf{pw} \cdot \sin\theta^* + C)/\cos\theta^*$. Finally, the server computes $m'_2 = H(\mathsf{pw}' \oplus \mathsf{id}')$ and verifies that $P_{\theta^*}(m'_2, \mathsf{pw}') = M_4$. The authentication is accepted only after successful verification.

3 Attacks and Weaknesses

We discuss several attacks and weaknesses of the proposed geometric hashing in this section.

Stolen-verifier attack - Authentication.

The stolen-verifier attack covers a situation when the attacker has stolen a user's verifier stored in the server. The attacker then tries to authenticate as the user. The scheme should be resistant to such attack. The verifier in the geometric scheme is the value $P_{\theta^*}(\mathsf{id}, \mathsf{pw})$. Contrary to the claim stated in [17], the geometric scheme is not resistant to the stolen-verifier attack.

First, observe that M_1, M_3 and M_4 messages are constant in each authentication for given $(\mathsf{id}, \mathsf{pw})$ pair. The only part of the authentication that depends on the time stamp t_c is $M_2 = H(m_1 \oplus t_c) = H(P_{\theta^*}(\mathsf{id}, \mathsf{pw}) \oplus t_c)$. Thus, the attacker can forge the authentication of the user:

1) Generate a fresh time stamp t_c.
2) Compute $M_2 = H(P_{\theta^*}(\mathsf{id}, \mathsf{pw}) \oplus t_c)$ using the stolen-verifier $P_{\theta^*}(\mathsf{id}, \mathsf{pw})$.
3) Send M_1, M_2, M_3, M_4, t_c, where M_1, M_3 and M_4 are eavesdropped messages from some previous run of the authentication.

Stolen-verifier attack - Identity and password recovery.

Even more damaging is the observation that the verifier $P_{\theta^*}(\mathsf{id}, \mathsf{pw})$ (i.e. m_1) is used for password encryption. Therefore, a possession of the verifier and an eavesdropped authentication messages allow the attacker to recover the password $\mathsf{pw} = M_3 \oplus m_1$. Having pw, the identity id can be computed as well.

Hash table overflow and underflow.

Since the angle θ^* is not adjusted when users change their passwords or new users are added, the angle and the corresponding resolution can become suboptimal. The parameters θ^*, C^* and res^*_θ are public. Therefore a malicious user (attacker) can cause:

1) An overflow of hash table. The authors of the geometric scheme acknowledge the possibility that the hash table can stretch. Seemingly, they do not recognize the possibility to cause an extreme increase of the hash table size. It is easy to maximize the index of $(\mathsf{id}, \mathsf{pw})$ pair by maximizing the value of formula $\mathsf{id} \cdot \cos\theta^* + \mathsf{pw} \cdot \sin\theta^*$.
2) An underflow of hash table. Similarly to the overflow problem, minimizing $\mathsf{id} \cdot \cos\theta^* + \mathsf{pw} \cdot \sin\theta^*$ cause, possibly large, negative index value. The hash table then must by adjusted for these indices and enlarged correspondingly.

Collisions in the hash table.

The values θ^*, C^* and res^*_θ are public. Hence anybody can compute index $\mathrm{idx}_{\theta^*}(\mathsf{id}, \mathsf{pw})$ for any pair

$(\mathsf{id}, \mathsf{pw})$. Moreover, for given id, one can easily compute various pw such that $\mathrm{idx}_{\theta^*}(\mathsf{id}, \mathsf{pw})$ is some predetermined value. Thus, the attacker (or a colluding set of users) can register a large number of users (or change their passwords) such that the idx_{θ^*} values collide. This causes long chains to store P_{θ^*} values and substantially degrade the performance of the hash table.

In addition, the index for the user is send as a part of his/her authentication in M_1 message. This allows to target any particular user and cause performance degradation just for this index.

Reducing the identity/password space.
The message M_1 contains the index value for the user. The attacker can use M_1 for reducing the space of possible identity/password pairs. If $\mathrm{idx}_{\theta^*}(\mathsf{id}', \mathsf{pw}') \neq M_1$ the attacker can conclude that $(\mathsf{id}', \mathsf{pw}')$ is not valid for the user. When the attacker learns user's id by some other means, it allows to test the password. Assuming uniform distribution of identities/passwords the test reduces the possible space by factor n, where n denotes the number of buckets in the hash table, i.e. the maximal index. Usually n increases with increasing the user-base. Hence, the larger the user-base, the more selective test. Moreover, combining with the weakness of hash table overflow, the attacker can choose the factor of the reduction.

Representation of values over real numbers.
The paper [17] lacks any detail how user's identity and password, commonly given as strings of printable characters, are mapped into domain of real numbers to perform geometric hashing. Moreover, some rounding or truncating should be applied for operations like recovering user's id in the verification procedure. The precise formula will depend on the mapping.

4 Conclusion

We showed the insecurity of the password authentication scheme based on geometric hashing proposed in [17]. The attacks and weaknesses presented in the this paper suggest that the use of the scheme should be avoided in practice. Moreover, because of numerous issues it is probably not worth to fix the scheme – it would be a completely new authentication scheme.

Acknowledgment

The author acknowledges support by VEGA 1/0259/13.

References

[1] P. K. Agarwal, B. K. Bhattacharya, and S. Sen, "Output-sensitive algorithms for uniform partitions of points," *Proceedings of 10th International Symposium on ISAAC*, LNCS 1741, pp. 403–414, Springer, 1999.

[2] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," *IEICE Transactions on Communications*, vol. E85-B, no. 11, pp. 2519–2521, 2002.

[3] D. Comer and M. J. O'Donnell, "Geometric problems with application to hashing," *SIAM Journal on Computing*, vol. 11, no. 2, pp. 217–226, 1982.

[4] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's Improvement on a Password Authentication Scheme for Multi-server Environments," *International Journal of Network Security*, vol. 16, no. 4, pp. 318–321, 2014.

[5] D. He, J. Chen, and J. Hu, "Weaknesses of a remote user password authentication scheme using smart card," *International Journal of Network Security*, vol. 13, no. 1, pp. 58–60, 2011.

[6] M. S. Hwang, C. C. Lee, and Y. L. Tang, "A simple remote user authentication scheme," *Mathematical and Computer Modeling*, vol. 36, no. 1-2, pp. 103–107, 2002.

[7] M. Kim and Ç. K. Koç, "A Simple Attack on a Recently Introduced Hash-Based Strong-Password Authentication Scheme," *International Journal of Network Security*, vol. 1, no. 2, pp. 77–80, 2005.

[8] W. C. Ku, C. M. Chen, and H. L. Lee, "Weaknesses of Lee-Li-Hwangs hash-based password authentication scheme," *ACM Operating Systems Review*, vol. 37, no. 4, pp. 19–25, 2003.

[9] W. C. Ku, "A hash-based strong password authentication scheme without using smart cards," *ACM Operating System Review*, vol. 38, no. 1, pp. 29–34, 2004.

[10] C. C. Lee, L. H. Li, and M. S. Hwang, *A remote user authentication scheme using hash functions*, *ACM Operating System Review*, vol. 36, no. 4, pp. 23–29, 2002.

[11] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[12] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727–740, 2006.

[13] C. Lin, H. Sun, and T. Hwang, "Attacks and solutions on strong-password authentication," *IEICE Transactions on Communications*, vol. E84-B, no. 9, pp. 2622–2627, 2001.

[14] M. Peyravian and N. Zunic, "Methods for protecting password transmission," *Computers and Security*, vol. 19, no. 5, pp. 466–469, 2000.

[15] M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol (SAS)," *IEICE Transactions on Communications*, vol. E83-B, no. 6, pp. 1363–1365, 2000.
[16] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password Authentication Schemes: Current Status and Key Issues," *International Journal of Network Security*, vol. 3, no. 2, pp. 101–115, 2006.
[17] X. Zhuang, C. C. Chang, Z. H. Wang, and Y. Zhu, "A Simple Password Authentication Scheme Based on Geometric Hashing Function," *International Journal of Network Security*, vol. 16, no. 4, pp. 271–277, 2014.

Martin Stanek is an Associate Professor in the Department of Computer Science, Comenius University. He received his PhD. in computer science from Comenius University. His research interests include cryptography and information security.

Guide for Authors
International Journal of Network Security

IJNS will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of network security. Topics will include, but not be limited to, the following: Biometric Security, Communications and Networks Security, Cryptography, Database Security, Electronic Commerce Security, Multimedia Security, System Security, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijns.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

The title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:
For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

Subscription Information

Individual subscriptions to IJNS are available at the annual rate of US$ 200.00 or NT 7,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijns.jalaxy.com.tw or Email to ijns.publishing@gmail.com.