GUI based Approach for Data Encryption and Decryption on MATLAB Platform

Shweta Joshi
M.Tech Scholar
Dept. of ECE
Govt. Engineering College, Ajmer

Rekha Mehra, PhD
Associate Professor
Dept. of ECE
Govt. Engineering College, Ajmer
Member IEEE, LM ISTE

ABSTRACT
In the era of digital technology, image (data) security has been a very vital concept for its practical applications. With the use of 'Steganography' a technique of hiding a special(secret) data (message) in any cover object while communicating between the transmitter and receiver, security of secret data always has been a critical factor since fast times. In this message work, a Hash – LSB based embedding of the encrypted text. RSA encryption is performed to provide further enhanced security data. Decryption of image steganography is done using RSA decryption algorithm, which helps to commute another cycle of security process implementation. Image steganography has been implemented using an Hash-LSB encoding and decoding RSA message or file encryption and decryption and chaotic used an image encryption decryption algorithm.

General Terms
Reversible data hiding methods, Encoding and Decoding.

Keywords
Cryptography, Hash LSB encoding, RSA Encryption, RSA Decryption, Steganography.

1. INTRODUCTION
A system for lossless and reversible data hiding in encrypted images proposes a lossless, a reversible, and a combined data hiding schemes. To add one more level of security the scheme is applied for cipher text images. The cipher text is then encrypted by public key cryptosystems. The first scheme is lossless scheme. In this scheme, the cipher text pixels are replaced with new values. The replacement of pixel is done to embed the additional data into several LSB-planes of cipher text pixels by multi-layer wet paper coding. Then, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. The second scheme is reversible scheme. In this scheme, a preprocessing is employed to shrink the image histogram before image encryption, so that the modification on encrypted images for data embedding will not cause any pixel oversaturation in plaintext domain. From the decrypted image we can then find the embedded data and the original image in spite of slight distortion. The third and final scheme is the combined scheme i.e. combination of lossless and reversible scheme. With the combined technique, there are two possible outcomes. A receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption. In literature survey, it was noticed that some of the previous system do not differentiate between the two system I.e. reversible and lossless system. It is also noticed that if data-embedding capacity increases then the image quality decreases. The existing system tries to overcome all these flaws. There are various techniques available for data protection. Out of which encryption and data hiding are two effective means of data protection. The encryption techniques convert plaintext content into unreadable cipher text. The data hiding techniques embed additional data into cover media. The data can be embedded by introducing slight modifications. Data hiding may be performed with a lossless or reversible manner. In the proposed system, the terms "lossless" and "reversible" will be distinguished. In the previous references, these two terms have the same meaning. If the display of cover signals, containing embedded data is same as that of original cover even though the cover data have been modified for data embedding, in thesis we can say that the data hiding method is lossless. If the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been introduced in data embedding procedure, in this case we can say that the data-hiding scheme is reversible

2. IMPORTANCE AND NEED OF SECURE DATA ENCRYPTON AND DECRYPTION TECHNOLOGY
With advanced interactive media, circulation over World Wide Web Intellectual Property Right (IPR) is more debilitated than any time in recent memory because of the likelihood of boundless duplicating. Therefore, by utilizing some encryption systems this effectively replicating of the information should be limited. However, encryption does not give general insurance. Once the encoded information are unscrambled, they can be unreservedly conveyed or controlled. This issue can be fathomed by concealing some possession information into the interactive media information which can be extricated later to demonstrate the proprietorship. This procedure for the most part utilized as a part of bank money where a watermark is inserted which is utilized to check the creativity of the note.

A similar idea called watermarking might be utilized as a part of interactive media advanced substance for checking the legitimacy of the first substance.

An extensive volume of information transmitted over web is private and classified. Encryption is the coveted to transmit the data effectively and securely. The security gave by steganography is more than the security gave by cryptography alone. These two ideas are utilized as a part of the framework alongside validation, which gives the approval to the client to utilize the framework with every single right usefulness.

Cryptography can ensure the information while transmission however when it is unscrambled, there is no more assurance left. To give more security and wellbeing data concealing strategies are utilized now a days and steganography is one of them, which enables the client to store a lot of information behind any picture. Cryptography goes for making information

incoherent for the third individual who is not approved to get the data. Steganography manages concealing the information from the third individual behind any picture. As the development of data innovation, more information accessible on the web so it confronts bunches of security issues. These security issues understood by numerous procedures, for example, cryptography, steganography, reversible information concealing and so forth the RDH method builds up on steganography and security. While exchanging the message from sender to recipient, exist the gatecrasher that takes the data between of them. This kind of transmission limited by a few applications, for example, military symbolism, law criminological and so on.

The water marking is most good strategy for giving the security to the framework. With the utilization of this system, we would watermark be able to the data and shield the data from gatecrashers. We can discover where the picture or information adjusted or played out the progressions by gatecrasher or outsider so we can without much of a stretch distinguish the alteration by utilizing the watermarking idea.

3. CONCEPT OF DATA HIDING

Data Hiding is a system used to install a succession of bits in a host picture with little visual weakening and the way to concentrate it subsequently. Most information concealing systems change and thusly contort the host motion with a specific end goal to embed the extra data. This twisting is normally little however irreversible. Reversible information hidings embed data bits by adjusting the host flag, yet empower the correct (lossless) reclamation of the first host motion in the wake of extricating the inserted data. Now and then, expressions like mutilation free, invertible, lossless or erasable watermarking are utilized as equivalent words for reversible watermarking.

In many applications, the little contortion because of the information inserting is normally middle of the road. Nonetheless, the likelihood of recouping the correct unique picture is an attractive property in many fields, as lawful, therapeutic and military imaging. Give us a chance to consider that delicate archives (like bank checks) are filtered, secured with a confirmation conspire in light of a reversible information covering up, and sent through the Internet. Much of the time, the watermarked records will be adequate to recognize unambiguously the substance of the archives. Nevertheless, if any vulnerability emerges, the likelihood of recouping the first unmarked archive is extremely intriguing.

To the best of our insight, none of the accessible reversible information hidings is satisfactory for watermarking double pictures. We propose in this thesis a reversible information stowing away for parallel pictures called RDTC (Reversible Data covering up by Template positioning with symmetrical Central pixels). Pictures watermarked by the proposed strategy have amazing visual quality, in light of the fact that lone low-perceivability pixels are flipped. RDTC is sufficient for watermarking most sorts of double pictures, as examined or PC produced writings, diagrams and design; toon like pictures; and bunched spot halftones. RDTC can even be utilized to watermark scattered spot halftones (like pictures produced by blunder dissemination), however the subsequent watermarked picture may not present high visual quality, in light of the fact that the idea "low-perceivability pixel" does not have any significant bearing to this sort of picture.

At that point, we utilize RDTC to make a reversible open key verification watermarking for parallel pictures named RATC (Reversible Authentication Watermarking by Template positioning with symmetrical Central pixels). Any reversible information concealing method can be effectively changed over into a reversible confirmation watermarking, gave that an enough number of bits can be installed into the host picture. To do it, the advanced mark (DS) of the first picture is processed utilizing the private key. At that point, the DS is implanted into the picture, alongside the data to permit recuperating the first picture. The confirmation calculation extricates the DS, reestablishes the first cover-picture and checks whether the DS coordinates the recouped picture.

The benefits of reversibly installing the DS over annexing it are self-evident. To start with, there is no additional data (other than the picture itself) to be put away or transmitted. Second, any lossless configuration transformation, for example, changing the organization from TGA to BMP, does not eradicate the inserted data. Third, the nearness of a reversible validation is less discernible than the apparently attached DS.

RATC has numerous potential pragmatic uses, in light of the fact that the vast majority of examined reports are double, and they should be carefully marked to guarantee their credibility and honesty. Utilizing RATC, the recipient of an Internet FAX record can make sure of the character of the sender of the archive and that the report was not messed with. It is likewise conceivable to distribute a database of paired records in the Internet (for instance, patent reports) and the peruse can make certain that the archives are legitimate and that they were not noxiously altered.

The watermarking concept make the system more secure by encryption the watermark image. ***Existing Techniques:*** Reversible Data Hiding - Data hiding is the way of hiding information into a cover media. It requires two set of data that are embedded data and set of cover media data. In some case cover media distorted due to perform hiding operation but this type of changes are not acceptable by some applications such as medical imagery, military imagery and law-forensic etc. so that a novel method become more popular among the researches i.e. known as Reversible data hiding (RDH).It is the technique that perform lossless embedding operation and recover the origin after the extraction. If cover medium distorted permanently when hidden message have been removed. Original Image encrypted into image encryption by using the encryption-key algorithm at the side of image owner. After that in the data hider module we can embed some additional data with the use of data-hiding key, finally gets the encrypted image that containing additional data and that image require to decryption at the receiver side. Reversible data hiding techniques can be generally classified into two frameworks: (1) Vacate room after encryption and (2) Reserve room before encryption

In the first framework, vacate room after encryption (VRAE), a content owner first encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data-hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key. In the second framework, reserve room before encryption (RRBE), the content owner first reserve enough space on original image and then converts the image into its encrypted version with the encryption key. Now, the data embed ding process in

encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance customary idea is followed in which the redundant image content is losslessly compressed and then encrypts it with respect to protecting privacy.

4. DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography is the exploration of utilizing arithmetic to encode furthermore, unscramble information and Steganography is the workmanship and investigation of concealing correspondence; a stenographic framework hence inserts concealed substance in unremarkable cover media so as not to stir an eavesdropper's doubt. A novel plan for the implanting information in pictures is CrypSteg in this technique joined cryptography and Steganography prepare in one calculation. To start with, we scramble the information and afterward insert with picture with new Steganography calculation. The technique is exceptionally proficient particularly when connected to those pictures whose pixels are scattered homogeneously and for little information. The given picture is divided into four level squares, and the information will be inserted into chosen the four slanting sub blocks values rely on key. This calculation just requires less strides and it can install information proficiently without disposing of picture. Installing 4 bits data in a 4*4 pixel square need to change less pixels by and large. Besides, the nature of the delivered stego-pictures is better than that of different techniques. The nature of stego-picture is extraordinarily enhanced when this calculation is utilized. Cryptography and Steganography are notable and comprehensively utilized methods that utilization data keeping in mind the end goal to figure or cover their reality individually. Steganography is the workmanship and art of imparting in an approach, which conceals the presence of the correspondence [2]. The Steganography covers up the message so it cannot be seen; Cryptography scramble a message so it cannot be comprehended [3]. Despite the fact that both strategies give security, a review is made to join both cryptography and Steganography techniques into one framework for enhanced covering and security.

Cryptography frameworks can be comprehensively ordered into symmetric-key frameworks that utilization a solitary key that both the sender and the beneficiary have, and open key frameworks that utilization two keys, an open key known to everybody and a private key that lone the beneficiary of messages employments. In Cryptography, a figure message for example, may incite doubt on the some portion of the beneficiary while an undetectable message made with stenographic techniques will not. Actually, steganography can be valuable when the utilization of cryptography is illicit: where cryptography and solid encryption are restricted, steganography can avoid such strategies to pass message secretly. Nevertheless, steganography and cryptography vary in the way they are judged: steganography falls flat when the "foe" can get to the substance of the figure message, while cryptography fizzles at the point when the "adversary" identifies that there is a mystery message exhibit in the stenographic medium. The branch of knowledge that review systems for translating figure messages and distinguishing conceal messages are called cryptanalysis also, steganalysis [4].

The past means the arrangement of techniques or getting the importance of encoded data, while the last is the specialty of uncover the undercover messages. The point of this thesis is to portray a technique for coordinating together cryptography and steganography through a few media, for example, picture, sound, video, and so on. In this thesis, we propose another calculation for shading full picture. As indicated by the strategy, a given picture is parceled into 4*4 squares, and afterward takes just slantingly hinder for information covering up in view of a few standards. Different information concealing procedures, for case, LSB (Least Significant Bit) approach, have been created as of late, the greater part of them are for shading and dark scale pictures and our technique is additionally for shading pictures. In spite of the fact that Steganography is relevant to all information questions that contain repetition, in this article, we consider shading pictures just (in spite of the fact that the strategies and techniques for steganography what is more, steganalysis that we introduce here apply to other information organizes also).

Individuals regularly transmit advanced pictures over email and other Internet correspondence, and shading picture is a standout amongst the most widely recognized path for sending mystery messages. Also, stenographic frameworks for the shading picture appear additional fascinating in light of the fact that the frameworks work in a change space and are not influenced by visual assaults [15].Visual assault implies gatecrashers can without much of a stretch recognize the message on the low piece board of a picture which for the most part happen shading picture.

Steganography as a method for clouding information without a doubt, alongside encryption, steganography is one of the crucial routes by which information can be kept classified. For better security, we consolidate steganography and cryptography together in this thesis. In the event that we transmit the mystery message with the assistance of this approach, nobody can undoubtedly distinguish the mystery message effortlessly.

Steganography is an exceptional instance of information covering up. The primary objective of steganography is to escape identification of mystery message. Steganography utilizes as a part of various frame by and large advanced type of steganography are utilized for correspondence over the web. In this paper, advanced type of steganography is utilized that is concealing a message inside a picture.

5. PROPOSED SYSTEM

In this proposed work, we have implement an image steganography using a Hash-LSB encoding and decoding, RSA message or file encryption and decryption, and chaotic used an image encryption decryption algorithm. Image, text and document type of data's are hidden into the image. The overall process creates a dual encryption. i.e., our secret data's encryption on RSA and chaotic algorithms; three level processes use this work in secure data transmission. (i) Secrete message or file Encryption decryption using RSA algorithm.(ii) Encrypted and decrypted message or file embedding and retrieving cover image using H-LSB Technique and (iii) Encrypt and Decrypt steganography image using chaotic Algorithm.

RSA Encryption (Embedding Algorithm): Step 1: Choose the cover image & secret message and in the Step 2: Encrypt the message using RSA algorithm; then in Step 3: Image

classification into two blocks – background as block B and textured region as block A. In Step 4: Find histogram maxima in block B (Select carrier in background region) and in Step 5: Block A LSBs Embedded into Block B. In Step 6: perform prediction and Determine prediction error image and in Step 7: Embed the secret information using LSB watermarking and in Step 8: Send stego image to receiver.

RSA Decryption (Retrieval Algorithm): Step 1: Receive a stego image. Step 2: Find 4 LSB bits of each RGB pixels from stego image. Step 3: Apply hash function to get the position of LSB's with hidden data. Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively. Step 5: Apply RSA algorithm to decrypt the retrieved data. Step 6: Finally read the secret message.

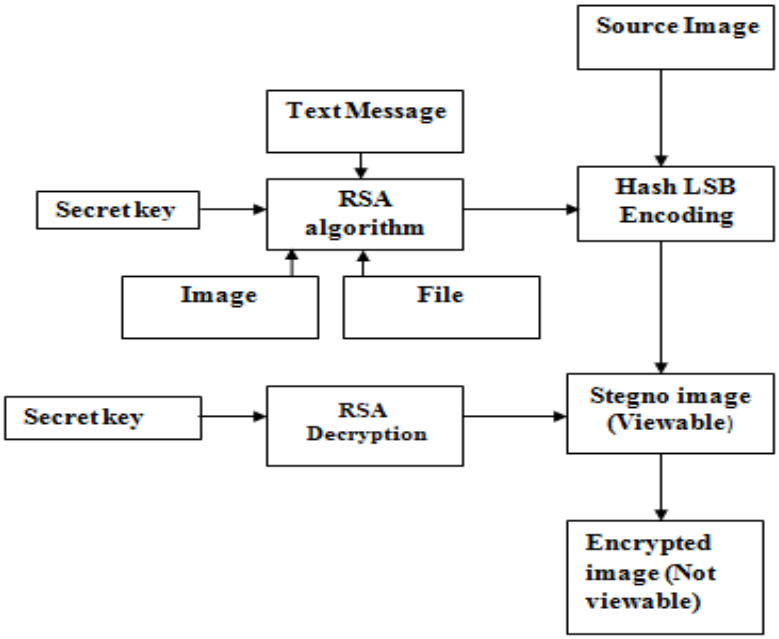

Fig 1: Block Diagram of Proposed System

6. RESULT AND CONCLUSION

Result: A Secure Image Steganography Based on RSA Algorithm and RDH using reserving room algorithm Technique has been implemented. An efficient encryption technique RSA used to encode the secret information or data file, and then hide into the cover image file using reserving room technique secret hidden process done without disturb image-viewing option. The reverse process will be done retrieving the original data according to secret key value for both RSA.

Conclusion: In this research work, a Hash-LSB based embedding of the encrypted text has been proposed. RSA encryption is performed for providing more security to data. The developed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the carry image. This technique makes sure that the data has been encrypted before embedding it into a carry image. Second level is to encrypt and decrypt steganography image using Blowfish algorithm, this action used to manage another cycle of security process implementation.

Currently, more consideration is paid to reversible information concealing (Reversible Data Hiding) in encoded pictures, since it keeps up the astounding property that the first cover can be losslessly recuperated after installed information is removed while securing the picture substance's privacy. Every single past strategy implant information by reversibly clearing room from the scrambled pictures, which might be liable to a few blunders on information extraction as well as picture rebuilding. In this paper, we propose a novel strategy by holding room before encryption with a customary RDH calculation, and accordingly it is simple for the information hider to reversibly insert information in the encoded picture. The proposed technique can accomplish genuine reversibility, that is, information extraction and picture recuperation are free of any blunder. Tests demonstrate that this novel strategy can install more than 10 times as substantial payloads for a similar picture quality as the past techniques, for example, for PSNR=40dB.

Presently a day's security is one of the significant issue confronting everywhere throughout the world. To shield your mystery data from the outsiders it is important to change over the data into unrecognizable shape. To shield data from unapproved get to different strategies for data concealing like steganography, cryptography, Hash-LSB procedures have been produced. In this paper, the proposed work is to display a Hash-LSB based inserting of the scrambled content and picture. RSA and Chaos calculations have been connected to scramble the picture and content to escalate the insurance or security in the correspondence region for information sending. RSA encryption is performed for giving more security to information

7. REFERENCES

[1] Anil Kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue No. 7, July 2013

[2] Aishwary Kulshreshta , Ankur Goyal"Image Steganography Using Dynamic LSB with Choatic

Algorithm" International Journal of Computer & Organization Trends, Vol 3 Issue No 7, August 2013.

[3] Mamta Juneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.

[4] Swati Tiwari, R. P. Mahajan, "A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion", International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.

[5] N. F. Johnson, S. Jajodia, "Steganography: seeing the unseen", IEEE Computer, Vol. 31, Issue No. 2, Pages No. 26 - 34, Feb., 1998.

[6] Wien Hong, Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", IEEE Transactions on Information Forensics and Security, Vol. 7, Issue No. 1, Pages No. 176 - 184, Feb., 2012.

[7] Komal Patel, Sumit Utareja, Hitesh Gupta"Information Hiding using Least Significant Bit Steganography and Choatic Algorithm" International Journal of Computer Applications, Vol. 63, Issue No.13, February 2013.

[8] R. Chandramouli, N. Memon, "Analysis of LSB based image Steganography techniques", International Conference on Image Processing, Vol. 3, Pages No. 1019 – 1022, 07 Oct 2001-10 Oct, 2001.

[9] Weiqi Luo, Fangjun Huang, Jiwu Huang, "Edge Adaptive image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol. 5, Issue No. 2, Pages No. 201 – 214, June, 2010.

[10] Ross J. Anderson, Fabien A. P. Petitcolas, "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 – 481, May, 1998.

[11] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, Tong-Yee Lee, "A High Capacity 3D Steganography Algorithm", IEEE Transactions on Visualization and Computer Graphics,Vol. 15, Issue No. 2, Pages No. 274–284, March- April, 2009.

[12] Nicholas Hopper, Luis von Ahn, John Langford, "Provably Secure Steganography", IEEE Transactions on Computers, Vol. 58, Issue No. 5, Pages No. 662 – 676, May, 2009.