Securing Information for Commercial File Sharing by Combining Raster Graphic and Vector Graphic Stseganographies

Rekha Kashyap, Manasvini Ganesh

Abstract: ***Commercial applications cannot declare use of steganography as its security model so as not to spoil the norm of "hidden" secret. Proposed paper suggests a model that can withhold security even after declaration of steganography's presence allowing applicability in commercial scope. File to be secured is compressed and converted to byte stream and hidden in both raster graphic and vector graphic cover images and encapsulated in a PDF and shared. To extract the secured file from the cover images a key is required by the party intending to receive the secured file. This key is shared by Elliptic Curve Diffie Hellman Key Agreement Protocol. The intended receiver extracts the file by applying steganalysis. To implement this model an android application is developed that shares files by securing it in aforesaid fashion and transferring them via Wi-Fi Direct. Most of the digital image steganography researched are based on raster graphic cover images. The proposed model is designed so that limitations present in raster and vector steganographies each can be counterfeited to produce a secure solution that can be offered in digital image steganography. This solution is suggested as security model in commercial scope.***

Index Terms: Image Processing, Information Security, Steganography

I.INTRODUCTION

INFORMATION Security is pillared by Confidentiality, Integrity and Authenticity of information. It is popularly known as the info-sec triad. To protect the pillars two major technologies can be employed – Cryptography and Steganography. Cryptography widely used in defense as well as commercial applications can be defined as study of techniques for confedential communication in the presence of third parties called "adversaries". It employs encryption to achieve this. But when crypt text is analyzed by an adversary it is understood that some secret is being communicated thus challenging the adversary to extract the confidential data [1]. Steganography on the other hand hides the confidential data in an innocent covert channel. Covert channel in digital world could be text, image, audio, video or network protocol that can secretively carry the confidential data. A covert channel as a digital image is called "cover image". Steganography thus prevents attacks from adversary as the presence of confidentiality in communication is obscure. The hiding in steganography is analogous to encryption in cryptography and is referred as "encoding"[2].

A. *Objective*

The objective of this paper is implementing digital image steganography for security in commercial applications. The security has to be achieved despite declaration of steganography's presence. Security must provide confidentiality, authenticity, authorized access and integrity of data.

B. *Contribution*

A security protocol is proposed that combines raster and vector steganographies. In this work the limitations of raster steganography are counterfeited by vector steganography and limitations of vector steganography are counterfeited by raster steganography. A commercial Android application is built as an illustration of the protocol and thus uses steganography as the security model. The illustrated commercial application shares files over Wi-Fi Direct network. The file to be shared is compressed and converted to byte stream onto which a combination of dual graphic steganography is applied using discussed combination of dual graphic steganography. PDF is shared using Wi-Fi Direct with intended receiver of file. A client - host connection is made for file transfer by using Wi-Fi network where clients and hosts identify each other using email IDs. Every user of the application must register with the application to use it for successful registration the email ID of the user is verified and acts as authentication ID of the user. Key agreement is made by Elliptic Curve Diffie Hellman (section 3.4) and key exchange is established when host accepts connection with client. The receiver then applies steganalysis to extract the confidential data. The application has restricted access with password for authorization. The implementation is discussed in detail in section 5. The proposed protocol is here on referred to as Ostracon which means, "Potsherd used for writing surface" since our objective is to "write" secret on "images" (analogous to ones painted on potsherds).

II.RELATED WORKS

Different techniques for steganography and steganalysis were studied. Abbas Chedasd [3] e.t. al' provided review and analysis of different methods of steganography along with describing common standards, guidelines and recommendations. Bin Li, e.t. al' [4] described a short survey on different types of steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image. R. Chandramouli e.t. al' [5] had put up analysis of most recent steganographic techniques. D. C.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Rekha Kashyap*, Professor and Head, Computer Science Department at Inderprastha Engineering College, Ghaziabad,India

Manasvini Ganesh, B. Tech in Computer Science Engineering from Inderprastha Engineering College, Sahibabad, affiliated with Dr. A.P.J. Abdul Kalam Technical University, Lucknow.

Wu e.t. al' [6] used pixel value differencing (PVD) method for secret data embedding in each of the component of a pixel in a colored image. C. H. Yang e.t. al' [7] proposed a new adaptive least-significant bit (LSB) steganography method using pixel-value differencing (PVD) They proposed enhanced embedding capacity and imperceptible stego-images as pixels located in the edge areas are embedded by a k-bit LSB substitution method with a larger value than that of the pixels located in smooth areas. W. Luo e.t. al' [8] suggested an image steganography using LSB matching and suggested edge adaptive scheme. Their proposed work selected the embedding regions on the basis of size of secret image and the difference between consecutive pixels in the cover image. They further proposed lower embedding rates for sharper edge regions without disturbing the smooth regions. For higher embedding rates more edge regions were released adaptively. X. Li, B. Yang, D. Cheng, and T. Zeng [9] used matrix encoding and cat mapping techniques to provide high imperceptibility towards steganalysis. Ming Yang[10], e.t. al proposed a joint cryptograph-steganography methodology, which combines both encryption and information hiding techniques to ensure patient information security and privacy in medical images. R. Singh and D. Shaw [11] ,suggested an application using Hybrid approach of Cryptography technique and dual watermarking for the purpose of Providing highly security and authentication of digital data. This paper used cryptography and QR Code in combined approach of LSB and DCT Digital image water marking technique. A. Gutub, A. Al-Qahtani and A. Tabakh [12] proposed "triple-A" algorithm using principle of LSB, where the secret is hidden in the least significant bits of the pixels, with more randomization in selection of the number of bits used and the color channels that are used. This randomization is expected to increase the security of the system and also increase the capacity. Ishwarjot Singh and J. P. Singh Raina [13] used hopfield algorithm & LSB technique. Hop-field algorithm is used on the original image to optimize the result. Further a key is generated from this result using LSB technique hiding the secret data behind this image. This forms a stego image where data can be hidden. Integrity check via steganography is a new emerging domain like K. S. babue.t. al' [14] proposed a solution to verify reliability of information to be transmitted using image steganography techniques. The proposed algorithm promises to verify whether the attacker has attempted for edit, delete or forge the secret information in the steganography image. The technique embeds the hidden information in the spatial domain of the cover image and uses two special AC coefficients of the Discrete Wavelet Transform domain to verify the veracity (integrity) of the secret information from the stego image. Michel K. Kulhandjian e.t. al' [15] considered the problem of extracting data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video), using raster steganographic techniques. N. Provos and P. Honeyman[16] presented research on detection, steganalysis techniques and mechanisms. J. Fridrich and J. Kodovsky [17] described a novel general strategy for building steganography detectors for digital images. In contrast to previous approaches, the model assembly is made a part of the training process driven by samples drawn from the corresponding cover- and stego-sources.J. Fridrich, J. Kodovsky and V. Holub [18] proposed an alternative and well-known machine learning tool-ensemble classifiers implemented as random forests-and argue that they are ideally suited for steganalysis. I. Avcibas, N. Memon, and B. Sankur [19] presented a novel technique for steganalysis of images with basic idea that the correlation between the bits planes as well the binary texture characteristics within the bit planes differs between a stego-image and a cover-image. These telltale marks can be used to construct a steganalyzer, that is, a multivariate regression scheme to detect the presence of a steganographic message in an image.S. Dumitrescu, Xialoin Wu and Zhe Wang [20] proposed a novel approach for detection of least significant bit(LSB) stegnography for image and audio based digital signals. Their solution claims to estimate the lengths of hidden signals embedded in the least significant bits of signal samples with relatively higher precision. Their proposed steganalytic approach uses statistical measures of sample pairs which are very sensitive to LSB embedding operations. They claim the proposed detection algorithm to be comparatively simple but efficient in terms of execution speed.

C. Yang e.t. al' [21] used exclusive or operation on the pixel group based trace model to simulate the MLSB embedding and further traced the transition relationship to find possible structures by some trace pixel group subsets. They further derived the estimation equations of embedding ratio from the transition probability matrix using trace subsets and the symmetry of regular and singular pixel group sets. Their experimentation results for triple pixel group promises estimation of low embedding errors with small error. T. K. Ivancevic, M. Rudolf, N. S. Loknar [22] elaborate on linear graphics and typographic elements in the function of hiding information in security printing. Hidden information is introduced with the goal to protect the originality of the produced graphic designs so their counterfeiting would be impossible. B. Mados, J. Hurtuk, M. Copjak, P. Hamas, M. Ennert [23] presented a new data hiding technique based on steganographic algorithms that is hiding information into vector images. The paper briefly introduced this technique and evaluated the benefits and drawbacks of the proposed approach.

III.BACKGROUND

Some of the pre requisite concepts before discussing the proposed protocol are enumerated in this section.

A. Raster and Vector Graphics

Digital images in computer graphics are represented in two forms namely Raster and Vector graphics. In Raster graphic representation an image is represented as a 2-D matrix where each element is called a pixel. A pixel contains color information. Vector graphic representation is made by dictating an image with mathematical functions like polygons, curves and vectors. JPEG (Joint Photographic Experts Group), PNG (Portable Network Graphics) and GIF (Graphic Interchange Format) are examples of raster graphic images while SVG (Scalable Vector Graphics) and PDF are examples of vector graphic images.Vector graphic images are scalable infinitesimally as they are simply mathematical functions that can be input with scaled parameters for scaling the image while raster graphic images become pixilated or aliased when scaled.

B. Steganography

Steganography can be classified on the basis of the cover media being used. Text, audio, video, image and network protocol are used as the cover media but digital image is the most popular and accepted media. Figure 1 is a description of the classification of digital image steganography in terms of raster and vector graphic steganographies and their techniques. Such a classification is expressed uniquely in this paper. Raster Graphic Steganography can be accomplished in transform and spatial domain. In spatial domain, steganography is directly applied to the pixels of the raster image. Least Significant Bit (LSB) steganography is the most common method in raster domains as discussed below with an example. The example uses 3 bit LSB. Let a 24 bit RGB pixel be represented as (10001**000**00010**001**11101**110**)$_2$. Then by replacing 3 least significant bits of each octet with a secret message say '4 2 1' which has binary equivalence (*100 010 001*)$_2$ gives (10001**100**00010**010**11101**001**)$_2$. When steganalysis is employed each LSB is extracted back to form the secret data. Transform domain is a function of spatial domain of image. For example when compressing an image to JPEG, Discrete Fourier Transform of image is computed. This is called Fourier or Frequency domain. Steganography is applied to this image in frequency domain. When Inverse Discrete Fourier Transform is applied original image is obtained. This image also contains steganographic data. This is raster steganography in transform domain. Raster steganography is quicker to perform in spatial domain if a lookup table for pixels and their locations are made. E.g., Pixel color at pixel position (1, 3) is red.

.

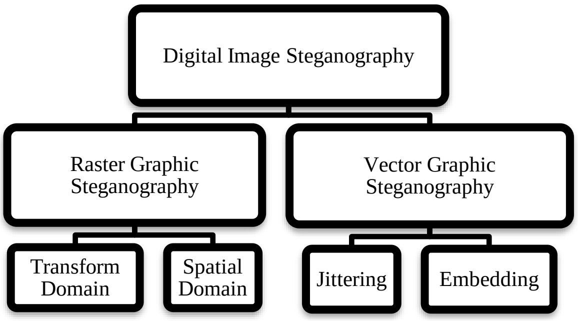

Digital Image Steganography
Raster Graphic Steganography
Vector Graphic Steganography
Transform Domain
Spatial Domain
Jittering
Embedding

Figure 1: Digital Image Steganography Techniques

Vector Graphic Steganography can be accomplished by two techniques "Jittering" and "Embedding" respectively. Jittering is the process of storing confidential information in least significant positions of anchor points in a vector image. If a point is at coordinate (x, y) as (2.0076, 9.8265) then by altering the LSB information one may hide data in anchor point thus modifying the coordinate as (2.0076**3659**, 9.8265**2948**). The image now has its anchor points a bit out of order as compared to the original image thus the name jittering technique. Jittering technique is not robust as when the vector image is scaled (up or down) the values of LSBs are lost. This is called the "jittering effect". Therefore confidential data encoded becomes corrupted.

In embedding technique extra anchor points are added (embedded) in path of the curve between existing anchor points. This does not disrupt the image output but unwanted anchor points confirm presence of steganography.

When adversary has access to **original cover image** and **encoded cover image** and derives inferences by comparing both cover images, to decode confidential contents the process is called **statistical attack**.

C. PDF – Postscript Document Format

PDF is a file format used to present documents in a manner independent of application software, hardware and operating systems. Each PDF file is composed of pages and each page contains text, fonts, graphics etc. PDF can contain raster as well as vector graphic components.

D. Elliptic Curve22519 Diffie Hellman

Applying Elliptic Curve Cryptography to Diffie Hellman key exchange resolved many vulnerabilities of key exchange problem. Elliptic Curve22519 Diffie Hellman is a variant of ECDH. It is used to generate a shared secret over an insecured channel between two parties each having an elliptic curve public-private key pair. [24]

E. *Wi-Fi Direct*

Wi-Fi Direct is a wireless in fidelity standard for devices which enables the wireless devices to communicate and connect without the requirement of wireless access point. Devices on Wi-Fi direct connects wirelessly in a manner similar to Bluetooth connection at speeds similar to Wi-Fi. This technology has opened interoperability in communication among devices from different manufacturers. Links in Wi-Fi direct are negotiated using the Wi-Fi protected setup. [25].

IV.PROPOSED WORK

Ostracon achieves security by combining raster steganography and vector steganography and encapsulating the cover images in a Postscript Document Format (PDF). The proposed combination of raster and vector graphic steganography is uniquely introduced in this paper. Selection of raster graphic image is made by randomly selecting a raster image that is not recently used. Vector graphic image is generated by a process called vectorization (conversion to vector graphics) and is performed on another raster graphic image (which is not used as cover image). To decode the PDF, secret is kept in keys and keys are shared using ECDH key exchange. The need for ostracon arrives due to limitations of raster and vector stegnography when applied individually.

A. Limitations of Individual Steganographies

Vector Stegnography has a major limitation of poor payload capacity. The reason being: Vector graphic cover image is linearly proportional to the number of nodes used to represent the vector image. The number of nodes required to represent a vector image is far less than the number of pixels required to represent similar raster image. Thus payload capacity of vector graphic steganography is far less than raster. The strength of payload capacity in raster is explained with an example image with following attributes –

a) The dimensions of example image in width x height is 512 x 512.

b) Image file size of this image is 35 KB

The payload capacity can be illustrated as follows.

Let LSB be performed such that in each pixel 1 byte of confidential data is encoded.

a) The number of pixels in cover image = 512 x 512 = 2,62,144
b) Since 1 byte is encoded in each pixel, total number of bytes that can be encoded = 2,62,144 bytes
c) 2,62,144 bytes = 256 KB (Since 1 KB = 1024 bytes)

So 256 KB data can be encoded in 35 KB file size of cover image. That is nearly 7.3 times the file size of cover image.

Raster steganography on the other hand has two major disadvantages, easy steganalysis and multiple cover images problem as explained below. *Easy Steganalysis problem*

Steganalysis is the process of detection of presence of secret data in cover media. A strong steganography technique should be able to handle this problem. Steganalysis of raster is easier than in vector graphics. This is because in raster graphics pattern among encoded pixels can reveal more information than pattern among coordinate values in vector. Pixel values are related with neighboring pixel color values and have fixed range of possible values. Whereas for coordinates the range is real number and the coordinate values are not related with neighbor coordinates as in raster. Another advantage with Vector is that steganalysis in it difficult because of jittering effect (section 3.2). If an adversary opens the vector image, a slight scale up or down can corrupt the confidential bytes encoded. Thus opening the image acts like a trap that destroys the data[2].

Multiple cover images problem

One cover image is not sufficient to encode confidential data completely. If the number of bytes of confidential data is more than payload capacity of cover image then more cover images are required.

Multiple unique cover images can be used to encode data completely. But locating multiple cover images, storing them and processing them is *not cost effective.*

Multiple copies of a single cover image can be used to encode data completely. If all cover images have same source image then they are vulnerable to statistical attacks. This is explained as follows. An adversary can analyze all the images, find a pattern and look for a trace of file metadata i.e., data about file. . If the adversary is successful in obtaining metadata of file then the structure of file encoded becomes obvious to them. This structure can further help in analyzing cover images for contents of file. For example the confidential file is a JPEG image. On analysis of cover images adversary identifies the pattern of encoding and knows that the first few bytes hidden are metadata of file. On analysis of first few bytes they can identify it as an image. And thus will observe the other bytes hidden as pixels. This information can help adversary reconstruct the confidential file.

B. Proposed model OSTRACON as a solution

A combination of raster and vector graphic steganography is proposed in Ostracon. To tackle the problem of multiple cover images faced by raster steganography Ostracon suggests single cover image or multiple copies of single cover image for larger confidential data. To counter the statistical attack Ostracon proposes encoding of metadata of confidential file in vector steganography as vector steganography provides better protection against steganalysis attacks. Rest of the data of confidential file will be encoded using raster steganography since it offers much better payload capacity. *Thus only two unique cover images are required, one for raster steganography and another for vector steganography.* Then the encoded cover images are encapsulated in PDF. To counter multiple cover images problem the pattern of selecting pixels from each cover image copy, should be different. Thus statistical attack would be difficult. The selection of cover images is proposed from web. To counter against any statistical attack, OSTRACON proposes, use of vectorization on raster graphic image which will produce vector graphic cover image. The vectorized image offers resistance against statistical attack.

V.IMPLEMENTATION OF PROPOSED WORK

Various libraries used in implementation of Ostracon and their purposes are enumerated in table 1.

TABLE 1 LIBRARY USED

Serial Number	Library Name	Purpose
1	Potrace	Vectorization of images
2	iText	PDF creation and manipulation
3	ECDH	Key Agreement
4	Salut	Wi-Fi Direct implementation
5	LoganSquare	Serialization (fastest serialization library)

Ostracon protocol has to be tested for practical applicability. Thus appropriate algorithms are written for each module. The major modules involved are –

a) Authentication
b) Authorization
c) Cover Image Resolver
d) Sharing keys and file by host and receipt of data by client
e) Encoding
f) Decoding

A. Authentication

Registered and verified email ID is used for authentication. The email ID is significant during data transfer through Wi-Fi Direct. Host (user sending file) and client (user receiving file) identify each other using email ID.

B. Authorization

Authorization is implemented by hashing the password before storing in database.

C. Cover Image Resolver

This module resolves cover images from web. Parameters considered while making choice of cover image are discussed below. The cover image to be used for raster graphic steganography should have dimensions in powers of 2 e.g. 512x256 (2^9X2^8).This is required for ease of computations. The selection of cover image for vector graphic steganography is done by vectorizing a raster graphic image. The significance is discussed in section 4. The raster image for this purpose must be such that the traced (vectorized) image has many coordinates for good payload capacity. As illustrated through figure 2 the image of globe has 75% more nodes as compared to “TUESDAY” so one has to do mathematical analysis to find such images.

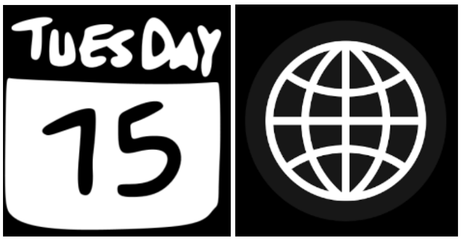


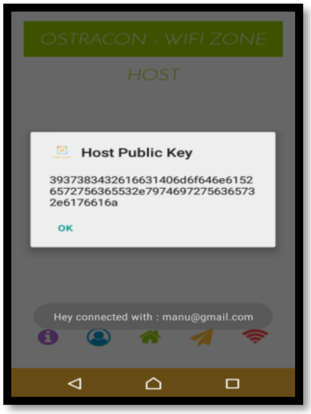
Figure 2: Vector graphic examples

For optimum execution a raster and vector table that stores pixel or coordinate value corresponding to an index is maintained. The index for raster graphic table is simply the two dimensional array indexes in which raster graphic image is represented. For vector graphic table the vector graphic coordinates are arranged in one dimensional array for quick access. These tables can be used for optimizing loops in the program. Sharing keys and file by host: LoganSquare is used to serialize the PDF. A key derived by ECDH algorithm is used to encrypt secret that contains file size and encoding pattern information. The serialized object and this encrypted secret are shared.

D. Sharing keys and file by host and Receipt of data at client

LoganSquare is used to serialize the PDF. A key derived by ECDH algorithm is used to encrypt secret that contains file size and encoding pattern information. The serialized object and this encrypted secret are shared.

List of found host networks available are displayed to the client by Ostracon. The client makes request to connect with the desired host. If host accepts the connection, a connection is established. Client receives the encoded PDF and the encrypted secret. Ostracon at client end decrypts the secret by deriving key from ECDH algorithm. The decryption yields file size and encoding pattern information. Using this information cover images in PDF are decoded.



Host Public Key

3937383432616631406d6f646e6152
6572756365532e7974697275636573
2e6176616a

Hey connected with : manu@gmail.com

Figure 3: Public Key of Host

E. Encoding

A PDF document is initialized by using iText. PDF Writer instance is instantiated with the PDF document. Metadata of confidential file is encoded in vector steganography and rest of file contents are encoded in raster as discussed in proposed work. The number of raster cover images required is calculated as $\frac{number\ of\ bytes\ in\ confidential\ file}{payload\ capacity\ of\ raster\ cover\ image}$ .These images are encapsulated in PDF using iText. The sequence diagram for encoding is shown in figure 4.

Variables used in Encode Operation:

a) **k**: number of LSBs to be replaced
b) **SE**: pixel
c) **secret_data**[ ]: byte array representing confidential file

Algorithm for Dncode Operation:

a) For each cover image iterate over **SE**
b) For each SE set **k**-LSB as 0s
c) Now extract k bits from **secret_data**[ ]
d) Add these bits to the **SE** by binary operations
e) Return the cover image

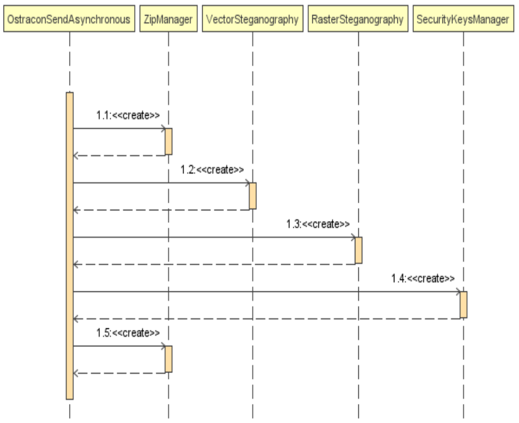


Figure 4: Ostracon’s sequence diagram for Encoding

F. Decoding

A PDF document is initialized by using iText. PDF Reader instance is instantiated with the PDF document. Decode of vector encoded cover image is followed by decode of raster encoded cover images. Image from each page of PDF is extracted. Once all pages of PDF have been read the process stops. The document and PDF Reader instances are closed. The sequence diagram for decoding is shown in figure 4.

Variables used in Decode Operation:

a) **k**: number of LSBs replaced (k = 3, see section 4 architecture of raster steganography)
b) **SE**: pixels
c) **secret_data**[ ]: byte array representing confidential file
d) **secret**: single byte extracted from SE used to create the complete **secret_data[ ]**

Algorithm for Decode Operation:

a. For each cover image iterate over **SE**
b. For each SE get **k**-LSB
c. Now save the extracted bits as a single byte in **secret**
d. Add **secret** to the **secret_data** [ ]
e. Return the **secret_data [ ]**

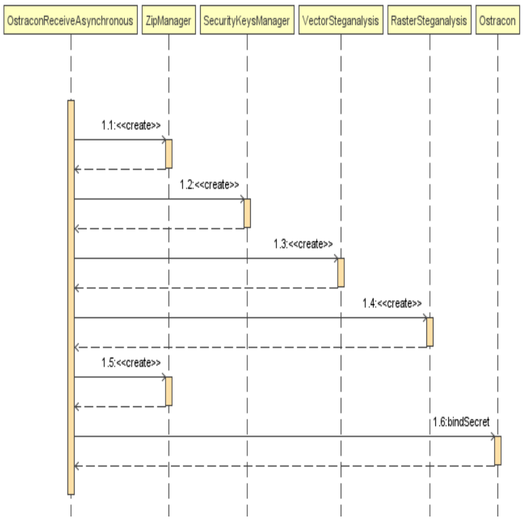


Figure 5: Ostracon's sequence diagram for Decoding

Figure 6 illustrates user interfaces through activity diagram. All these activities are performed by Ostracon.

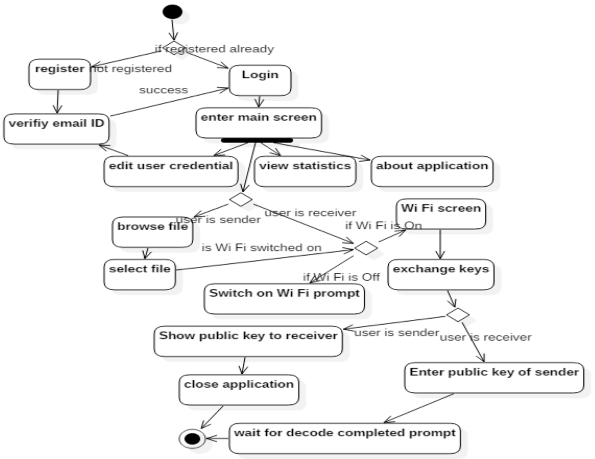


Figure 6: Activity Diagram

VI.SECURITY ANALYSIS

a) Confidentiality: Encoding in raster steganography and traps due to jittering effect (see section 4) in vector steganography contribute to confidentiality of data.

b) Authenticity: Verified email IDs act as authenticated IDs. And since key of intended sender has to be input it also acts as authentication ID. But to make Wi-Fi connection authentication check must be done so email IDs are necessary.

c) Authorization: Password protected logins and key protects authorization. When receiver enters sender's public key only the intended receiver can access the document. Thus keys also provide authorization.

d) Integrity: Jittering effect maintains integrity of confidential data as mentioned in section 4.

VII.PERFORMANCE ANALYSIS

Table 2 shows the time taken for the two major operations in Ostracon – **Encoding** and **Decoding**. To improve the performance, the encoding and decoding procedure is analyzed.

Key points noted are –

a) 145 bytes takes more time encoding than 1.2 KB. The reason is 1.2 KB files is compressed before transfer and thus becomes "lighter". Whereas if we ZIP compress 145 bytes resultant ZIP file becomes heavier because of redundant encoding in ZIP.

b) On increasing file sizes to be secured, a sudden drop in encoding time is observed. Referring to this point as "drop point", the reading following drop point, gives larger encoding time than any reading observed prior to it. This is because; a new page is added to the PDF which increases the execution time. Decoding time monotonically increases with increase in file size of input unlike encoding time. This is shown in Table 2 and Figure 7.

Table 2 Encoding And Decoding Time For Varying File Size Needed To Be Shared Securely

FILE SIZE	ENCODING TIME	DECODING TIME
145 B	2.259 s	0.674 s
1.2 KB	1.697 s	0.622 s
6.2 KB	1.499 s	0.732 s
21.1 KB	1.8 s	0.887 s
40.6 KB	1.964 s	0.976 s
119.5 KB	3.24 s	1.436 s
215 KB	4.789 s	2.204 s
361 KB	3.229 s	3.87 s
687 KB	7.154 s	5.737 s
1.2 MB	10.589 s	11.344 s
6.1 MB	49.526 s	57.404 s

- **Hardware - Qualcomm MSM8226 processor (Sony Xperia)**
- **Software – Android 5.1.1 (Lollipop) OS**
- **Minimum SDK – API level 19**
- **Compilation SDK – API level 23**
- **Target SDK – API level 25**
- **For better performance Android NDK is used with JNI as an interface with Java and C++.**

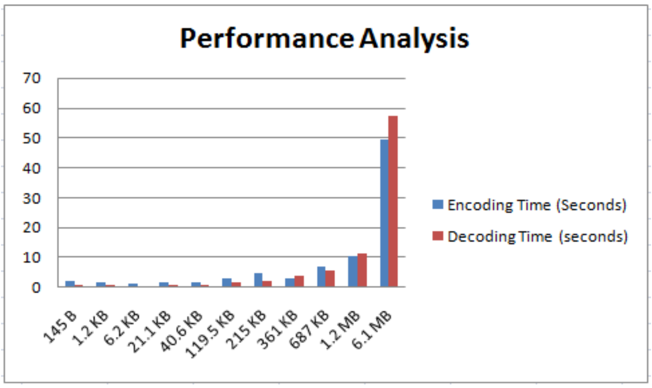


Figure 7: Encoding and decoding time on varying file size

A. *Time Complexity Analysis:*

If m and n are taken as number of coordinates in SVG (where m is number of x-coordinates and n is number of y-coordinates) and for raster graphic m and n are dimensions of the image in width x height resolution.

k is the number of bytes of secret data (or file) and each pixel has a payload capacity of 1 byte then, the order of execution is O (m x n x k) that is cubic polynomial.

Ostracon improves this by constructing a look up table at the first execution of the application. The look up table is used to map values of pixels/coordinates when queried by Ostracon. The ranges of permissible indices are marked in fields of class that represent the table. Two such tables are constructed one for each graphic medium. So now querying for encoding or decoding procedure only takes O (k) that is linear asymptotic time!

B. Space Complexity Analysis:

If k1 is the size of a cover image required in vector graphic and k2 is the size of a cover image required in raster and p1 is the number of vector cover images and p2 is number of raster cover images then space required is$O((k1 * p1) + (k2 * p2))$. The asymptotic complexity is quadratic.
The static space requirement of the application is 2.1MB.

VIII.CONCLUSION

Ostracon is a secured solution for commercial implementation of steganography. The combined use of raster and vector steganography protects the hidden information without compromising on payload capacity and at the same time offers strong check against steganalysis. Ostracon can be used with interesting feature upgrades. Future scope of work deals with new features that can be added for betterment.

a) Authorization can be improved with fingerprint (or other Biometrics) as password.
b) Authentication can be improved by standards like OAuth 2.0
c) Instead of receiver typing in sender's public key, receiver can simple scan a QR code in sender's screen.
d) It can even be used to set access rights to the file so that the file cannot be duplicated and screenshot cannot be taken under Ostracon.
e) A timer can be set after which the file is automatically destroyed from shared peers.
f) Ostracon can be upgraded to support real time chat environment.
g) It can be used in mail security.
h) It can be used to secure documents internally for user's self document protection.

REFERENCES

1. T. Rajani Devi, "Importance of Cryptography in Network Security", International Conference on Communication Systems and Network Technologies, 2013
2. Alaa A. Jabbar Altaay, Shahrin Bin Sahib, Mazdak Zamani, "An Introduction to Image Steganography Techniques", International Conference on Advanced Computer Science Applications and Technologies, 2012
3. Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt. (2009, September). "Digital Image Steganography: Survey and Analysis of current methods". School of computing and Intelligent Systems, Faculty of Computer Science and Engineering, University of Ulster at Magee, London,Northern Ireland UK[Online]. Available:http://abbascheddad.net/Survey.pdf
4. Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, April 2011, pp. 141-173.
5. R. Chandramouli, M. Kharrazi, and N. Memon, "Image Steganography and Steganalysis: Concepts and Practice", T. Kalker et al. (Eds.): IWDW 2003, LNCS 2939, Springer-Verlag Berlin Heidelberg, 2004, pp. 35-49.
6. D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613–1626, 2003.
7. Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, September 2008, pp.488-497.
8. W. Luo, F. Huang, J. Huang, "Edge Adaptive Image Steganography Based On LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, vol.5, no.2,pp.201-214, Feb. 2010.
9. X. Li, B. Yang, D. Cheng, and T. Zeng, "A generalization of lsb matching", IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69-72, 2009.
10. Ming Yang, Monica Trifas, Guillermo Francia and Lei Chen,(2009) " Cryptographic and Steganographic Approaches to Ensure Multimedia Information Security and Privacy" International Journal of Information Security and Privacy (IJISP), 3(3),2009, |Pages 37-54.
11. Ranjeet Kumar Singh, Dilip Kumar Shaw, "A Hybrid Concept of Cryptography and Dual Watermarking (LSB_DCT) for Data Security",International Journal of Information Security and Privacy (IJISP), 12(1), 2018, pp 1-12.
12. Gutub, A., Al-Qahtani, A., and Tabakh, A., "Triple-A: Secure RGB image steganography based on randomization", Computer Systems and Applications, AICCSA 2009, IEEE/ACS, pp. 400 – 403, 2009.
13. Ishwarjot Singh, J. P. Singh Raina"Advance Scheme for Secret Data Hiding System using Hop-field & LSB "International Journal of Computer Trends and Technology (IJCTT),V4(7):2216-2221 July Issue 2013 .ISSN 2231-2803.www.ijcttjournal.org. Published by Seventh Sense Research Group.
14. K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON-2008, (2008) November, pp. 1-6.
15. Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, "Extracting spread-spectrum hidden data from digital media", IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.
16. N. Provos, P. Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy, Vol. 1, No. 3, 2003, pp. 32-44.
17. J. Fridrich, J. Kodovsky, "Rich models for steganalysis of digital images", IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 868-882, Jun. 2012.
18. J. Kodovsky, J. Fridrich, V. Holub, "Ensemble classifiers for steganalysis of digital media", IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 432-444, Apr. 2012.
19. I. Avcibas, M. Kharrazi, N. D. Memon, B. Sankur, "Image steganalysis with binary similarity measures", EURASIP J. Appl. Signal Process., vol. 17, pp. 2749-2757, 2005.
20. S. Dumitrescu, X. Wu, Z. Wang, "Detection of LSB steganography via sample pair analysis", IEEE Trans. Signal Process., vol. 51, no. 7, pp. 1995-2007, Jul. 2003.
21. C. Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.
22. T. K. Ivancevic, M. Rudolf, N. S. Loknar. "Steganography of vector graphics and typography using infrared security printing."ActaGraphica. vol. 27 no.1, 2006 [Online]. Available:http://www.actagraphica.hr/index.php/actagraphica/article/view/93/87
23. B. Mados, J. Hurtuk, M. Copjak, P. Hamas, M. Ennert. "Steganographic Algorithm for information hiding using scalable vector graphic images", 2014
24. Shengbao Wang1 , Zhenfu Cao1 , Maurizio Adriano Strangio2 and Lihua Wang, "Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Key Agreement Protocol", 2007, National Institute of Information and Communications Technology, Japan
25. Daniel Camps-Mur, Andres Garcia-Saavedra, Pablo Serrano, "Device-to-device communications with Wi-Fi Direct: overview and experimentation", 2013, IEEE Wireless Communications

AUTHORS PROFILE

Dr Rekha Kashyap. During her twenty-six year career including 17 years in academics and 9 years in corporate, Dr Rekha Kashyap is currently working as Professor and Head, Computer Science Department at Inderprastha Engineering College, Ghaziabad,India. She did her Ph.D. from Jawaharlal Nehru University, New Delhi in 2012. Her research has been published in leading journals(including Springer, Wiley, Inderscience etc.), and in proceedings of various peer-reviewed conferences in India and abroad. She is member of many International societies including IEEE, CSI(Computer Society of India),Indian Society for Technical Education (ISTE) and International Association of Engineers (IAENG) . She is in the editorial board and reviewer's panel of many International Journals and conferences. Her teaching and research interest includes, Block Chain Technologies, Grid and Cloud Computing, Cryptography and Network security.

Manasvani Ganesh received her B. Tech in Computer Science Engineering from Inderprastha Engineering College, Sahibabad, affiliated with Dr. A.P.J. Abdul Kalam Technical University, Lucknow, in the year 2017. She has contributed to her department in college by developing projects and leading as president for the technical society "Genesis". She is also a member of IAENG International Journal of Computer Science. She has developed many websites and mobile applications which empowers her to understand major privacy violations happening in the web and mobile application domain.