# An Implementation and Modification of Various Techniques to Secure Images using various methods like Stegnography Watermarking and Cryptography

*Varsha Shakti
**Mr. Anil Khandeker

## ABSTRACT

The amazing developments in the field of network communications have created a great requirement for secure transmission of images over the Internet. Internet is a public network; therefore it is not so secure for the transmission of confidential images. As this information are very secure, therefore security over network and at the end of confidential image is very important. To provide security to images, several methods in steganography and cryptography have been proposed. Cryptography techniques are required to accomplish a certain level of security, integrity, confidentiality and as well as, to prevent unauthorized access of sensitive information during transmission over network.

*Pursuing M.E., Indore Institute of Science & Technology, Indore, varsha.sh87@gmail.com
**Asst. Professor, Indore Institute of Science & Technology, Indore,

## INTRODUCTION

The amazing developments in the field of network communications have created a great requirement for secure transmission of images over the Internet. Internet is a public network; therefore it is not so secure for the transmission of confidential images. As this information are very secure, therefore security over network and at the end of confidential image is very important. To provide security to images, several methods in steganography and cryptography have been proposed. Cryptography techniques are required to accomplish a certain level of security, integrity, confidentiality and as well as, to prevent unauthorized access of sensitive information during transmission over network. But, there are many disadvantages of these approaches; Steganography which deals with security using image has a very big disadvantage of increase in the image size. Cryptography which deals with encryption of images using the keys generated by various algorithms has the disadvantage of difficulty in remembering the key which can be easily cracked. Even sharing of key over network need additional security. These approaches provides single level of security. The issue of secrecy for image is resolved in many digital applications, such as broadcasting, sensitive visual aids, military services, rare satellites images and confidential medical images [5]. To meet this challenge, cryptographic techniques are applied.

In recent research, to increase level of security combination of Steganography and cryptography is also used. This makes security of two levels. So, getting the confidential image is being more secured and cannot be easily accessible to unauthorized user. The main objective of this study is to provide more level of security to the confidential images and use chaotic method for encryption. To increase level of security, an approach of generating key using different images will be used.

## OVERVIEW

The frequent developments in the field of network communications during the past years have created a great requirement for securing image transmission over the Internet. Internet is a public network; therefore it is not so secure for the transmission of confidential images over internet. To meet this challenge, cryptographic techniques had been applied. Cryptography is technique for protecting the privacy of information during communication [6]. Other way to provide security to image is Steganography and watermarking. In Steganography approach, confidential image is hiding inside other carrier image. In watermarking approach image is digitally signed and verified at the receiver’s end.

## SCOPE OF WORK:

To meet image security over pubic network, cryptographic techniques are applied at higher level. Cryptography is important way to address image transmission security requirements. Encryption and decryption of images are performed at sender’s and receiver’s end respectively in cryptography. Cryptography alone is not sufficient to make image secure. To make image more secure Steganography will be combined with Cryptography. Steganography is a mechanism of hiding the original images inside other image. Here the secret message is sent as image through the encryption of the message in which secret key is arranged for those intended receivers. The receiver uses this shared secret key to obtain original image. Confidential image can be encrypted as hidden message in any form as audio or video or image. In this project we will be using image. Combination of steganography and cryptography techniques results in appearing a highly secured method for image communication [4].

It is possible to combine the techniques by encrypting image using cryptography and then hiding the encrypted image inside other image using steganography. The resulting stego-image can be transmitted over internet. Furthermore, even if an attacker accesses the stego-image. He will only get the encrypted image. To get the original image attacker has to decrypt the encrypted image using crypto-key[12].

## OBJECTIVE:

i. Provide image security with combination of Cryptography and Steganography.

ii. Secure Key generation using n meaningful images.

iii. Encrypt the image using generated key, to make it meaningless or noisy.

iv. Hide meaningless secret image inside a carrier image without effecting size and clarity of carrier image.

v. Transfer carrier image over network.

vi. Secured Transfer of key generator images over network.

## LITERATURE SURVEY

The word steganography is originally derived from Greek words which mean “Covered Writing”. It is defined as "hiding information within a noise; a way to supplement encryption, to prevent the existence of encrypted data from being detected" [1]. It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave’s head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back [ 2, 4,5,7].

In Saudi Arabia at the King Abdulaziz City of science and technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany [10].

Five hundred years ago, the Italian mathematician Jérôme Cardan reinvented a Chinese ancient method of secret writing. The scenario goes as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as an innocuous text. This method is credited to Cardan and is called Cardan Grille [4].

This section attempts to give an overview of the most important steganographic techniques in digital images. The most popular image formats on the internet are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and to a lesser extent - the Portable Network Graphics (PNG). One of the earliest methods to discuss digital steganography is credited to Kurak and McHugh [1], who proposed a method which resembles embedding into the 4 LSBs (least significant bits). They examined image downgrading and contamination which is known now as image-based steganography.

The survey of Johnson [6] appeared in the “Information hiding” book, which limits its distribution compared to a Journal paper which can be more affordable. The classification, herein, of the techniques and that of Johnson are different. Johnson classify steganography techniques into: Substitution systems, transform domain techniques, spread spectrum techniques, statistical methods, distortion techniques, and cover generation methods. Johnson survey neither talks about the history of steganography nor its applications.Johnson work has not included test images that can allow readers visualize the concepts.

Creighton T. R. Hager worked on the Performance and Energy Efficiency of Block Ciphers in Personal Digital Assistants [3]: The author has performed a comparative analysis of various encryption algorithms on various kinds of data. This research has proved that blowfish outperforms all other encryption algorithms. Blowfish is the best, unbreakable and fast encryption algorithm than others. Gary C.Kessler has written an Overview of Cryptography: Cryptographic [3]: This is an old published paper on cryptography by Gary C. Kessler, and since then it was continuously updated till date. It was last updated in 2014. The author suggested the great source for the cryptography algorithms again. It is very important to understand the encryption algorithm structure before putting it in the use.

Navita Agarwal et al. have developed Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography [1]: The authors have conducted a similar research, where they have applied compression, encryption and steganography on the digital image data. Pixel shuffling based symmetric encryption algorithm, DCT for compression, WinRAR to Image steganography are used to achieve the proposed model in this paper.

## PROBLEM DOMAIN

For Security of sensitive or secret image, researchers have been presented many kinds of digital image encryption techniques and all the techniques are working to keep the secret content of image from accessing of all unauthorized users. For the protection of transmitted image over network many techniques have been proposed including chaos based system, key generation based encryption algorithms, etc. Problem domain of the project is that, in existing system encryption is done by generated key then this key is stored somewhere to remember. Here level of security decreases because stored key can be stolen easily. In previous research key is given manually and this key has to be remembered. To address this problem we have used images to generate secure key. Here meaningful images are given as input and after processing these images key is generated which need not to remember or stored. As compared to existing system henon chaotic map algorithm for encryption is stronger because of its unpredictable and random nature.

## SOLUTION DOMAIN:

Our work contains four different modules i.e. Steganography, Cryptography, Secure Key generation and Watermarking. Here analysis of proposed Image Security Mechanism will be done and after that all four modules will be analyzed individually.

we have proposed image security mechanism which will combine Steganography, Cryptography, Secure Key Generation and Watermarking techniques to make image more secure. Three meaningful images are taken and processed to generate key. This key will be further utilized for cryptography (Encryption at sender‟s end). To generate this key, grayscaling, halftoning, thresholding and chaos sequence generation processes are applied.

Output of these processes will be a numeric key. This key will be used to encrypt the Secret Image. After encryption output will be a noisy image or meaningless image. This noisy image will be steganographed (hide) inside a carrier image. A manual stego-key will be used for steganography. This carrier image along with the stego-key will be sent to receiver. Receiver will also require three meaningful images for generation of secret key. To make these meaningful images more secure, these meaningful images will be watermarked and sent to the receiver using separate channel.

## PROPOSED ALGORITHM

### Algorithm for Proposed Image Security Mechanism

### Algorithm at Sender's end

i. Load three images

ii. Process these images to generate Secure Key

iii. Watermark these three images and send it to receiver.

iv. Encrypt Secret Image using generated secure key

v. Apply Steganography on encrypted image.

vi. Hide encrypted image inside a carrier image using Stego-Key

vii. Send Stego-Image and Stego-Key to receiver.

### Algorithm at Receiver End

i. Load carrier image

ii. Apply de-steganography on carrier image using shared Stego-Key

iii. Output of above step will be a de-steganographed image.

iv. Load three Watermarked images which was shared separately

v. Verify these watermarked images

vi. If watermark verification is success then load verified images

vii. Process verified images to generate secure key

viii. Decrypt de-Steganographed image (generated at step iii) using generated secure key

ix. Output will be the Secret Image.

## Class Diagram for proposed Image Security Mechanism

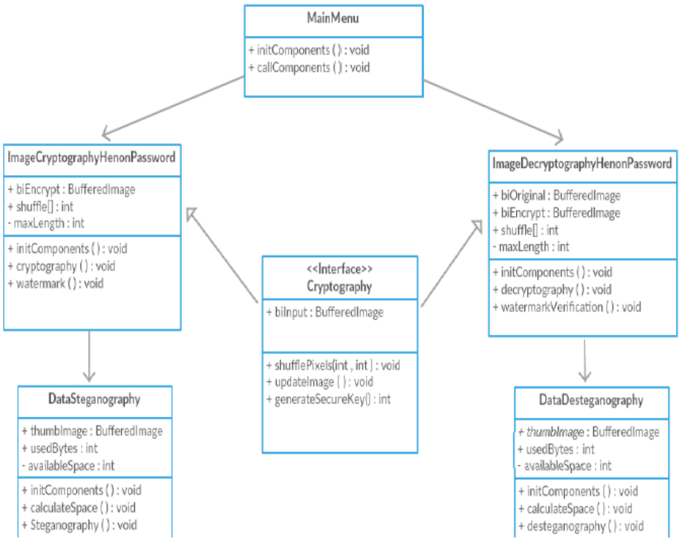

MainMenu
+ initComponents ( ) : void
+ callComponents ( ) : void
ImageCryptographyHenonPassword
+ biEncrypt : BufferedImage
+ shuffle[] : int
- maxLength : int
+ initComponents ( ) : void
+ cryptography ( ) : void
+ watermark ( ) : void
<<Interface>>
Cryptography
+ biInput : BufferedImage
+ shufflePixels(int , int ) : void
+ updateImage ( ) : void
+ generateSecureKey() : int
ImageDecryptographyHenonPassword
+ biOriginal : BufferedImage
+ biEncrypt : BufferedImage
+ shuffle[] : int
- maxLength : int
+ initComponents ( ) : void
+ decryptography ( ) : void
+ watermarkVerification ( ) : void
DataSteganography
+ thumbImage : BufferedImage
+ usedBytes : int
- availableSpace : int
+ initComponents ( ) : void
+ calculateSpace ( ) : void
+ Steganography ( ) : void
DataDesteganography
+ thumbImage : BufferedImage
+ usedBytes : int
- availableSpace : int
+ initComponents ( ) : void
+ calculateSpace ( ) : void
+ desteganography ( ) : void

Figure 1: Class Diagram for Proposed Image Security Mechanism

## Algorithm for Cryptography

## Algorithm for Encryption

i Load secret image as input image.

ii Convert 2 - Dimensional image into 1 - Dimensional byte array.

iii Calculate new position of pixels with the help of α and β.

iv Use the values of α = 1.4 and β = 0.3

v New position of x = 1 + (old y) – (α * (old x2)).

vi New position of y = β * (old x).

vii Now add offset to new position.

viii To generate planned randomness [(New x) + Offset] & [(New y) + Offset]

ix Swap pixels with new position.

## Algorithm for Secure Key Generation

i. Load 3 images (shares)

ii. Apply Grayscale process

iii. Apply the process of halftoning and thresholding.

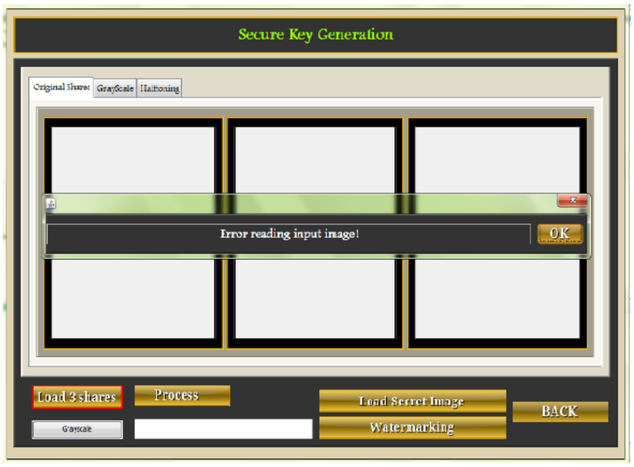
iv. Apply chaos sequence generator

v. Secure Key is generated.

## RESULTS ANALYSIS

Application is tested with various test cases described in below sections. After end to end testing of this application, results are analyzed and compared with existing system.

### Testing File Format of Input:

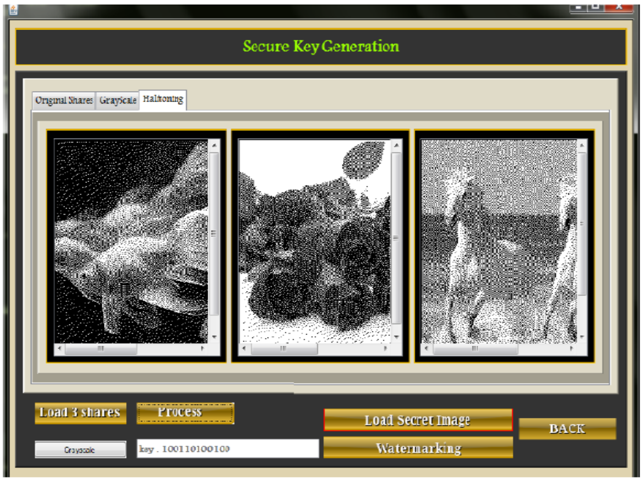


Error reading input image!

Figure 2: Testing File Format of Input

To generate secure Key 3 image files need to be loaded. In above figure the given input is word file therefore no input will be accepted and message will be displayed which is shown in above fig  And further no process will be done. In this condition no key will be generated.

### Key Generation By applying the process of Grayscale and Halftoning

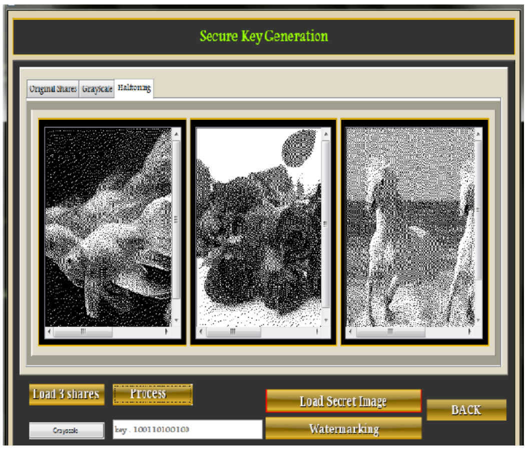


key . 100110100100

Figure 3: Key Generation by grayscale & Halftone (sender)

In above figure three images are loaded as input images and the process of grayscale and halftoning is applied on these images. The output of this processing is generated key i.e. 100110100100. The Generated key is in binary form. Key cannot be generated without input images.

### Generating key by using same images which were used at sender's end.



key . 100110100100

Figure 4: (At Receiver End) Key Generation with images used at sender end

At receiver end key generation process is done by using same images which were used at sender's end. Here the generated key is 100110100100 which is same as key generated at sender"s end. This generated key is correct.

### Modification Detected in Watermarked image:

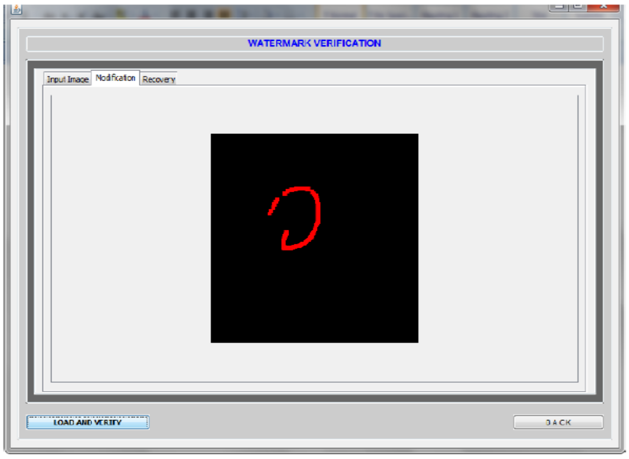


Figure 5: Modification Detected in Watermarked image

In above figure the changed pixels are highlighted in red color. With the help of watermark verification technique a modification in image can be detected easily.

## CONCLUSION

The communication technologies have major impact in this world hence to ensure security while transferring of information is important. In this thesis we have presented a new image security system in which combination of Steganography, watermarking and cryptography with secure key generation is used. And this proposed system could be proven as highly secured method for data communication in near future. Our proposed system focuses on generating key based on images. The generated key need not have to be stored. It can be generated just using three images. To provide high security to these key generating images, alpha watermarking technique is used. This technique watermarks the images and save those images in (.TGA) file format. These watermarked images cannot be accessed by anyone other than receiver. Here a new image encryption scheme using a chaotic method is presented. To make steganography process stronger, we have used alphanumeric key as stego key. This stego key makes the entire system more strong. The proposed High secured system using steganography, watermarking and cryptography with secure key is tested by encrypting secret image an and hiding it in carrier image. The results that are obtained from these experiments are recorded.

## FUTURE WORK

- Stegno key can be generated using some mechanism using images or other input to make secret image more secure.
- Output images can be stored in any format (jpg, bmp etc).

## REFERENCE

[1]. Kai-Hui Lee and Pei-Ling Chiu: “Digital Image Sharing by Diverse Image Media”, IEEE transactions on information forensics and security, vol. 9, no. 1, January 2014 PP: 88-98.

[2]. R.Nivedhitha, Dr.T.Meyyappan: “Image Security Using Steganography AndCryptographic Techniques”, International Journal of Engineering Trends and Technology- Volume3Issue3- 2012.

[3]. Parag Kadam, Mangesh Nawale, Akash Kandhare and Mukesh Patil: “Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique”, Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22.

[4]. Pye Pye Aung and Tun Min Naing: “A Novel Secure Combination Technique of Steganography and Cryptography”, International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No. 1, February 2014.

[5]. Ramesh Kumar yadava, Dr. B. K.singh, S.K.sinha, K. K.pandey: “A New Approach of Colour Image Encryption Based on Henon like Chaotic Map”, Journal of Information Engineering and Applications www.iiste.orgISSN 2224-5782 (print) ISSN 2225-0506 (online)Vol.3, No.6, 2013- Selected from International Conference on Recent Trends in Applied Sciences with Engineering Applications.

[6]. Manjunath Prasad and K.L.Sudha: “Chaos image encryption using pixel shuffling with henon map”, et al./ Elixir Elec. Engg. 38 (2011) 4492-4495

[7]. Souvik Roy1 and P. Venkateswaran: “Online Payment System using Steganography andVisual Cryptography”, 2014 IEEE Students‟ Conference on Electrical, Electronics and Computer Science.

[8]. Robert Ulichney: “A Review of Halftoning Techniques”, Cambridge Research Lab, Compaq Computer Corp., 1 Kendall Sq., Cambridge, MA 02139, USA.

[9]. Anuprita U. Mande, Manish N. Tibdewal: “Parameter Evaluation and Review of VariousError-Diffusion Half toning algorithms used inColor Visual Cryptography”, ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 8, February 2013.

[10]. Tun Hussein, Rosziati Ibrahim and Mohd. Najib: “Digital Watermarking Algorithm Using LSB”, 2014 International Conference on Computer Applications and Industrial Electronics (ICCAIE 2014), December 5-7, 2014, Kuala Lumpur, Malaysia.

[11]. http://www.academia.edu/4916694/Image_Encryption_Using_Henon_Chaotic_Map _with_ B yte_Sequence

[12]. Muhalim Mohamed Amin, Subariah Ibrahim, Mazleena Salleh and Mohd Rozi Katmin: “Information hiding using steganography”, Information Hiding using Steganography Approach, Vot 71847

[13]. http://www.naturalspublishing.com/files/published/964u6i11fz5kh7.pdf

[14]. https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ma485-watermarking.pdf

[15]. Miss. Apurva B. Parandekar, Prof. S.S.Dhande and Prof. H.R.Vhyawhare: “A Review on Changing Image from Grayscale to Color”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 1, January 2014

[16]. http://whatis.techtarget.com/definition/grayscale

[17]. http://www.dyclassroom.com/image-processing-project/how-to-convert-a-color-image-into-grayscale-image-in-java

[18]. Mr.M.Venkatesan, Mrs. P.MeenakshiDevi, Dr. K.Duraiswamy and Dr.K.Thyagarajah: “Secure Authentication Watermarking for Binary Images using Pattern Matching”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008