IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 11-16
www.iosrjournals.org

Enhanced Security with Steganography and Cryptography

Radha S. Phadte[1], Rachel Dhanaraj[2]

[1]*(Department of Computer Engineering, Goa College of Engineering, Goa India)*
[2]*(Department of Computer Engineering, Goa College of Engineering, Goa India)*

Abstract: *Steganography is an art of hiding secret information into another cover medium like image, audio, video. Cryptography is an art of converting plain data into unreadable format. Steganography can be integrated with Cryptography in order to enhance the security of data. In this paper, a new method is proposed that integrates Steganography and Cryptography for 24 bit color images. In this method, LSB based method is used to hide an image in another image. The resulting stego image is then encrypted using chaotic theory. This new integrated method ensures the enhancement in the data hiding capacity and the security of the image.*

Keywords: *Image, Steganography, Cryptography, Encryption, Decryption, Data hiding, Security*.

I. Introduction

There has been a tremendous development in the communication field in recent time. Hence the security and confidentiality of information has become a basic and important requirement for communication. With the rapid development of the Internet and multimedia techniques, we use digital data such as texts, images, videos, audios in our day to day life. Huge information can be transmitted via computer networks. However, the security of data over the internet is not up to the mark, and the data can be intercepted by an illegal or unauthorized user. Hence ensuring the Security and Confidentiality of data transmission is very important and current necessity. This requirement can be achieved by different techniques like Steganography and Cryptography [1].

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the secret data. However Cryptography scrambles data so that it becomes unreadable. Steganography hides the secret data so that it cannot be seen.

Cryptography systems can be broadly classified into two types. Symmetric-key systems in which a single key is used by both, the sender and the receiver, and Public-key systems in which two keys are used, a public key which is known to everyone and a private key which is known only to the recipient of messages. In Cryptography, a cipher data might create suspicion to the recipient while an invisible message created with steganographic methods will not. Steganography can be useful when the use of cryptography is risky or prohibited [2].

The study techniques for deciphering cipher messages is called as cryptanalysis and techniques for detecting hidden messages in the stego-media is called as steganalysis. The former refers to the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages. This paper is focusing on a method for combining together cryptography and steganography for images.

This paper is organized in five sections. Section I gives the introduction of this paper. Section II shows the survey of different existing methods of cryptography and steganography. Section III explains the proposed method. Section IV shows the implementation and results. Finally section V gives the conclusion of this paper.

II. Literature Review

There are various methods implemented in case of Steganography and Cryptography. Enhancements in these existing methods can be done after a review of such existing methods.

Authors in [5] proposed two methods of combined cryptography and steganography. In first method an image is secured by converting it into an encrypted form using S-DES algorithm and a secret key and then the encrypted image is concealed in another image. In the second method, an image is secured by encrypting it using S-DES algorithm and an image key. The resulting image is then concealed inside another image so as to hide its very existence. Both these techniques have been tested and it has been observed that they prevent the possibilities of steganalysis also.

Authors in [6] have proposed an improved LSB information hiding algorithm of color image using secret key, combining information hiding and cryptography, and the identity authentication based on digital signature and encryption technology to improve the security of information hiding. Authors have improved the randomness of the LSB embedding position, and encrypted the message which controls the embedded positions, so the hidden information cannot be extracted without the corresponding private key. In order to prevent the forgery of the hidden information, authors have also added a digital signature to authenticate only the right sender just to extract the hidden information.

Authors in [7], have proposed a hybrid approach which uses combination of image encryption and image hiding, to provide higher security. Image encryption is done using Blowfish Algorithm and for image hiding LSB technique is used.

Authors in [8], have proposed a method which is a combination of cryptography and steganography. The data is encrypted in the system using AES and it is embedded in the least significant bit (LSB) of randomly selected pixels of image. After that the stego image is split into fragments on the basis of various intensity of RGB color component of pixel. Then the split parts are encrypted and transmitted to the receiver. The sender informs the secret key to the receiver through email. The receiver extracts each image fragments and combines to form the stego image. Then the receiver decodes the secret data from the image. Thus the original image and secret data are received securely.

Authors in [9], have proposed an algorithm that encrypts the image using Henon Map which is a discrete time dynamic system which possesses all the properties of chaos. The image encryption algorithm is completed in two steps. The first step generates a chaotic sequence using Henon map. The second step encrypts each pixel of the plain image as a function of chaotic sequence generated in the first step.

Authors in [10], have proposed a new algorithm for symmetric encryption. This algorithm is based on the principle of chaotic confusion and diffusion, using chaotic sequences generated by one-dimensional chaotic applications, called logistic maps. This algorithm consists of several confusion rounds done by means of chaotic sequence and chaotic confusion keys KeyConf as well as two diffusion rounds that allow mixing properties of adjacent pixels with chaotic diffusion keys KeyDiff.

Authors in [11], have proposed a new encryption technique to encrypt the image. This method encrypts the image using Chaotic System and Wavelet Transform. The fingerprint of the image is also created using Hash Function which is to be transmitted to the receiver. This method along with the privacy also maintains integrity of the image.

Authors in [12], have proposed a new 2-D chaos based lossless image encryption method. This method is user key based encryption and decryption. It is based on series of confusion and diffusion processes guided by user key. Chaos is generated separately for red, green, and blue components of RGB image and after chaos generation encrypted image of R, G, and B components are placed at their respective places.

In the above survey, certain challenges are found. They can be summarized as:

1. The steganography methods incorporated the data hiding techniques that provide less embedding capacity.
2. The extraction of the secret data from stego-media do not ensure 100 percent recovery of the secret data.
3. The combined techniques of steganography and cryptography use traditional encryption algorithms which are not suitable for encryption of multimedia data.

III. Proposed Model

This system provides the enhanced method of steganography along with cryptography for images. This method proposes an improved LSB technique for color image steganography and uses chaotic theory for encryption of stego-image. The block diagram for the proposed method is shown in Fig. 1.

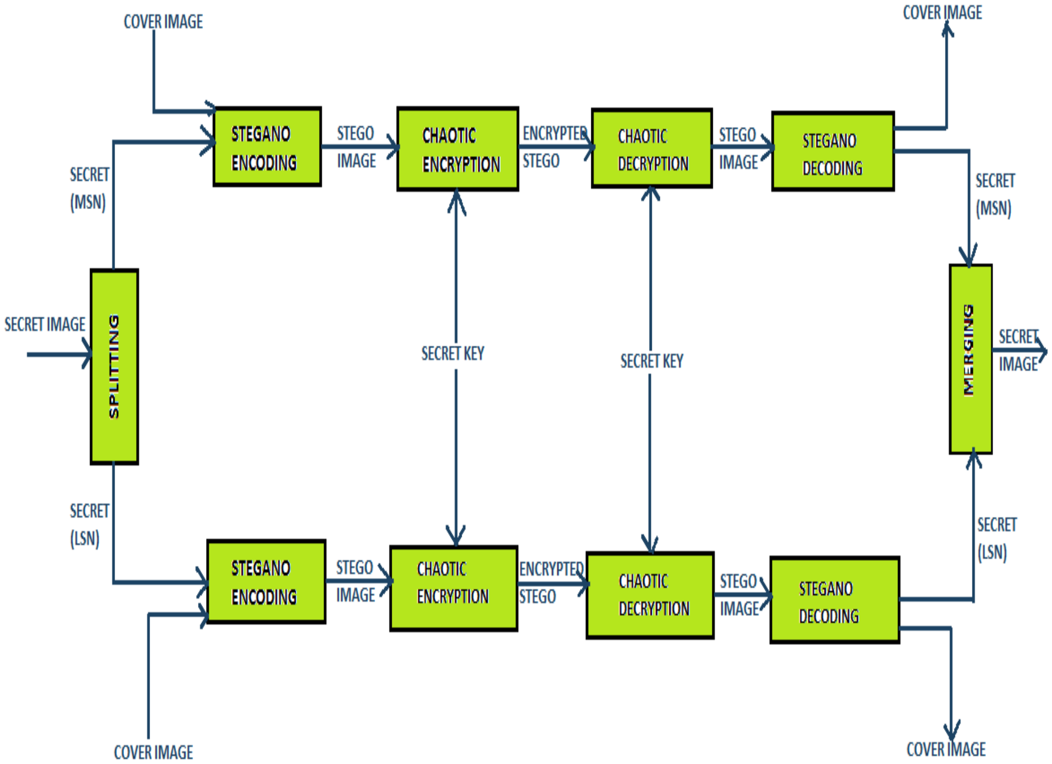

Fig 1. Block Diagram of Proposed Model

The proposed system has following six modules.

1. Splitting
2. Stegano Encoding
3. Chaotic Encryption
4. Chaotic Decryption
5. Stegano Decoding
6. Merging

In the first module, the 24 bit secret image is taken and split into three planes: Red, Green and Blue. Each plane is then split into two parts at bit level of each pixel. The two parts are named as Secret MSN (Most Significant Nibble) and Secret LSN (Least Significant Nibble). In the second module, two 24 bit cover images are chosen. Both secret MSN and secret LSN are embedded in two different cover images using 4-4-4 data hiding technique of steganography. In the third module, both the stego images are encrypted using chaotic theory and a secret key. Here the encryption is applied by number of confusion and diffusion rounds on stego images. Confusion is applied to shuffle the pixel positions of the stego images. Diffusion is applied to change the intensity values of pixels of stego images. Both the encrypted stego images are then transmitted from sender to receiver. In the fourth module, receiver decrypts both the images using reverse process and the same secret key. In the fifth module, secret MSN and secret LSN are extracted from both the stego images. In the sixth module, Secret MSN and secret LSN are merged together to obtain final secret image. A single secret key is used at sender as well as receiver. Sender informs the receiver about the key through email.

IV. Implementation and Results

The proposed model in this paper is implemented in modular way in Matlab. Both Secret image and cover images are of 24 bits. The size of secret image should be lesser than or equal to the size of cover image. The secret image is shown in Fig 2.

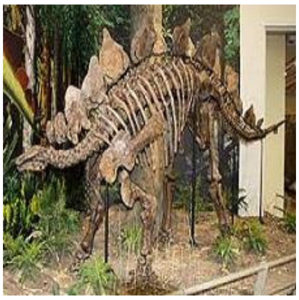

Fig 2 Secret Image

The output of the first module i.e. Splitting is shown in Fig. 3a to 3f.

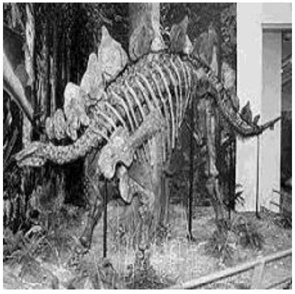

Fig. 3a. Secret Red MSN

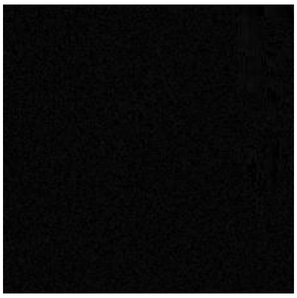

Fig 3b. Secret Red LSN

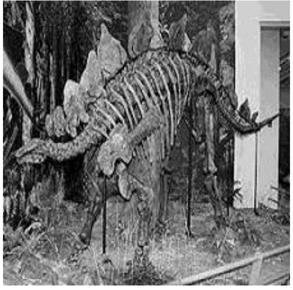

Fig.3c. Secret Green MSN

Fig.3d. Secret Green LSN

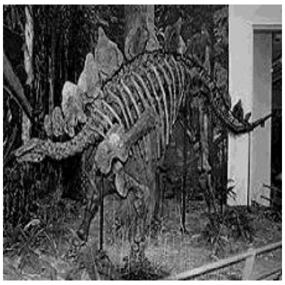

Fig.3e. Secret Blue MSN

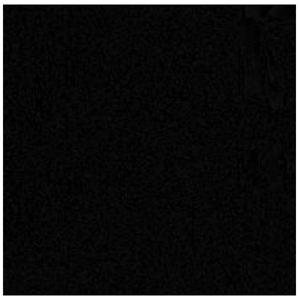

Fig.3f. Secret Blue LSN

In second module i.e. Stegano-Encoding two 24 bit cover images are taken which are shown in Fig. 4a and 4b.

Fig.4a. Cover Image 1

Fig.4b. Cover Image 2

In Stegano-Encoding both secret MSN and secret LSN are embedded in two different cover images using LSB based 4-4-4 data hiding technique of steganography. The output of this module are stego-images which are shown in Fig.5a and 5b.

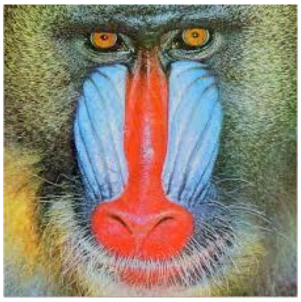

Fig.5a. Stego-Image 1

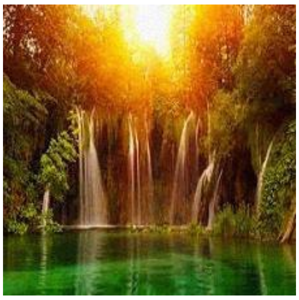

Fig.5b. Stego-Image 2

In the third module both the stego images are encrypted using chaotic confusion and diffusion. The output of this module is shown in Fig.6a and 6b.

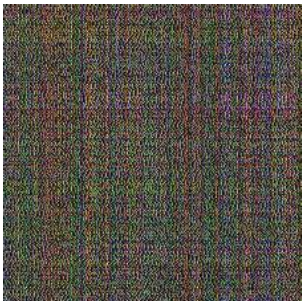

Fig.6a. Encrypted Stego 1

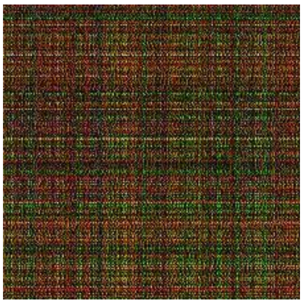

Fig.6b. Encrypted Stego 2

Both the encrypted stego images are then sent to the receiver. The receiver applies the reverse process in order to decrypt and extract the secret images i.e. secret MSN and secret LSN. Then both the secret parts are merged to get the final secret image. The final output obtained at the receiver side is shown in Fig. 7. The secret image is recovered at the receiver end without any data loss.

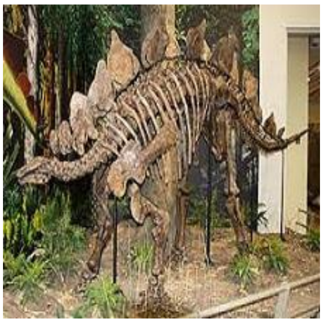

Fig.7 Secret Image

V. Conclusion

The focus of this paper is security and confidentiality of data. A new method of image steganography and cryptography is implemented in order to enhance the security and also the data embedding capacity of the image. An image is hidden inside another image with the help of 4-4-4 data hiding technique. Hence the embedding capacity of 24 bit image is improved as compared to that of existing LSB methods. The security of the image is further enhanced by implementing chaotic encryption of stego images. The method ensures the high security of the secret image as it is split into two parts and embedded in two different cover images. The two images are then sent separately over the network. If the intruder intercepts one image and tries to extract the secret data then he/she will be able to recover the data only partially. Hence this method enhances the data embedding capacity, ensures 100 percent recovery of secret data, and also ensures the security of data at three levels: Steganography, Cryptography, and Transmission by splitting.

References

[1] Shahzad Alam, S M Zakariya, M Q Rafiq, “Analysis of Modified LSB Approaches of Hiding Information in Digital Images”, *2013 5th International Conference on Computational Intelligence and Communication Networks, @ 2013 IEEE.*

[2] A. Joseph Raphael, Dr. V. Sundaram, “Cryptography and Steganography–A Survey”, *Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630*.

[3] Vipul Shanna, Madhusudan, “Two New Approaches for Image Steganography Using Cryptography”, *2015 Third International Conference on Image Information Processing, © 2015 IEEE.*

[4] Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin, “An Improved Method for LSB Based Color Image steganography Combined with Cryptography”, *copyright 2016 IEEE ICIS 2016, June 26-29, 2016, Okayama, Japan.*

[5] Moresh Mukhedkar, Prajkta Powar, Peter Gaikwad, “Secure non real time image encryption algorithm development using cryptography & Steganography”, *©2015 IEEE.*

[6] Jitha Raj.T, E.T Sivadasan, “Secure Transmission of Data by Splitting Image”, *2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India, ©2015 IEEE.*

[7] Joshi Rohit A, Joshi Sumit S, G. P. Bhole, “Improved Image Encryption Algorithm using Chaotic Map*”, International Journal of Computer Applications (0975 – 8887) Volume 32– No.9, October 2011.*

[8] Fadia TALEB, “A New Chaos Based Image Encryption Scheme Using Chaotic Logistic Maps”, *©2014 IEEE.*

[9] Manish Mishra, Shraddha Pandit, “Image Encryption Technique Based on Chaotic System and Hash Function”, *2014 IEEE International Conference on Computer Communication and Systems(ICCCS '14), Feb 20-21, 2014, Chennai, INDIA, ©2014 IEEE.*

[10] Nikhil Debbarma, Lalita Kumari, Jagdish Lal Raheja, “2D Chaos Based Color Image Encryption Using Pseudorandom Key Generation”, *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 4, July – August 2013.*