ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

A Crypto- Steganography System for Double Tier Security

Yogita[1], Harjinder Singh[2]

Department of Electronics & Communication Engineering, University College of Engineering,

Punjabi University, Patiala, India[1]

Assistant Professor, Department of Electronics & Communication Engineering, University College of Engineering,

Punjabi University, Patiala, India[2]

Abstract: The two important aspects of security that deal with transmitting information through some medium like internet are cryptography and Steganography. Cryptography deals with hiding the contents of a message and Steganography deals with hiding the presence of a message. In this paper, image is encrypted by ElGamal Algorithm and then encrypted image hide in other image for double tier security. For hiding the encrypted Image Modified LSB technique is used. The Modified LSB technique has more capacity as compared to LSB technique. Also in this paper MSE and PSNR of proposed Algorithm are compared with existing algorithm.

Index Terms: ElGamal, Modified Least Significant bit (MLSB), Peak signal to Noise Ratio (PSNR), Mean Square Error (MSE), Encryption, Steganography.

I. INTRODUCTION

The popularity of internet and its technologies increases day by day and so are the threats to the security of our information transmitted through the internet. One of the reasons why the attackers become successful in intrusion is that they have an opportunity to read and comprehend most of the information from the system. Intruders may reveal the information to others, misuse or modify the information.

In order to provide security of data being accessed by unauthorized people [1,2], two important techniques cryptography and steganography are used. Both are well known and widely used methods in information security.

Steganography is an art and science of hiding information in some cover media. Steganography comes from the Greek origin, means "Concealed writing". The word 'Steganos' means "covered or protected" and 'graphie' means "writing" [3]. Steganography is thus; not only the art of information hiding, but also the art and science of hiding the fact that communication is even taking place. There are several techniques to conceal information inside cover image [4].

1. Spatial domain technique
2. Frequency domain technique

1. Spatial domain technique: These techniques manipulate the cover image bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes.

2. Frequency domain technique: The transform domain techniques embed the message in the frequency domain of the cover image.

Cryptography is a physical progression that scuttles information by postponement and substitution of content making it unreadable to anyone except the person proficient of unscrambling it [5]. Cryptography system can classified into two parts [6].

1. Symmetric Key Cryptography
2. Public Key Cryptography

1. Symmetric Key Cryptography: In symmetric key cryptography system sender and receiver share a single key which is used to encrypt and decrypt a message. It is also called secret key cryptography.

2. Public Key Cryptography: In public key cryptography there is pair of keys one is secret key and other is public key. In which one is used for encrypting the plain text, and the other is used for decrypting the cipher text.

The paper is organized as follow; section II starts with the Literature Survey and section III Starts with the proposed methodology in which block diagram, algorithm. Section IV illustrates the results in which work MSE and PSNR are compared with existing technique. The conclusion is drawn in section V.

II. LITERATURE REVIEW

In the literature, many techniques about data hiding have been proposed. Hashimet. Al [7] in this paper, both color and grayscale image of any size saved in Portable network graphics (PNG), Joint Photographic Experts group (jpg) can be encrypted & decrypted using a modification of the ElGamal cryptosystem Algorithm. However, the ElGamal cryptosystem security is based on the difficulty of finding discrete logarithms modulo a large prime, this modification gives better security over images because breaking this cryptosystem depends on solving discrete logarithm problem to get the private key (a) and knowing X. Therefore, figuring the private keys (a)and X much harder than figuring only (a). Therefore, this study suggests a modification of ElGamal cryptosystem over a primitive root of a large prime. This modification is applied on image to give more secure cryptosystem. This modification can

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

make the ElGamal cryptosystem is more immune against some attacks than before. That leads to an increase of the confidence in the security of using this modification.

Odehet. al [8], in this paper, a new steganography algorithm for Unicode language (Arabic). The algorithm employs some Arabic language characteristics which represent extension letters. Kashida letter is an optional property for any Arabic text and usually is not properly used. In their work this property is used to hide data and reduce the probability of suspicions. The algorithm first introduces four scenarios to add kashida letters. Then random concepts are employed for selecting one of the four scenarios for each round. Message Segmentation principles are also applied, enabling the sender to select more than one strategy for each block of message.

Piper et. al [9], basic cryptographic concepts and techniques are defined. The paper also describes various methods to hide the secret or confidential message in an original file so that it is unintelligible to an interceptor.

Rajyaguruet.al[10], in this paper user enters username, password and a key. A key is taken from automatic key generator device which generates a unique key after some specific time. After this the secret message and key is encrypted and encrypted message is embedded into cover image and stego image is produced.

Barhmtoshy et.al [11], in this paper the secret message is first compressed then the message is hashed and encrypted using encryption key. This method results in robust model and achieves two important principles of security i.e. privacy and authenticity.

In this paper, we took motivation from these papers and Crypto-Steganography system is proposed for double tier security.

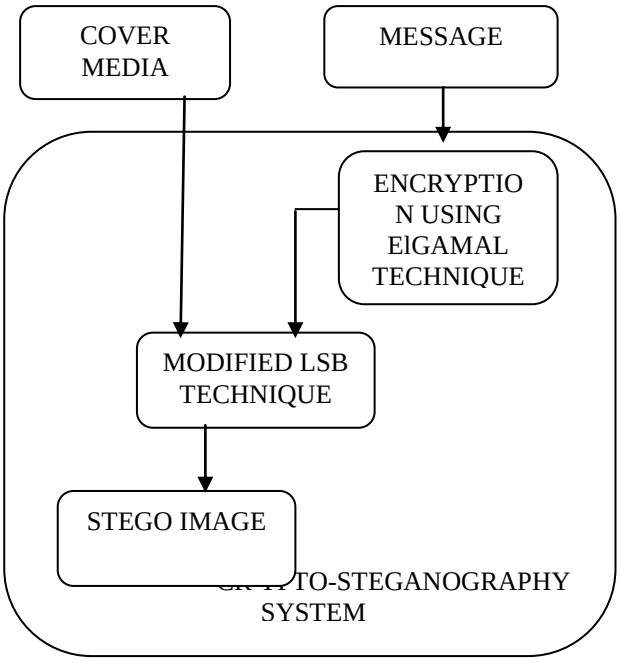
III. PROPOSED METHODOLOGY

In this section explanations of Crypto-Steganography System using ElGamal Cryptography and Modified LSB Steganography technique. The description of Transmitter block diagram as follows:

1. Cover Media: The Cover Media that will carry the message that is to be hidden. In this paper image taken as a Cover Media.
2. Message: A message can be anything like data, file or image etc. In this paper image taken as a message. The message is encrypted using ElGamal Cryptography Technique.

ELGAMALCRYPTOGRAPHY TECHNIQUE OVERVIEW

The ElGamal cryptosystem is a well- known cryptosystem, invented by T.ElGamal in 1985. Its security is based on the difficulty of finding discrete logarithms modulo a large prime. In the ElGamal cryptosystem, each person choose a very large prime number p, a primitive root r of p, and an integer a with $2 \leq a \leq p-2$. This integer a is the private key that must be kept secret by that person, and the corresponding public key is (r, s, p) such that, $s \equiv r\ a \pmod p$. The message M can be encrypted to the pair (x,y) such that $x \equiv r\ k \pmod p$ and $y \equiv (m * sk) \pmod p$. Then encrypted message (x,y) can be decrypted by $M \equiv [y((x)a)-1] \pmod p$. Breaking this cryptosystem depends on finding (a) which is a unsolvable conjuncture in mathematics called the discrete logarithm problem, because it needs thousands of years to find all the possible solutions of it. The ElGamal cryptosystem is well-known to be used in encrypting and decrypting texts, e-mails, files, images, frames etc [7].



PROPOSED BLOCK DIAGRAM OF CRYPTO-STEGANOGRAPHY SYSTEM

3. Stego Image: The Stego image is generated after hiding the message in cover image using Modified LSB technique.

MODIFIED LSB TECHNIQUE OVERVIEW

In Modified LSB technique the data bits hides in cover image LSB bits. For Example:

1. Cover Image Pixels:

Table 1

10101100	00110011	11001000	11110000
00010001	10001001	11001101	11101000

2. Message Bits: 11000110
3. Stego Image Pixels:

Table 2

10101110	00110001	11001000	11110011
00010001	10001001	11001101	11101000

PROPOSED ALGORITHM

1. Read Cover and Data image.
2. Extract their information.
3. Apply ElGamal Cryptography technique on data for encryption.
4. Hide Encrypted data in cover image using Modified LSB Technique.
5. Calculate MSE and PSNR and compared with existing results.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

IV. SIMULATION RESULTS

In this paper we simulate Crypto-Steganography system using ElGamal and Modified LSB technique in MATLAB 2013. MATLAB, which stands for MATrix LABoratory, is a state-of-the-art mathematical software package, which is used extensively in both academia and industry. It is an interactive program for numerical computation and data visualization, which along with its programming capabilities provides a very useful tool for almost all areas of science and engineering. It is one of the leading software packages for numerical computation. The results of this algorithm as follows:

1. Cover Image: Read the cover image and extract their Red, Green and Blue plane as shown in figure 2.

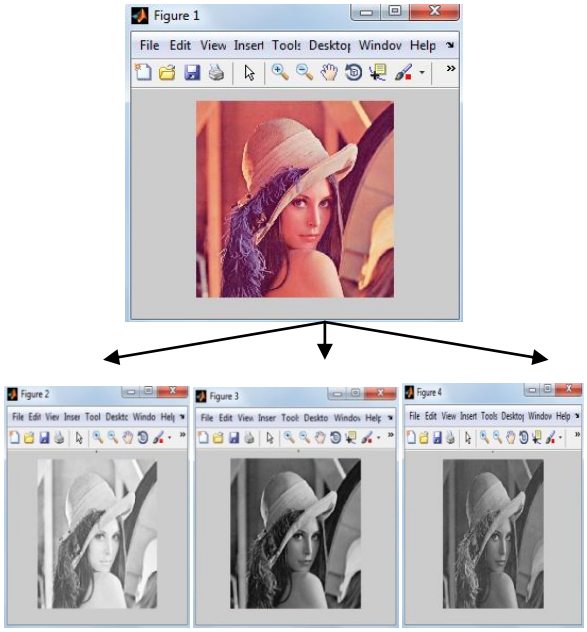
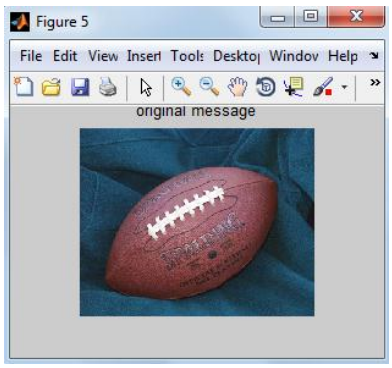


Figure 2: Cover Image and Their Planes

2. Data Image: Read the message image and extract their planes and after encryption using ElGamal Cryptography as shown in figure 3.



Message Image

To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar or different the stego image with the cover image is.

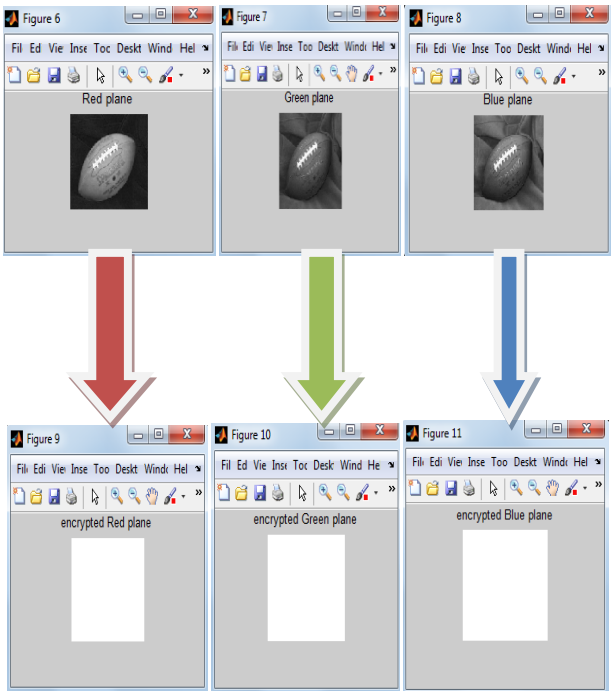


Figure 3: Data Image and their Planes and their Encrypted Planes

3. Stego Image: The Stego Image generated after hiding encrypted image in cover image using Modified LSB technique as shown in figure 4.

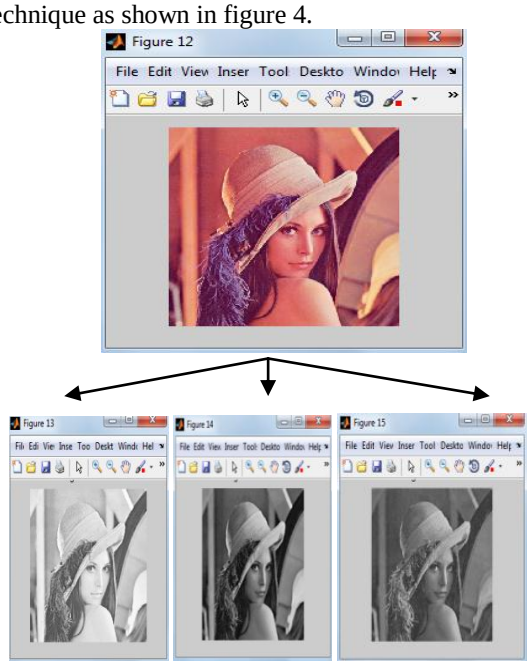


Figure 4: Stego Image and Their Different Planes

The following metrics are used:

1. Mean Squared Error (MSE) is computed by performing byte by byte comparisons of the cover image and stego image. The Computation expressed as[4]

$$MSE = \frac{1}{M*N}\sum_{1}^{M}\sum_{1}^{N}(Fij - Gij)^2$$

M: number of rows of cover image
N: number of columns of cover Image
Fij: Pixel value from cover image
Gij: Pixel value from Stego Image

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Higher value of MSE indicates dissimilarity between Cover image and Stego image.

2. Peak signal to noise ratio (PSNR) measures in decibels the quality of the stego image compared with the cover image. The higher the PSNR better the quality. PSNR is computed using the following equation [4].

$$PSNR=20\log_{10} Peak - 10\log_{10} MSE$$

Table 3

Cover and Data Image Information	
Cover: Lena.jpg	512*512
Data:Football.jpg	128*128

Table 4

Parameters	Existing Technique[4]	Proposed Technique
Mean Square Error	2.4	0.44
Peak Signal to Noise Ratio	44.1dB	47.68dB

V. CONCLUSION

In this Paper, Crypto-Steganography system is proposed for double tier security. In this paper, data first encrypted using ElGamal technique then hide using Modified LSB technique. This technique has better hiding capacity as compared to LSB and better MSE and PSNR as compared to existing MLSB technique.

REFERENCES

[1] B. Karthikeyan, Jagannathan Chakravarthy, Ramasubramanian "Amalgamation of Scanning paths and Modified Hill Cipher for Secure Steganography", Australian Journal of Basic and Applied Science, pp. 55-61, 2012.

[2] Md. Khalid Imam Rahmani, Kamiya Arora, Naina Pal, "A Crypto-Steganography: A Survey", International Journal of Advanced Computer Science and Application, vol. 5, pp. 149-154, 2014.

[3] GunjanChugh, RajkumarYadav, and Ravi Saini, "A new Image Steganographic Approach based on Mod Factor for RGB Images", International Journal of Signal Processing, Image Processing, and Pattern Recognition, vol. 7, pp. 27-44, 2014.

[4] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajnehand Sahel Alouneh, "FPGA hardware of the LSB Steganography",International Conference on Computer, Information and Telecommunication Systems (CITS), Pages 1-4, 2012.

[5] Napa Ram, RoushanRanjan, SreeparnaChakrabarti, "Application of data structure in the field of cryptography", International Journal of Innovative Technology and Research, pp. 65-68, 2015.

[6] Maulik P. Chaudhari, Sanjay R. Patel, "A Survey on Cryptography Algorithms", International Journal of Advance Research in Computer Science and Management Studies, vol. 2, pp. 100-104, March 2014.

[7] Hayder Raheem Hashim, Irtifaa Abdalkdum Neamaa, "Image Encryption and Decryption in a Modification of ELGamal Cryptosystem in MATLAB", International Journal of Science: Basic and Applied Research, vol. 14, pp. 141-147, 2014.

[8] Ammar Odeh, Khaled Elleithy, Maid Faezipour, "Steganography in Arabic Text using Kashida Variation Algorithm", IEEE conference on Long Island Systems, Application and Technology, pp. 1-6, May 2013.

[9] F. Piper, "Basic Principles of Cryptography", IEEE colloquium on public uses of cryptography, pp. 1-3, April 1996.

[10] Mihit H Rajyaguru, "Crystography-Combination of Cryptography and Steganography with Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, vol. 2, pp. 329-332, October 2012.

[11] H. Al-Barhmtoshy, E. Osman and M. Ezzaand, "A Novel Security Model Combining Cryptography and Steganography",Technical Report, pp. 483-490, 2004.