IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-3 E-ISSN: 2347-2693

Concealing Cipher Data using an Amalgam of Image Steganography and two-level Image Cryptography

Anirban Bhowmick[1*], Vishal Kapur[2] and Surya Teja Paladi[3]

Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal, India

anirban.bhowmick1993@gmail.com, vishalrkapur@gmail.com, suryateja2197@gmail.com

www.ijcseonline.org

Received: Mar/02/2015 Revised: Mar/08/2015 Accepted: Mar/22/2015 Published: Mar/06/2015

Abstract— With the mounting significance of data security over the network, steganography and cryptography are two emerging fields of research. Steganography is the technique in which confidential data is concealed in a cover medium. Cryptography is an approach of translating the personal data to some unintelligible form to keep it safe from intruders. Steganography and Cryptography attempt to accomplish identical objective of data security via different means. In this paper, the authors state a novel system to mask secret data. The confidential text is encrypted using modified Playfair cipher in the first step. In the second step, the cipher text is subjected to image steganography. In this step, the cipher text is embedded into the image using LSB encoding. To further enhance the concealment of the message, the image is subjected to a two-level simple but secure symmetric key encryption which comprises of two image encryption algorithms. These encryption algorithms use two pseudo random number generators that is Linear Congruential Generator and Blum Blum Shum algorithm.

Keywords— Modified Playfair cipher, Image Steganography, LSB encoding, Image Encryption, Linear Congruential Generator, Blum Blum Shub, Pseudo Random Number Generators.

I. INTRODUCTION

The growth of internet technology has resulted in constantly rising concern about the security of information transmitted over the network. A major challenge is to defend the confidentiality of secret data so that it cannot be misused. Information security is crucial in the period of electronic data exchange. When it comes to ensuring data confidentiality [1], one can use either cryptography or steganography. In the approach presented in this paper, an amalgamation of the two is used. This establishes superior safety of the secret information.

Playfair cipher [2] is an instance of substitution cipher [3]. The classical playfair cipher requires a 5x5 matrix. To enhance the security of the private text, the authors use an improved 6x6 playfair matrix [4]. The 6x6 matrix embraces all the alphabets together with the single digit numbers. In addition, the classical playfair cipher treats I and J as the same alphabet. The revised playfair matrix treats I and J as two dissimilar entities.

Image steganography is a process in which the confidential data is implanted into a cover image, with the secret message invisible to unlicensed users. There are three requirements for a steganographic system - perceptual transparency, hiding capacity and robustness [5]. After embedding the message, the stegno image is obtained. At the receiver's end the hidden data can be extracted from the stegno image using the reverse algorithm.

Cryptography aims at attaining security by encoding information to make them unreadable. It is a technique in which the information to be transmitted is transformed into an unreadable form to deliver secure communication even in the presence of third parties. There are two types of cryptographic systems [6]:

- Secret key cryptography or symmetric key cryptography
- Public key cryptography or asymmetric key Cryptography

A pseudo random number generator (PRNG) [7] is an algorithm which generates a sequence of random numbers. The random numbers generated exhibit two properties [3]

- Randomness: The two measures that authenticate that a sequence of numbers is random are uniform distribution and independence.
- Unpredictability: The possibility of predicting the subsequent number in the generated sequence should be minimal. A PRNG is said to be inefficient if the numbers generated have some kind of pattern to it or if the number to-be-generated next can be predicted.

The two pseudo random number algorithms used in this paper are Linear Congruential generator [8] and Blum Blum Shub [9].

The vulnerability of a cryptographic and steganographic system is exploited by cryptanalysis [10] [11] and

steganalysis [12] respectively. Cryptanalysis is the retrieval of original data without the knowledge of the key. Steganalysis is analogous to cryptanalysis. Steganalysis is accessing the hidden information by unauthorized entities. The gaining prominence of the above mentioned assaults has forced the researchers to take them into thoughtful attention while developing a secure algorithm.

The rest of the paper is divided into following sections. Section 2 highlights the existing work done in the field of steganography and cryptography. Section 3 delivers a thorough explanation of the algorithm suggested. Section 4 encompasses the results of this algorithm. Section 5 concludes the paper.

II. RELATED WORK

In [13], the authors have used 1D chaotic logistic map to produce a pseudo random sequence. The index values of the sorted pseudo random numbers are the positions used to implant the message in the cover image.

In [14], the authors have suggested a steganographic technique that combines both the spatial domain as well as the transform domain technique. The authors have picked LSB substitution technique for spatial domain implanting and Discrete Wavelet Transform for transform domain embedding. The authors also put forward a technique to combine cryptography with the proposed image steganography technique. The authors make use of the simplified DES algorithm for encryption.

Authors in [15] have proposed wavelet transform approach and LSB technique for screening data to achieve a new methodology for hiding an audio in an image. The LSB technique hides the secret message in the 8th bit plane of the cover data. Wavelet transform is used here for the compression of speech.

In [16], the authors have proposed an amalgamation of steganography and cryptography. In the first step the plaintext is transformed into cipher text using blowfish algorithm. The encrypted text is then concealed into a carrier image using LSB steganography.

Authors in [17] recommend a system to hide secret message into a cover image using Five Modulus Method. The secret message is concealed within a 5x5 window as a non-multiple of 5. The private key that is to be sent is the window size.

In [18], the authors have used AES algorithm to encrypt data and a part of the message is hidden in DCT of an image. The remaining part of the message is used to produce two keys to make the algorithm efficient.

Authors in [19] have used AES-128 to encode the message before it is implanted into image. After the message is encrypted then it is embedded in to image using Pseudo random numbers in LSB of image.

In [20], the authors have proposed system which uses edge adaptive image steganography that uses the amalgamations of chaotic cat mapping to deliver added security and matrix encoding and LSBM to embed the data in the image.

III. PROPOSED TECHNIQUE

A. First Phase – Data Encryption

The first phase of encryption involves encrypting the confidential data using modified Playfair cipher algorithm which makes use of a 6x6 Playfair matrix. The traditional playfair cipher had two major flaws.

- It treated I and J as a single alphabet which initiated ambiguity at the time of decipherment.
- Encryption of digits in the plain text was not possible owing to the deficiency of numbers in the playfair matrix.

The modified Playfair cipher system recommended in was able to overcome these imperfections.

Example

Original Text – MYBIRTHDATE16APRIL
Keyword – ENCRYPTION

E	N	C	R	Y	P
T	I	O	A	B	D
F	G	H	J	K	L
M	Q	S	U	V	W
X	Z	0	1	2	3
4	5	6	7	8	9

Table 1: Playfair Matrix

The digraphs obtained are
MY BI RT HD AT E1 6A PR IL
Cipher text, C = VEDOEALOBIRX7OEYDG

B. Second Phase – Image Steganography

In the proposed system, the next phase of data screening uses LSB encoding in which the encoded message (C) is implanted into an image. In this phase, each character of the encrypted message (C) is mined and the ASCII value of the character is used to generate the corresponding bit pattern. Each bit of this pattern replaces the last bit of the intensity value of a pixel. Each character is signified by an 8 bit binary number. Thereby, for each character, 8 consecutive

pixels will be obligatory. Further, the next character will be embedded in the next 8 pixels and so on.

Example
Character to be embedded: **Z**
ASCII value of Z: **90**
8 bit binary representation of the ASCII value: **01011010**
8 consecutive pixel values in binary format (consider 8 bit values)
10010101 10111101 10101000 01101110 00101110 10100000 01010101 10001101

Bit to be embedded	8 consecutive pixel values	
	Before embedding	After Embedding
0	10010101	1001010**0**
1	10111101	1011110**1**
0	10101000	1010100**0**
1	01101110	0110111**1**
1	00101110	0010111**1**
0	10100000	1010000**0**
1	01010101	0101010**1**
0	10001101	1000110**0**

The LSB encoding algorithm is presented below:

Algorithm: Embed the encrypted text message into the cover image

Input: Encrypted text, Cover image
Output: Stegno image
Initialize: i ← 0, j ← 0, k ← 0, S ← 0,
P ← pixel intensity values of the cover image,
1: **while** i < Length (encrypted text message) **do**
2: c ← Get the i^{th} character of encrypted text
3: ascii ← Get ASCII value of the character
4: bin ← Get binary pattern of ASCII
5: **while** j < Length (bin) **do**
6: pixbin ← Get the binary pattern of k^{th} pixel value in P
7: S [j] ← Store the last bit of pixbin
8: Replace the last bit of the image pixel intensity value with bin [j]
9: j ← j+1
10: k ← k+1
11: **end**
12: i ← i+1
13: **end**

C. Third Phase – Image Encryption

To further enhance the cover up of the secret text, the authors subject the stegno image to two-level secure encryption. The encryption algorithms use pseudo random numbers to carry out the encryption. The pseudo random number generators used are

- Linear Congruential Generator (LCG)

A linear congruential generator is an algorithm that produces a sequence of pseudo random numbers calculated with a discontinuous piecewise linear equation. A linear congruential generator takes the form

$$X_{n+1} = (aX_n + c) \bmod m$$

where X is the sequence of pseudorandom values. At each step of the LCG algorithm, some output is derived from X_{n+1}. Also, m is the modulus, a is the multiplier and c is the increment value. c and m should be relatively prime to attain a longer period.

Algorithm: Linear Congruential Generator Algorithm
Input: a, c, m, seed
Output: Sequence of pseudo random numbers
Initialize: Num ← (a*seed+c) mod m
1: **while** Num != 0 **and** Num is non repeating **do**
2: Used as the next number of the sequence
3: Num ← (a*Num + c) mod m
4: **end**

- Blum Blum Shub (BBS)

Blum Blum Shub is a pseudorandom number generator proposed in 1986 by Lenore Blum, Manuel Blum and Michael Shub. Blum Blum Shub takes the form

$$Xn+1 = X_n^2 \bmod M$$

where M is the product of two large primes p and q. The output at each iteration is derived from X_{n+1}. The initial seed X_0 should be an integer that is co-prime to M and not 1 or 0.

Algorithm: Blum Blum Shub Algorithm
Input: p, q, seed
Output: Sequence of pseudo random numbers
Initialize: M ← p x q, Num ← (seed x seed) mod M
1: **while** Num != 0 **and** Num is non repeating **do**
2: Used as the next number of the sequence
3: Num ← (Num x Num) mod M
4: **end**

As discussed previously, the authors subject the stegno image to two-level encryption for improved resistance to security attacks. The first step involves encryption initiated by transposition in which the positions of the pixels are altered generating a scrambled image. This scrambling is carried out by the random numbers generated by LCG algorithm. Initially, the columns are permuted followed by the permutation of the rows. In the first step of this encryption, each column is traversed and swapped with another; the latter's number being picked by the random number generated at that instant and restricting its

magnitude to the width of the image, making use of the modulus operation. While permuting the rows, the same approach is used but this time the magnitude of the random number is less than the height of the image. At the end of the first step, an intermediary cipher image is generated.

Algorithm: Permutation based Encryption
Input: Stegno image, sequence of random numbers
Output: Intermediary cipher image
Initialize: k ← 0
1: **while** k < (width of the image) **do**
2: Obtain pixel value of each pixel in the k^{th} column
3: Obtain pixel value of each pixel in a column, the column number depending on the random number generated at that instance.
4: Swap pixel results obtained in STEP 3 and STEP 4
5: k ← k+1
6: **end**
7: k ← 0
8: **while** k < (height of the image) **do**
9: Obtain pixel value of each pixel in the k^{th} row
10: Obtain pixel value of each pixel in a row, the row number depending on the random number generated at that instance.
11: Swap pixel results obtained in STEP 9 and STEP 10
12: k ← k+1
13: **end**

The second step encompasses substituting the pixel intensities. The random numbers generated at each instant by the BBS algorithm is XORed with each pixel of the intermediary cipher image. The magnitude of the random number used in this case should not me more than 255. This produces the final cipher image in which correlation coefficients of pixels are low.

Algorithm: Substitution based Encryption
Input: Intermediary cipher image, sequence of random numbers
Output: Final cipher image
Initialize: k ← 0
1: **while** k < (width x height of the image) **do**
2: Obtain pixel value of the k^{th} pixel
3: XOR the pixel value obtained in STEP 2 with the random number generated at that instance
4: Place the result of STEP 3 in the corresponding pixel position
5: k ← k+1
6: **end**

IV. RESULTS

This division highlights the original image, the stegno image and the encrypted images. The authors have subjected the proposed algorithm on two images to examine the appropriateness and efficiency of the proposed algorithm. The results obtained at each step have been presented in this section.

A. Test Case 1

The secret text used and the cipher text generated, after subjecting the plain text to enhanced playfair cipher, is shown in Table 1.

Original Text	THEQUICKBROWNFOX
Key	JUMPED
Encrypted Text	XCDOJKBLASW2VNQW

Table 1: Original and Encrypted Texts

The encrypted text is then embedded into the original image to attain the stegno image. The stegno image is further subjected to permutation and substitution based encryption to further enhance the security.


Fig 1: Original Image


Fig 2: Stegno Image

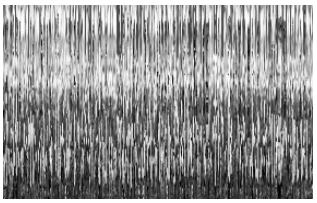
Fig 3: Row Column Distorted Image

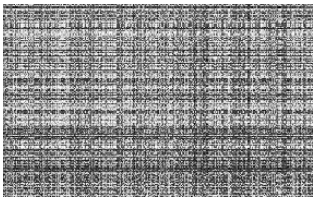
Fig 4: Intermediary Cipher Image

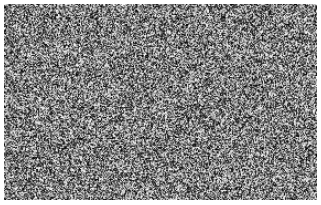
Fig 5: Final Cipher Image

B. Test Case 2

The secret text used and the cipher text generated, after subjecting the plain text to enhanced playfair cipher, is shown in Table 2.

Original Text	NETWORKSECURITY9
Key	HACK123
Encrypted Text	MFQZLUCTMEVSFV16

Table 2: Original and Encrypted Texts

The encrypted text is then embedded into the original image to attain the stegno image. The stegno image is further subjected to permutation and substitution based encryption to further enhance the security.

Fig 6: Original Image

Fig 7: Stegno Image

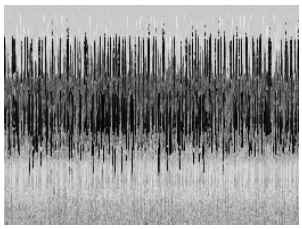

Fig 8: Row Column Distorted Image

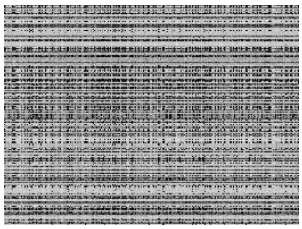

Fig 9: Intermediary Cipher Image

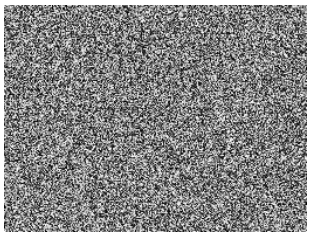

Fig 10: Final Cipher Image

V. CONCLUSION AND FUTRE WORK

Secure communication is a vital prerequisite. This can be attained by obscuring the secret data. In this work, the authors have concealed the secret data in an image after subjecting it to encryption. To enhance the data security, the stegno image is subjected to two phase encryption. This amalgamation of cryptography and steganography certifies that even if the image is intercepted by an unauthorized entity, the individual doesn't discover the secret data.

The variance in the original image, the stego image and encrypted image has been presented in Section 4. The lack of difference between the two figures verifies that there is no alteration in the image file caused by the embedded text.

The only blemish in the proposed algorithm is observed when the number of characters in the plaintext exceeds the number of pixels available in the cover image to conceal those characters. This necessitates appropriate selection of the cover image to screen those characters but this can increase the time complexity of the proposed scheme.

As a part of future work, the authors recommend more secure data encryption algorithms to be employed like AES and DES. Further, different steganographic techniques can also be employed.

VI. REFERENCES

[1] Behrouz A. Forouzan, "Cryptography and Network Security" special Indian Edition 2007, Tata McGraw-Hill Publishing Company Limited, New Delhi

[2] Derek Bruff, Ph.D, The Playfair Cipher Revealed Wynne MLAS 280-07 Cryptography July 13, 2009

[3] William Stallings," Cryptography and Network Security", 5th Edition

[4] Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya, P. Komuraiah, "An Extension to Traditional Playfair Cryptographic Method", International Journal of Computer Applications (0975 – 8887)Volume 17– No.5, March 2011

[5] S. Das, B. Bandyopadhyay and S. Sanyal, "Steganography and Steganalysis: different approaches", Cornell University Library, 2011

[6] Ayushi, "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Applications (09758887) Volume 1 – No. 15

[7] "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology, Special Publication 800-22 Revision 1a.

[8] An article on Linear Congruential Generator is available "http://en.wikipedia.org/wiki/Linear_congruential_generator".

[9] Nishith Sinha, Anirban Bhowmick, Kishore B, "Encrypted Information Hiding using Audio Steganography and Audio Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 112 – No. 5, February 2015

[10] M U Bokhari, Shadab Alam, Faheem Syeed Masoodi, "Cryptanalysis techniques for Stream Cipher: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 104 – No 15, October 2014

[11] Andrew S Tanenbaum, "Computer Networks", 4th Edition

[12] Yambem Jina Chanu, Kh. Manglem Singh, Themrichon Tuithung, "Image Steganography and Steganalysis: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 52– No.2, August 2012

[13] Shreenandan Kumar, Suman Kumari, Sucheta Patro, Tushar Shandilya, Anuja Kumar Acharya, "Image Steganography using Index based Chaotic Mapping", International Journal of Computer Applications (0975

– 8887) International Conference on Distributed Computing and Internet Technology (ICDCIT-2015)

[14] Saurabh V. Joshi Ajinkya A. Bokil Nikhil A. Jain Deepali Koshti, "Image Steganography Combination of Spatial and Frequency Domain", International Journal of Computer Applications (0975 – 8887) Volume 53– No.5, September 2012

[15] Nitin Kaul, Nikesh Bajaj, "Audio in Image Steganography based on Wavelet Transform", International Journal of Computer Applications (0975 – 8887) Volume 79 – No3, October 2013

[16] Ajit Singh, Swati Malik, "Securing Data by Using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013 ISSN: 2277 128X

[17] Firas A. Jassim, "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method", International Journal of Computer Applications (0975 – 8887) Volume 72– No.17, June 2013

[18] Dipti Kapoor Sarmah, Neha Bajpai, "Proposed System for Data Hiding Using Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887)Volume 8– No.9, October 2010

[19] Unik Lokhande, A. K. Gulve, "Steganography using Cryptography and Pseudo Random Numbers", International Journal of Computer Applications (0975 – 8887) Volume 96– No.19, June 2014

[20] V. Lokeswara Reddy, B. Sailendar, "Enhanced Chaos based Image Steganography using Edge Adaptive and Cat Mapping Techniques", International Journal of Computer Applications (0975 – 8887) Volume 104 – No 11, October 2014