International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-12 E-ISSN: 2347-2693

A Novel Approach on Adaptive Block Steganography Based Crypting Technique for Secure Message Passing

Sudipta Sahana[1*] and Abhipsa Kundu[2]

[1]*Computer Science and Engineering, JISCE, West Bengal University of Technology, India*
[2] *Computer Application, National Institute of Technology, Durgapur, India*

www.ijcseonline.org

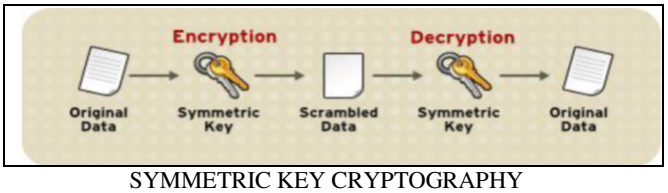
Received: Dec/01/2014 Revised: Dec/13/2014 Accepted: Dec/23/2014 Published: Dec/31/ 2014

***Abstract*—** The enhancement of using internet system has increased the ease of information communication which throws challenge in data security. Now a days harmless and safe data transmission become more vital and significant. Cryptography and Steganography are two important areas of exploration that comprise a great percentage of applications. Cryptography is the expertise technology that involves encoding a message text into an unreadable text form that is known as cipher text and the steganography is an art and technology of hiding information in a multimedia file without causing statistically significant change to this file for involving a secret message transmission. In our suggested work the plain text is converted to a cipher text using the method of Cryptography, where different person can able to use their preferable key for encoding the text and also some Boolean algebraic operations are used in the succeeding steps and after that this cipher text is buried inside a cover media of gray scale image with dimension of 2^n x 2^n and a secure pictorial block steganography based encryption algorithm is proposed for transferring text message and also revealed the Cryptanalysis and Steganalysis technique for regaining data at receiver side. The experimental outcome indicates that for using different length of text message the distortion of picture is very much less that is negligible in open eyes. At last it can be mentioned that without knowing the appropriate knowledge of cryptanalysis and steganalysis retrieving of message is quite impossible.

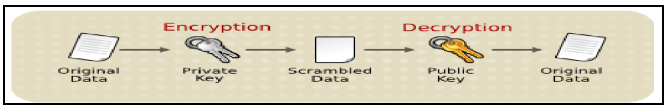
***Keywords*—** Cryptography, Steganography, Plain text, Cipher text, Cryptanalysis, Steganalysis

I. INTRODUCTION

Cryptography is generally a key enabling technology for protecting distributed systems. An encryption algorithm incomes the original message and a key, and modifies the original message scientifically based on the key to create a novel encrypted message. Similarly a decryption algorithm incomes an encrypted message and renovates it to its original form using one or more keys. There are two general concepts of cryptographic keys: Private key and public key system. When same key is use for encryption and decryption both purpose then this is identified as symmetric key encryption by using secret key. Where public-key encryption is also known as asymmetric-key encryption. The private key is recognized only to your computer, use for only encrypt the message while the public key is shared by computer to computer who wants to communicate securely with it.



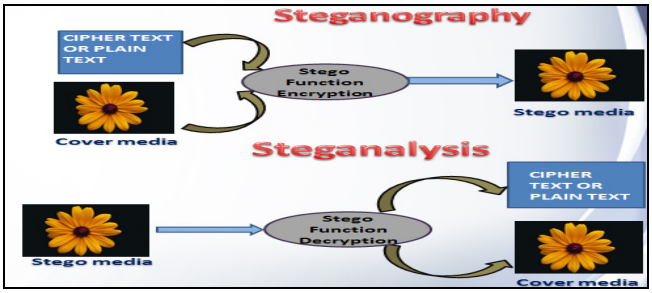
SYMMETRIC KEY CRYPTOGRAPHY



ASYMMETRIC KEY CRYPTOGRAPHY

In this paper, secure data transfer by using cryptography with Boolean algebra and key concept is focused where different body can use a particular mentioned length key that generally can't be guessed by a third person.

Steganography is the process of communication of secret data by using a multimedia carrier like image, video, audio or it also can be send by using an IP Datagram. Generally people cannot detect the secret communication of data. Message to be hidden is concealed in another file called cover media. Combination of secret message and cover file is called as – stego media. The stego function controls over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media.



Corresponding Author: *SUDIPTA SAHANA,*
ss.jisce@gmail.com

The paper is organized as follow. Section 2 describes the different types of steganography Techniques. In Section 3 section the algorithms of cryptography, steganography for data encryption technique on the other hand cryptanalysis and steganalysis for the decryption technique are discussed followed by an example in Section 4. Section 5 shows the Analysis Work. Finally, in Section 6 the conclusion of this paper is included.

II. RELATED WORK

In this section the past work related to the problem of hidden text in an image file is analyzed. A literature survey in this extent finds an amount of work is done in encrypting the text message and also decoding the text. Here the methodology and highlights of contributions, conventions is summarized.

In M. Bellare [1] formalized the new cryptographic primitive, Message-Locked Encryption (MLE), where the key under which encryption and decryption are accomplished is itself derived from the message. MLE delivers a method to reach secured duplication (space-efficient secure outsourced storage), an objective currently embattled by numerous cloud-storage providers. On the theoretical side the challenge is standard model explanations, and this technique makes

Rig Das et al. [2] performed the Huffman encoding upon the secret message /image and then embedded each of the encrypted bits, the size of Huffman encoded bit stream, Huffman table into the cover image by altering the least significant bit (LSB) of each of the pixels.

G.KarthigaiSeivi at al. [3] proposed a technique of finding the edge of the image using the Least-Significant-Bit (LSB) algorithm by employing Laplacian detector, and then data is hidden on center pixels whose blocks are located at the sharper edges.

Yam bernJina Chanu at al. [4] describes different types of steganography techniques for image in 3-D and transform dominions and steganalysis techniques for the revealing of secret message in the image in spatial domain by mentioning the strong points and weak points of the techniques.

In k. singla et al. [5] proposed a hash based Steganography approach for protected steganography using edge detection. The method accomplishes high implanting capacity and improves the eminence of the encoded image. This procedure first senses the edges in the image by well-known canny method and then the hash sort is used to embed the text data in to the edges of the color image. The hash function delivers a secure and fast method for image steganography.

InS.Malik, A. Sardana [6] proposed unique methodology A Keyless Approach to Image Encryption without the use of encryption keys. The core idea behind this technique employs Sieving, Separation and Shuffling to produce random portions such that with minimal computation, the original secret image can be recovered from the random portions without any loss of image quality.

Ali Daneshkha et al in his "A More Secure Steganography Method in Spatial Domain" [7] paper proposed a technique in which, the two bits of message is inserted in a pixel of image in a way that not only the Least Significant Bit (LSB) of picture component is allowed to change but also the second and fourth bit planes are allowed to be operated, but the idea is in every inserting process only one alternation in one bit plane is allowed to happen. It is compared by the technique LSB-Matching, the results shows this

S. Sarreshtedari et al. [8] proposed a great method for convert field image steganography and algorithm workings on the wavelet transform coefficients of the original image to embed the secret data by retaining integrity of the wavelet coefficients at high capacity embedding.

III. ALGORITHM

A. *Cryptography Algorithm:*

Password Matrix:

STEP-1: Different password can be chosen for different PT but always it will be reserved 8 characters length.

STEP 2: Transform every single character of the password into its corresponding ASCII value.

STEP 3: Convert each ASCII value into its 8 bit binary representation and place them in separate rows to generate a password matrix.

Generation of Auxiliary Keys :

STEP 4: For that purpose the diagonal elements of password matrix is chosen as the first auxiliary key AK1, beginning from bottom left corner bit to terminate in top right corner bit.

STEP 5: The second auxiliary password AK2 is generated by retaining the 0th bit of AK1 as the 0th bit of AK2 and doing XOR operation between the nth bit and (n+1)th bit of AK1 to obtain (n+1)th bit of AK2. And this process has further carry on for other AKs where from AK2 to AK3 and from AK(n) to AK(n+1) has been got.

STEP-6: The number of Auxiliary keys generated depends on the number of letters in the plain text.

Formation of Cipher Text:

STEP-7: Choose a plain text of variable length and calculate its length.

STEP-8: Change each character into its ASCII value and then into its equivalent 8 bit binary representation at the end arrange them as a matrix of nx8 where n is size of letters in plain text.

STEP-9:Perform bitwise XOR operation in between the binary values P1, P2, P3,…,Pn and the auxiliary keys AK1, AK2, AK3, ….,AKn respectively.

STEP-10: Complement the even position bits (column no. : 2, 4, 6, 8) of every row of the last transformed value.

STEP-11: Divide the last generated 8 bits values into 4 parts each part having 2 bits, numbering them 1,2,3,4 and now arrange them as 4,2,1,3.

STEP-12: 8 bits of each row of the matrix now has to be reversed.

STEP-13: At last get our Cipher text 8 bit binary representation and convert it to corresponding decimal value or the ASCII Value. This text will be transferred.

B. Steganography Algorithm:

In this paper we have considered a gray scale image first; where we can encrypt the cipher text (encrypted data after cryptography process). At first we calculate the length of the cipher text and converted the text into its corresponding ASCII value. The size of the gray scale image is 256x256.

STEP-1: Taken the ASCII value cipher text as an input.

STEP-2: Calculate the number of ASCII value of cipher text and stored it into a variable CT.

STEP-3: Taken a gray scale image with dimension of 2n x 2n.

STEP-4: Apply the partial BTB technique on this image with n x n size block matrix and each matrix Contain 2(n-m) x 2(n-m) (where, n = 2m) matrix size.

STEP-5: Calculate the number of ASCII value of cipher text and stored it into a variable CT.

STEP-6: Now convert the ASCII value of CT to its binary value of 8 digit and for getting '1' from the corresponding binary value of CT the image pixel value has been increased two and also for getting '0' this pixel value has been increase one.

STEP-7: Now check the number of digit in CT. If it is less than or equal to n then only the 1st block 1st bit placed into 1st image block (1,1 position),then 1st block 2nd bit placed into 2nd image block(1,1 position) thus the process will continue less than n (no. of character) or equal to n time.

STEP-8: If the no. of character is greater than n then the 8 bit greater positions will be considered or Then the n+1 character 1st block 1st bit placed into 1st image block(8,8 position), 1st block 2ndbit place into 2nd image block (8,8 position) such as 2n+1 character 1st block 1st bit placed into1st image block (16,16 position),1st block 2nd bit placed into 2nd image block(16,16 position),then for 3n+1 characters to 4n (24,24 positions) will be considered and for 4n+1 to 5n (32,32) positions will be considered.

STEP-9: This coded image will be transferred to the receiver side.

C. Steganalysis Algorithm:

At receiver side the reverse technique of the previous method has to be followed for decaying the image matrix and easily the text will be retrieve by the decryption algorithm.

STEP-1: At first we have taken the Stego image that is got from sender side and then collect the original cover image.

STEP-2: Compare both image and make a size of 256x256 matrix contained the differentiate value of these two images where most of the values are zero excepting some are 2s and 1s.

STEP-3: Neglect all those 0 values and arrange the others digits in a separate matrix whose size of column is 8. It is very imperative that the arrangement of the digits must not be hampered from the previous order.

STEP-4: After getting the new matrix the number of the row signifies the number of characters present in the CT.

STEP-5: Now replace the value of 2 with '1' and 1 with '0' and after that which matrix will be generated this is the 8 bit binary representation of our CT.

STEP-6: Now convert the binary value with the corresponding decimal value and got the ASCII value representation of CT.

D. Cryptanalysis Algorithm:

STEP-1: Generate the PASSWORD MATRIX that was described in the previous section 3.1.

STEP-2: As well as create the AUXILARY KEYS from password matrix maintain the same rule followed as 3.1.

STEP-3: Taken the ASCII value of Cipher text and convert them as 8 bit binary representation. Arrange the value of bits in nx8 matrix where n = size of CT.

0	1	0	1	0	0	1	1
0	1	1	1	0	1	1	0
0	1	0	1	0	1	0	0
0	1	1	1	1	0	1	1
0	1	0	1	1	0	1	0
(1)		(2)		(3)		(4)	

STEP-4: Reverse the each 8 bits values of every single row.

STEP-5: Divide the last generated 8 bits values into 4 parts each part having 2 bits, numbering them 4,2,1,3 and now arrange them as 1,2,3,4.

STEP-6: Complement the odd bits (column no.:1,3,5,7) of every row of the last transformed value.

STEP-7: Perform bitwise XOR operation in between the binary values of last transformed CT1, CT2, CT3,…,CTn and the auxiliary keys AK1, AK2, AK3, ….,AKn respectively And then got the original P1, P2, P3,….Pn.

IV. EXAMPLE:

A. Cryptography Algorithm:

Suppose our plain text is EARTH that has to be securely transferred to the receiver side

Password Matrix:

Suppose our 8 letter word password matrix is UNIVERSE=

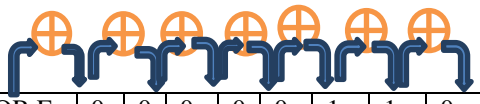
0	1	0	1	0	1	0	1
0	1	0	0	1	1	1	0
0	1	0	0	1	0	0	1
0	1	0	1	0	1	1	0
0	1	0	0	0	1	0	1
0	1	0	1	0	0	1	0
0	1	0	1	0	0	1	1
0	1	0	0	0	1	0	1

a. 8 Bit Binary Representation.

As per mentioning in the algorithm for 5 letters plain text 5 auxiliary key will be formed at first.

Auxiliary Key Formation:

After taking bottom left corner to top right corner diagonally elements we will get 01000011. That is AK1



AK1 XOR E	0	0	0	0	0	1	1	0
AK2 XOR A	0	0	1	0	0	0	1	1
AK3 XOR R	0	0	0	0	0	0	0	1
AK4 XOR T	0	0	1	0	1	1	1	0
AK5 XOR H	0	0	0	0	1	1	1	1

AK1	0	1	0	0	0	0	1	1

AK2	0	1	1	0	0	0	1	0
AK3	0	1	0	1	0	0	1	1
AK4	0	1	1	1	1	0	1	0
AK5	0	1	0	0	0	1	1	1

b. Formation of auxiliary keys

c. 8 bits representation of plain text

d. perform XOR operation between AKs with plain text

e. complement even bit position

1	1	0	1	0	1	0	0
1	0	1	1	0	1	0	1
0	0	0	1	0	1	0	1
1	1	1	1	0	1	1	0
1	0	0	1	0	1	1	0
(4)		(2)		(1)		(3)	

f. Rearrangement of columns

0	0	1	0	1	0	1	1	= 43
1	0	1	0	1	1	0	1	= 173
1	0	1	0	1	0	0	0	= 168
0	1	1	0	1	1	1	1	= 111
0	1	1	0	1	0	0	1	= 105

g. Reverse Each 8 bits of every Row

B. Steganography Algorithm:

Consider n = 8 and m = 3. The ASCII value representation of the Cipher text is

43	173	168	111	105

0	0	1	0	1	0	1	1
1	0	1	0	1	1	0	1
1	0	1	0	1	0	0	0
0	1	1	0	1	1	1	1
0	1	1	0	1	0	0	1

8 bit Binary value representation.

We have reserved a 256 x 256 size of gray scale image for hiding the bit representation of cipher text, as the distortion of gray scale image is very much less than color image so it is considered.

1	1	0	1	0	1	0	0
1	0	1	1	0	1	0	1
0	0	0	1	0	1	0	1
1	1	1	1	0	1	1	0
1 (4)	0	0 (2)	1	0 (1)	1	1 (3)	0

0	1	0	1	0	0	1	1
0	1	1	1	0	1	1	0
0	1	0	1	0	1	0	0
0	1	1	1	1	0	1	1
0 (1)	1	0 (2)	1	1 (3)	0	1 (4)	0

n_{00}	n_{01}	.....	n_{030}	n_{031}
n_{10}	n_{11}	.....	n_{130}	n_{131}
. . . . .	.....	. . . . .		
. . . . .	.....	. . . . .		
n_{300}	n_{301}	.....	n_{3030}	n_{3031}
n_{310}	n_{311}	.....	n_{3130}	n_{3131}

At first we will decompose this image at 8X8 matrix, where each cell of 8X8 matrix will consist 32x32 size of matrix.

N_{00}	N_{01}	N_{02}	N_{03}	N_{04}	N_{05}	N_{06}	N_{07}
N_{10}	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}
N_{20}	N_{21}	N_{22}	N_{23}	N_{24}	N_{25}	N_{26}	N_{27}
N_{30}	N_{31}	N_{32}	N_{33}	N_{34}	N_{35}	N_{36}	N_{37}
N_{40}	N_{41}	N_{42}	N_{43}	N_{44}	N_{45}	N_{46}	N_{47}
N_{50}	N_{51}	N_{52}	N_{53}	N_{54}	N_{55}	N_{56}	N_{57}
N_{60}	N_{61}	N_{62}	N_{63}	N_{64}	N_{65}	N_{66}	N_{67}
N_{70}	N_{71}	N_{72}	N_{73}	N_{74}	N_{75}	N_{76}	N_{77}

Suppose the value of n_{11} of N_{00} is 123, N_{01} is 231, N_{02} is 19 …… and N_{20} is 127, N_{21} is 34….N_{40} is 111 likewise N_{47} is 23.

Then after inserting those bits value the value of n_{00} of N_{00} will be 124 as the bit is 0, N_{01} will be 232 N_{02} will be 21 as the bit is 1, likewise the value of n_{00} of N_{40} will be 112 and N_{47} will be 25.

C. Steganalysis Algorithm:

We have compared the cover image with the stego image and getting values 2 and 1 we replaced 2 with 1 and 1 with 0. Arranged them in a matrix containing 8 columns and rows of plain text string size (here 5). This is the binary matrix representation of our cipher text.

D. Cryptanalysis Algorithm:

At first we will create the 5 auxiliary keys using the foregoing algorithm from the same Password that was UNIVERSE.

Now, we have already got our 8 bit representation of cipher text from the image.

0	0	1	0	1	0	1	1
1	0	1	0	1	1	0	1
1	0	1	0	1	0	0	0
0	1	1	0	1	1	1	1
0	1	1	0	1	0	0	1

h. 8 bit representation of cipher text

i. Reverse of each 8 bit of each row

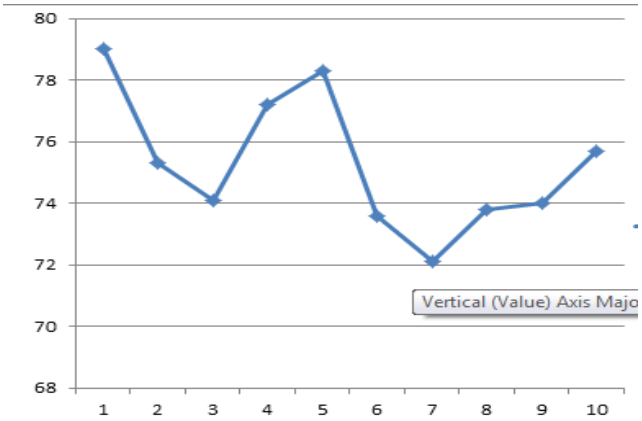
j. Rearrangement of each 8 bit of each row.

0	0	0	0	0	1	1	0	= AK1 XOR ?
0	0	1	0	0	0	1	1	= AK2 XOR ?
0	0	0	0	0	0	0	1	= AK3 XOR ?
0	0	1	0	1	1	1	0	= AK4 XOR ?
0	0	0	0	1	1	1	1	= AK5 XOR ?

k. Compliment even position bits of every row.

V. WORK ANALYSIS:

After undertaking some experimentation with different plain text into the same cover image we have acquired different stego images but the variance between the two images in every cases is negligible in open eyes. After receiving the PSNR value of each case we have got a graph that is:



Graph of PSNR (peak signal to noise ratio).Values on a single image for different plain texts.

VI. CONCLUSION

In this paper; a new method of utilizing the concept of cryptography and steganography together is proposed.

Cryptography prominences in preserving the contents of a message as a secret to an unreadable format and on the other hand the steganography stretches the attentions on shielding the existence of a message to be secret that cannot be exposed by a third party without having the knowledge of the both cryptanalysis and steganalysis algorithm. The new algorithm is more efficient as the text is not the original message but it is the cipher text and also it is hidden within the image without any deformation of the image. In this suggested method a secret key for transforming the plain text to cipher text is used. The new approach can be available to use on any type of 8 bit ASCII character which helps the proposed work for universal adoptability.

REFERENCES

[1] Thomas Ristenpart , and Sriram Keelveedhi , Mihir Bellareand, "Message-Locked Encryption and Secure Deduplication", Eurocrypt 2013, Volume 7881, 2013, pp 296-312

[2] RigDas , ThemrichonTuithung "A Novel Steganography Method for Image Based on Huffman Encoding", 2012 IEEE

[3] G.KarthigaiSeivi, Leon Mariadhasan, K. L. Shunmuganathan ,"Steganography Using Edge Adaptive Image", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]

[4] Themrichon Tuithung, Yam bern Jina Chanu and Kh. Manglem Singh, "A Short Survey on Image Steganography and Steganalysis Techniques", 2012 IEEE

[5] Sumeetkar and kirtikaSingla "Hash Based Approach For Secure Image Steganography Using Canny Edge Detection Method", ISSN-0973-7391, Vol. 3, Number 1, January-June 2012, pp. 155-157.

[6] Anjali Sardana, Siddhartha Malik, "A Keyless Approach to Image Encryption", IEEE, International Conference on Communication Systems and Network Technologies 2012.

[7] Hassan Aghaeinia , Seyed Hamed Seyedi, and Ali Daneshkhah, "A More Secure Steganography Method in Spatial Domain", Second International Conference on Intelligent Systems, Modelling and Simulation, 2011.

[8] S. Ghaemmaghami, S. Sarreshtedari , "High Capacity Image Steganography in Wavelet Domain," International Conference on Consumer Communications and Networking,pp.1-6, 2010.

AUTHORS PROFILE

SUDIPTA SAHANA is an assistant professor of a renowned engineering college of west Bengal. More than 3 years he has worked in this region. He has passed his M.tech degree in Software Engineering and B.Tech Degree in Information Technology from west Bengal university of technology with a great CGPA/DGPA on 2010 and 2012 respectively. He is recently work in Ph.D. on the domain of "security of cloud computing". He has made significant contributions to advancing the knowledge and understanding of computer networking and systems, evidenced by over 15 published works. He is a member of the Computer Science Teachers Association (CSTA), and also a member of International Association of Computer Science and Information Technology (IACSIT).

ABHIPSA KUNDU is a student of M.Tech in software engineering of National Institute of Technology, Durgapur. She has passed her B.Tech in Computer Science and Engineering degree on 2014 from West Bengal University of Technology with a great CGPA/DGPA. She had published her new planned work in 2 publications. She is recently worked in Big data analysis of cloud computing. She was selected for 1 year membership of British Council from 28th September 2013 to 28th September 2014. Her achievements was selected as the student topper of semester in college