Diagonal Block Steganography Based Enhanced Auxiliary Key Crypting for Secure Data Transfer

Sudipta Sahana, Abhipsa Kundu

Abstract— In the ever-increasingly related sphere, the necessity of collaborating data over the internet has full-grown noticeably. This data can be seized and modified so there needs to be secured process against fraudulent entree. Cryptography and Steganography are two vital parts of consideration that consist of a excessive proportion of applications. In cryptography, encryption is a serious security measure for guarding data secrecy, where the steganography is a skill and expertise technology of walloping information in a multimedia file without causing statistically momentous change to this file for concerning a secret message broadcast. In our recommended work the plain text is altered to a cipher text using the Cryptography process, where different person are capable to use their preferable sentence or word from where the method creates it different keys for encoding the text and furthermore some Boolean algebraic operations are used in the following steps and after that this cipher text is suppressed inside a cover media of image where the image type and size is not fixed, also exposed the Cryptanalysis and Steganalysis method for recovering data at receiver side.

Keywords- Cryptography, Steganography, Cryptanalysis, Steganalysis, Plain text, Cipher text.

I. INTRODUCTION

The quick evolutions of computer networks have permitted bulky files such as videos, images, texts all are transported over the intranet and internet. Data encryption is broadly used to provide guarantee in security & privacy of the data. For the use of encrypted data, we use private key as well as public key. In our example we have preferred a randomized word or sentence from this the key will automatically generated by the shadow of the algorithm that is the uniqueness of the proposed work where key is not directly supplied and also the key is not same for different appliers. After using the key concept other Boolean algebra operations are also used for creating the text more safe.

Steganography is the procedure of communication of secret data by consuming a multimedia file like image, video, audio or it also can be send by using an IP Datagram. Generally people cannot aware about the secret communication as the distortion of the multimedia carrier is negligible in open eyes.

Manuscript received Oct, 2014.

Sudipta Sahana, *Computer Science and Engineering JIS College Of Engineering, West Bengal University Of Technology , Kalyani, India, Phone/ Mobile No: 9474733974*

Abhipsa Kundu, *Software Engineering, National Institute of Technology, Durgapur, India, Phone/ Mobile No 9126680164.*

The media that is chosen for the hiding information is known as cover media and the combination of secret message and cover media is called as stego media. In this paper a image is used as a cover media image size can be neglected. The paper is systematized as follows in section 2 the similar work plan that was already proposed has discussed where in section 3 the algorithm of our planned work is discussed followed by section 4 with a suitable example. In section 5 describes the work analysis and the paper is concluded in section 6.

II. RELATED WORK

In Q.HUANG *et al*. [1] planned the problem in LSB Matching revisited (LSBMR) ALGORITHM to create regions assortment on images to invent fit zone. By calculating on each pixel it can be decided if it is secure or not. It can improve the visual imperceptibility and deplorability of the LSB matching method. By altering the parameters of the adjacent pixels, the max implanting capacity can be increased as needed.

In Piyu Tsai *et al.* [2] separated the image into blocks of 5x5, where the remaining image is considered using linear calculation. Then the secret data is entrenched into the residual values, followed by block renovation. Histogram-based data walloping is another commonly used data hiding scheme.

In S.Sahana *et al.*[3] divided an 256x256 size of gray scale image at the block of size 8x8 where each cell of 8x8 matrix contained 32x32 blocks and this inner cells are used for hiding the text which is an unreadable cipher generated by the using same and unique key followed by some boolea algebraic operation.

In Diaa Salama Abdul. Elminaam *et al.* [4] have related the several encryption algorithms with dissimilar settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed.

In A. Almohammad *et al.* [5] proposed the enactment of both color version and gray scale of a cover image when they are used with a specified Steganography process, capability and effect of using the chrominance constituents for data hiding. There are two Steganography approaches are used as test processes, JSteg and JMQT. As a Consequence, using color images is better than using gray scale images for data hiding.

In S.Sahana *et. al* [6] proposed an unique cryptography technique by using fixed length of user preferable key for data encrypting and this cipher text is hidden inside a gray scale image where the image is at first divided into 16x16 blocks where each block is holding different 16x16 blocks and those innermost 16x16 blocks are considered for data hiding.

In S. Sarreshtedari *et al.* [7] suggested a high capacity process for transforming domain image steganography algorithm

works on the wavelet transform coefficients of the original image to embed the secret data by absorbing integrity of the wavelet coefficients at high capacity embedding.
In A.Mondal *et al.*[8] proposed a distinctive cryptography technique without using any key where a triangulation of XOR operation has done followed by some other operation.

III. ALGORITHMS

III.A CRYPTOGRAPHY ALGORITHM:

III.A.a AUXILIARY KEY FORMATION:

STEP-1: Choose a preferable word or a sentence, take its 1st letter and the particular letter whose position is the last of 2^k form positions (like 1,2,4,8,16,….etc.).
STEP-2: Convert this two letters to its ASCII Value representation and then its corresponding 8 bits binary values.
STEP-3: Forming the 1st Auxiliary Key (AK1) of 8 bits whose 1st 4 bits are the last 4 bits of the 1st letter and the last 4 bits are the 1st 4buts of the 2nd letter.
STEP-4: Make a triangulation using NAND gate then take the left 8 diagonal elements from top to bottom for generating AK2 .
STEP-5: Repeating the same triangulation process for creating other AK_s but for even number of AK_s the left diagonal bits are considered and for odd number of AK_s the right diagonal elements from top to bottom of triangle are taken.
STEP-6: Thus the number of AK_s will be equal to the number of letters are present in the plain text.

III.A.b GENERATION OF CIPHER TEXT:

STEP-1: Choose a variable length of plain text and convert it corresponding ASCII Value succeeding of 8 bits binary representation.
STEP-2: Complement each 8 bit value of this binary representation and store it at CP[]. Then perform a bitwise XNOR operation between CP1, CP2, CP3,….CPn and AK1, AK2, AK3, ….,AKn one-to-one .
STEP-3: Twist the bit of odd position with its succeeding odd position bit (like 1st with 3rd and 5th with 7th position) and as well as twist each bit of even position with its afterward bit of even position (like 2nd with 4th and 6th with 8th position) for every bit stream.
STEP-4: Reverse each 8 bits or interchange the position of 1st to 8th as 8th to 1st .

III.B STEGANOGRAPHY ALGORITHM:

In this paper variable size of image can be used for hiding the cipher text. The minimum size of the image should be 8x8 for walloping at least one letter and nxn size of image can shield maximum (n/8) number of letters. Gray scale image as well as RGB image both can be deliberated on behalf of this process.
STEP-1: At first the innermost 4x4 matrix of the taken image is considered. The four corner cells of this matrix are used for saving the bits of cipher text and the process of saving those bits is for receiving '1'the value of the image pixel has to be increased by two and after getting '0' this increment will be one.
STEP-2: Then the four corner cubicles of 8x8 matrix that is covering up this 4x4 matrix are used for saving the next four bits and at this point a total 8 bits of a character of the cipher text has been kept in the image.
STEP-3: Thus the similar procedure has to be repeated and the size of the outer matrix is always 4x4 greater than the inner matrix. So after 8x8 the succeeding size of matrix will be 12x12 then 16x16 and soon.
STEP-4: Always the bits will be saved as maintaining the clock wise direction, beginning the left top cell of the matrices.

III.C STEGANANALYSIS ALGORITHM:

At receiver side the inverse method of the earlier technique has to be charted for moldering the image matrix and effortlessly the cipher text will be recovered by the decryption algorithm.
STEP-1: At first the Stego image that is got from sender side and the unusual cover image both are collected , compare those and exactly the same size of the image size matrix is formed.
STEP-2: The common values of this matrix are 0 excepting some are 1 and 2. This 1 and 2 values are present at the corner cells of some matrix. Starting from the innermost 4x4 matrix and collect it's left top diagonal cell value then make a clockwise rotation take other diagonal cell's values.
STEP-3: Thus the similar procedure has to be repeated for the outer matrices and the size of the outer matrix is always 4x4 greater than the inner matrix. So after 4x4 the succeeding size of matrix will be 8x8 then 12x12 and soon.
STEP-4: Arrange row wise those values without hampering its sequence in a 8xn size of matrix where n is the size of the plain text.

III.D CRYPTANALYSIS ALGORITHM:

STEP-1: Generate the auxiliary key (AK_s) that is discussed in the section.
STEP-2: Collect the 8xn matrix that is got from the steganalysis algorithm and reverse 8 bit values of each row.
STEP-3: For each row twist the bit of odd position with its succeeding odd position bit (like 1st with 3rd and 5th with 7th position) and as well as twist each bit of even position with its afterward bit of even position (like 2nd with 4th and 6th with 8th position) and store it in CP[].
STEP-4: Perform bitwise XNOR operation between the CP1 to AK1, CP2 to AK2 , …. CPn to AKn . Then compliment each 8 bit values. And after complimenting process the original plain text value will be retrieved.

IV. EXAMPLE

IV.A CRYPTOGRAPHY ALGORITHM:

Suppose the word 'WORLD' that has to be securely transmitted to the receiver side. And the word MOON is booked for auxiliary key formation. In MOON(shaded letter are in 2^k position) the first letter is M and the last 2^k position letter is here 4th position and the letter at this position is N.
M= 77=01001101
N=78=01001110
AK1= 11100100

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

0 0
1

AK2= 1010110

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

AK3= 11011011
Similarly AK4= 10110110 & AK5= 01101101.
WORLD=
87 79 82 76 68

Table I: 8bits representation of ASCII values

87=	0	1	0	1	0	1	1	1
79=	0	1	0	0	1	1	1	1
82=	0	1	0	1	0	0	1	0
76=	0	1	0	0	1	1	0	0
68=	0	1	0	0	0	1	0	0

Table II: complement values of previous table

W'	1	0	1	0	1	0	0	0
O'	1	0	1	1	0	0	0	0
R'	1	0	1	0	1	1	0	1
L'	1	0	1	1	0	0	1	1
D'	1	0	1	1	1	0	1	1

Table III: different auxiliary keys

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

Table IV: bitwise XNOR operation

AK1 XNOR W'	1	0	1	1	0	0	1	1
AK2 XNOR O'	1	1	1	0	0	0	1	0
AK3 XNOR R'	1	0	0	0	1	0	0	1
AK4 XNOR L'	1	1	1	1	1	0	1	0
AK5 XNOR D'	0	0	1	0	1	0	0	0

Table V: same colored columns were twisted

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

Table VI: reverse each row of previous table

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

IV.B STEGANOGRAPHY ALGORITHM:

Suppose the image that is taken here is a RGB image and the size of the image is 512x512. So as per our algorithm it can be held maximum of 64 letters where the no. of letters present in the cipher text is 5.

Fig. I: Cover Image

The first bit of the cipher text is here 0 and suppose the top left corner cell of the innermost 4x4 matrix value is 123 and for getting 0 the value will be 124, the next clockwise directed corner cell value is 245 after getting the next bit '0' it will be 246 like the last bit value is 1 and it will be inserted at the left bottom cell of 20x20 matrix and if the value is here277 then after getting '1' it will be 279.

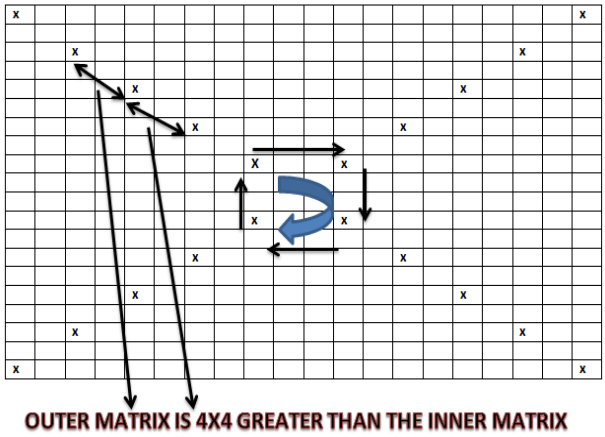

Fig II: Matrix representation of the image

IV.C STEGANALYSIS ALGORITHM:

After comparing the cover image with the stego image we have got values 2 and 1 change all 2s with 1s and all 1s with 0s. Without changing its sequence or collect them always maintaining a clockwise direction Organized them in a matrix holding 8 columns and n number of rows (here n=5). This is the binary values of cipher text.

IV.D CRYPTANALYSIS ALGORITHM:

The matrix of binary values that is acquired from the steganalysis algorithm is:

Table VII: matrix gained from image row wise reverse operation will be operated here

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

Table VIII: same color column will be twisted

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

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

Table IX: resultant of bitwise XNOR operation

1	0	1	1	0	0	1	1	AK1 XNOR PT1’
1	1	1	0	0	0	1	0	AK2 XNOR PT2’
1	0	0	0	1	0	0	1	AK3 XNOR PT3’
1	1	1	1	1	0	1	0	AK4 XNOR PT4’
0	0	1	0	1	0	0	0	AK5 XNOR PT5’

Table X: different auxiliary keys

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

Table XI: complement values of plain texts

PT1’	1	0	1	0	1	0	0	0
PT2’	1	0	1	1	0	0	0	0
PT3’	1	0	1	0	1	1	0	1
PT4’	1	0	1	1	0	0	1	1
PT5’	1	0	1	1	1	0	1	1

Table XII: finally the plain text values

0	1	0	1	0	1	1	1	= 87 = W
0	1	0	0	1	1	1	1	= 79 = O
0	1	0	1	0	0	1	0	= 82 = R
0	1	0	0	1	1	0	0	= 76 = L
0	1	0	0	0	1	0	0	= 68 = D

So, the text that was transmitted - ‘WORLD’.

V. RESULT AND DISCUSSION

After performing some experiments with the same image but altered the length of text values we have got different PSNR values and after plotting those values in X & Y axis this is shown as:

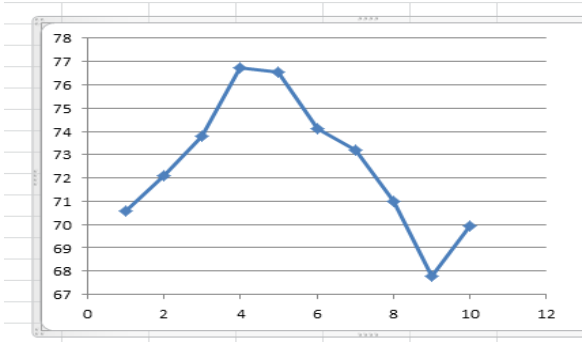

Fig III: Graph of Peak to signal noise ratio (PSNR) values where a single image is considered for different text

VI. CONCLUSION

In this paper, we have recommended a fresh method of exploiting the concept of cryptography and steganography together. Cryptography stresses in preserving the subjects of message as a secret to an unreadable format and on the other hand the steganography emphases on keeping the presence of a message to be secret that cannot be revealed by an unknown without having the awareness of the both cryptanalysis and steganalysis algorithm. The new algorithm is more efficient as the text is cipher text, where this cryptography process is somehow difficult as the key is generated from the random sentence or word not fixed and also this cipher text is hidden within the image without any deformation of the image. This technique is also used in practical purpose.

REFERENCES

[1] Quinhua Huang and WeiminOugang, “Protect fragile regions in Steganography LSB Embedding” 3rd International Symposium on Knowledge Acquisition and Modeling, 2010.

[2] P. Tsai, Y.C. Hu, H.L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing 89
(6) (2009) 1129-1143.

[3] Sudipta Sahana, Abhipsa kundu, Ahana Pal, “Crypt arithmetic stego based encryption algorithm”, International Journal of Computer Applications.(ISBN-973-93-80879-46-7)

[4] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, “Performance Evaluation of Symmetric Encryption Algorithms”, International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

[5] Adel Almohammad and Gheorghita Ghinea, “Image Steganography and Chrominance components “, 10th IEEE International Conference on Computer and information Technology, 2010

[6] Sudipta Sahana, Akash Pal, Archisman Chakroborty, “Optimized Block Steganography based Crypt Encryption for Secured Data Transfer ”, 3rd international conference on Computing, Communication and Sensor Network (CCSN) 2013.

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

[8] Anupam Mondal, Joy Samadder, Ivy Mondal, Neha Majumder, Sudipta Sahana, “Asymmetric Key based Secure Data Transfer Technique”, 2nd international conference on Computing, Communication and Sensor Network (CCSN) 2012.

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 in 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

