Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Dynamic Size Based Cipher Aided Image Steganography Technique for Network Security Enhancement

Abhipsa Kundu
M.Tech Scholar, Dept. of CA
National Institute of Technology
Durgapur, West Bengal, India

Sudipta Sahana
Asst. Professor, Dept. of CSE
JIS College of Engineering
Kalyani, West Bengal, India

Abstract— The improvement of spending internet system has enlarged the cosiness of data communication which throws competition in information security. Now recent days not hurtful and nontoxic data broadcasting become more vigorous and substantial. Cryptography and Steganography are two important areas of investigation that involve a great proportion of applications. Cryptography is the technology that encompasses to convert a message into an unreadable cipher text and the steganography is a skill and technology of walloping information in a multimedia file without triggering statistically significant change to this file for comprising a secret message communication. In our recommended work the plain text is changed to a cipher text using the method of Cryptography, where individual can able to use their desirable key for encrypting the text and also some Boolean algebraic operations are used in the following steps and next this cipher text is suppressed inside a cover media of 2n x 2n dimension gray scale image and a secure pictorial block steganography grounded encryption algorithm is suggested for transporting message and also exposed the Steganalysis and Cryptanalysis technique for retrieving data at receiver side. The investigational result specifies that for using altered length of message text, distortion of picture is too much less which is negligible in open eyes. At the end it can be declared that deprived of knowing the proper knowledge of cryptanalysis and steganalysis regaining of message is quite impossible.

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

I. INTRODUCTION

Cryptography is usually a key supporting technique for guarding disseminated systems. An encryption algorithm earns the original message and a key, then modifies the original message scientifically by cantered on the key to create a fresh encrypted message. Similarly a decryption algorithm gains an encrypted message and return to its original form consuming one or more keys. There are two general concepts of cryptographic keys: Private key and public key system. When identical key is use for encryption and decryption equal purpose then this is recognized as symmetric key encryption and the key is known as secret key. Where public-key encryption is recognized as asymmetric-key encryption. The private key is familiar for only on your computer, use for encryption purpose where the public key is communal by computer to computer who wants to interconnect securely with it. For decoding an encrypted message, a computer must use the public key.

In this paper, sheltered data transmission by using cryptography with key concept and Boolean algebra both are focused.

Steganography is the communiqué process of surreptitious data by consuming a multimedia carrier like image, video, audio or an IP Datagram is also used for this purpose. Generally people unable to detect the stealthy communication of data. Media where the message is hidden is renowned as 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.

II. RELATED WORKS

In this section the past work related to the problem of hidden text in an image file is analysed. 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.

Rig Das et al. [1] 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.

In M. Bellare [2] 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. Yam bernJina Chanu et al. [3] 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. [4] 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 colour image. The hash function delivers a secure and fast method for image steganography.

Ali Daneshkha et al in his "A More Secure Steganography Method in Spatial Domain" [5] 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

G.KarthigaiSeivi at al. [6] 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 centre pixels whose blocks are located at the sharper edges.

S. Sarreshtedari et al. [7] 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.

InS.Malik, A. Sardana [8] 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.

III. ALGORITHM

A. Cryptography Algorithm:

1. Password Matrix:

STEP-1: People can able to choose different password but always it will be reserved 8 characters length.

STEP 2: Transform each character of the password into its corresponding ASCII value and again those convert to its 8 bit binary values.

2. Generation of Auxiliary Keys :

STEP 3: For generating first auxiliary key AK1, 6th column of the password matrix is to be considered

STEP 4: The second auxiliary password AK2 is generated by holding the 1st bit of AK1 same as the 1st bit of AK2 and doing XNOR operation between the nth bit and (n+1)th bit of AK1 to acquire (n+1)th bit of AK2. And this procedure has advanced in further AKs where from AK2 to AK3 and from AK(n) to AK(n+1) has been obtained.

STEP-5: The number of Auxiliary keys has to be produced depends on the number of letters present in the plain text.

3. Formation of Cipher Text:

STEP-6: Choose a variable length of plain text and convert each character into its ASCII value forwarding by its 8 bit binary representation at the end arrange them as a matrix of nx8 where n is size of letters in plain text.

STEP-7: Reverse each column of this matrix.

STEP-8:Perform bitwise XOR operation in between the binary values of each row and the auxiliary keys AK1, AK2, AK3, ….,AKn respectively.

STEP-9: Complement the odd bits position(column no. : 1,3,5,7) of every row of the last obtained matrix.

STEP-10: Twist the column value with its next column but at most once.

STEP-11: change the n rows sequence, in spite of 1 to n they has arranged as n to 1.

STEP-12: At last we have got our cipher text binary value matrix representation.

B. Steganography Algorithm:

In this paper at first we have taken a 2n x 2n size of gray scale image; where the cipher text is buried

STEP-1: Taken the 8 bit matrix representation value of cipher text as an input.

STEP-2: Divide this matrix as 2(n-4) x 2(n-4) size of matrix where each cell of this matrix hold 16x16 size of matrix

STEP-5: The position of this matrix is depending on AKs value and its corresponding number of cipher text bits will be hold in this position.

STEP-6: The maximum 2(n-4) no. of letters can be hold in a image

STEP-7: In each iteration 2(n-7) no. of letters has occupied in this image so at most 8 iteration will be needed for getting full the image.

STEP-8: If we get '1' in cipher text bit values then the corresponding pixel position value has to be increased by 3 and for getting '0'values the corresponding pixel position has to be increased 2

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 2n x 2n differentiate value of these two images where most of the values are zero excepting some are 2s and 3s.
STEP-3: Disregard 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 3 with '1' and 2 with '0' and after that which matrix will be generated this is the 8 bit binary representation of our CT.

D. Cryptanalysis Algorithm:
STEP-1: Produce the PASSWORD MATRIX which 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 8 bit binary representation of cipher text. Arrange value of bits in nx8 matrix where n = size of CT.
STEP-4: change the sequence of row represent them as n to 1 where previously it was 1 to n.
STEP-5: Twist the column with its next column at most once.
STEP-6: Complement the odd bits position(column no. : 1,3,5,7) of every row of the last obtained matrix.
STEP-7: Perform bitwise XOR operation in between the binary values of each row of the previous matrix and the auxiliary keys AK1, AK2, AK3, ….,AKn respectively.
STEP-8: Reverse each column bit values of this matrix.

IV. EXAMPLE

***A. Cryptography Algorithm*:**

Suppose our plain text is RAIN that has to be securely transferred to the receiver side. As the number of letters in the plain text is 4 so four auxiliary keys will be formed.

1. Password Matrix:

Suppose our 8 letter word password matrix is ACRIDINE

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

So, as per the algorithm AK1= 00001011

TABLE I. AUXILIARY KEY GENERATION BY USING XNOR GATE

C(n+1) =C(n)		C(n+1)' = C(n) XNOR C(n+1)						
AK1	0	0	0	0	1	0	1	1
AK2	0	1	1	1	0	0	0	1
AK3	0	0	1	1	0	1	1	0
AK4	0	1	0	1	0	0	1	0

TABLE II. 8 BIT BINARY REPRESENTATION OF RAIN

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

TABLE III. REVERSE EACH COLUMN VALUE

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

XOR

AK1	0	0	0	0	1	0	1	1
AK2	0	1	1	1	0	0	0	1
AK3	0	0	1	1	0	1	1	0
AK4	0	1	0	1	0	0	1	0

TABLE IV. AFTER BITWISE XOR OPERATION THE RESULT

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

TABLE V. ODD POSITION BITS(1^{ST}, 3^{RD} , 5^{TH}, 7^{TH}) COMPLIMENT

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

TABLE VI: AFTER TWISTING EACH COLUMN WITH ITS NEXT COLUMN

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

TABLE VII: AFTER CHANGING THE SEQUENCE OF ROW, FROM BOTTOM TO TOP

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

***B. Steganography Algorithm*:**

Suppose we have considered the image size 512x512. So the maximum letter can be hold here 32. In each iteration the image can occupied 4 letters.

Suppose our image is:

Fig.1: Cover Image

Now our image is divide into 32x32 matrix where each cell of this matrix hold 16x16 matrix.

A_{00}	A_{01}	A_{02}	…….....	……...	…….	A_{031}
A_{10}	A_{11}	A_{12}	……..	…….	……..	A_{131}
……	…..	……	…..	……	…….	……
……	…….	……	…….	…….	……	…..
A_{310}	A_{311}	A_{312}	……	…….	…….	A_{3131}

Each cell of this matrix hold 16x16 size of matrix

a_{00}	a_{01}	a_{02}	…….....	……...	…….	a_{015}
a_{10}	a_{11}	a_{12}	……..	…….	……..	a_{115}
……	…..	……	…..	……	…….	……
……	…….	……	…….	…….	……	…..
a_{150}	a_{151}	a_{152}	……	…….	…….	a_{1515}

We have inserted the cipher text value inside this a matrix.

The 1st cipher text value has inserted in the position of AK1 that is – 0000 1011 = 0 11, so a011 position of A00 to A07 has occupied for the 1st 8 bits. Then for the 2nd 8its the next AK2 position that is 0111 0001 = a71 position has considered thus the process has done.

And the 1st bit value is 0 so if in a011 position of A00 pixel value is 125 then after getting 0 it will be changed to 127 and if the a011 position 0f A01 value is 234 then after getting 1 it will be 237, thus the codded image has made.

C. Steganalysis Algorithm:

After relating the cover image with the stego image we have got values 3 and 2 change all 3s with 1s and all 2s with 0s. Always collect them maintain a sequence and arrange them without hampering its sequence.

D. Cryptanalysis Algorithm:

Generate the auxiliary keys and password matrix as described the previous section..

TABLE VIII: BINARY MATRIX REPRESENTATION GOT FROM IMAGE

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

TABLE IX: AFTER CHANGING THE SEQUENCE OF ROW, FROM BOTTOM TO TOP

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

TABLE X: AFTER TWISTING EACH COLUMN WITH ITS NEXT COLUMN

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

TABLE XI: COMPLIMENT ODD POSITION BITS(1^{ST}, 3^{RD} , 5^{TH}, 7^{TH})

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

TABLE XII: RESULT OF BITWISE XOR OPERATION

AK1 XOR T1	0	1	0	0	1	1	1	0
AK1 XOR T1	0	1	0	0	1	0	0	1
AK1 XOR T1	0	1	0	0	0	0	0	1
AK1 XOR T1	0	1	0	1	0	0	1	0

TABLE XIII: AUXILIARY KEYS

AK1	0	0	0	0	1	0	1	1
AK2	0	1	1	1	0	0	0	1
AK3	0	0	1	1	0	1	1	0
AK4	0	1	0	1	0	0	1	0

TABLE XIV: REVERSE OF EACH COLUMN OF THE PLAIN TEXT

T1	0	1	0	0	1	1	1	0
T2	0	1	0	0	1	0	0	1
T3	0	1	0	0	0	0	0	1
T4	0	1	0	1	0	0	1	0

TABLE XV: PLAIN TEXT 8 BIT BINARY MATRIX REPRESENTATION

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

From the previous matrix we get the plain text was RAIN.

V. WORK ANALYSIS

After commissioning some investigations with different size of plain text into the same cover image we have acquired different stego images but the difference between the two images in every cases is negligible in open eyes. After calculating the PSNR values of each case we have got a graph that is:

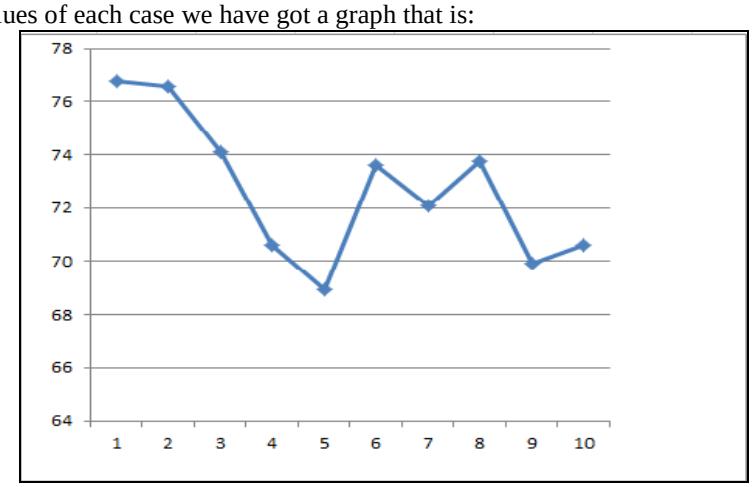

Fig 2: Graph of PSNR values

VI. CONCLUSION

In this paper; a fresh scheme of operating the concept of cryptography and steganography together is proposed. Cryptography eminences in protecting the substances of a message as a surreptitious to an unreadable format and on the other hand the steganography bounces the considerations on defending the presence of a message to be secret that cannot be uncovered by a third party without having the knowledge of the both cryptanalysis and steganalysis algorithm. The new algorithm is more effective as the text is not the original message but it is the cipher text and also it is hidden within the image without any distortion of the image. In this suggested method adaptable 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] RigDas , Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding", 2012 IEEE

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

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

[4] 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.

[5] 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.

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

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

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

