ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

ADAPTIVE ON DEMAND SIZE BASED IMGAGE STEGANOGRAPHY WITH CIPHER TECHNOLOGY

Sudipta Sahana*, Juhi Gangopadhyay
* CSE Department, JIS College of Engineering, Kalyani, Nadia, W.B. India

KEYWORDS: Cryptography, Cryptanalysis, Steganography, Steganalysis. Plain text, Cipher text.

ABSTRACT

The improvement of spending internet system has enlarged the cosiness of data communication which throws competition in information security. Now recent day's not hurtful and nontoxic data broadcasting become more vigorous and substantial. 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.

INTRODUCTION

Steganography is an art of hiding information. The steganographicsystem embeds secret content in a cover media and makes it unremarkable for the eavesdropper. Earlier people used invisible ink or hidden tattoos to transmit steganographic content. The information embedding process in a steganographic system starts by identifying the redundant bits of the cover medium. The embedding process results in a stego medium by replacing the redundant bit of the cover medium with the data of the secret message. The main aim of using such a technique is to make the secret message undetectable to the unauthorized users. There is one more technique used to cipher the existence of the secret message which is cryptography. Cryptography scrambles a message so that it cannot be understood whereas steganography is a technique that is used to hide the secret message so that it is undetectable by the unintended users.

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

Basically, the purpose of cryptography and steganography is to provide secret communication. Steganography can be used to cloak hidden messages in image, audio, video and even text files. The two most common methods used for hiding information inside a picture, audio and video files are LSB (Least Significant Bit) and Injection.In this paper, audio medium is used for steganography and a modified LSB algorithm is used to embed the secret message.

RELATED WORK

Vivek*et al.* (2012) [1] proposed a method to implement the steganography and cryptography for concealing the data into a medium. The steganography medium used in this data hiding system is audio and Least Significant Bit (LSB) algorithm is used for encoding the message in the cover medium. The encryption and decryption algorithm thus used makes the security of the system more efficient in concealing the data.

Abikoye*et al.* (2012) [2] proposed a system that integrated both cryptography and steganography where audio file is used as cover medium for steganography and a more powerful and qualified LSB algorithm is applied in order to achieve security of the information to be transmitted.

Jayaram*et al.* (2011) [3], presented the different types of audio steganographic methods, its advantages as well as disadvantages. This paper has proposed an efficient and robust method of unperceivable audio data hiding. Thus we conclude that audio data hiding techniques can be used for a list of other intents than covert communication or deniable data storage, tamper detection, finger printing and information tracing.

Raphael *et al.* (2011) [4], discussed how combining both steganography and cryptography will provide better security and confidentiality.Cryptography makes the information incomprehensible so that no intruder can

interpretthe original information. However, steganography focuses on hiding the existence of the secret information.

Sujay*et al.* (2010) [5] proposed a technique where cryptography and steganography is combined to encrypt the data and hide the data which is encrypted in the cover medium so that the secret data that is being sent is completely concealed.This paper proposes two new methods in which cryptography and steganography are fused to encrypt the data as well as to hide theencrypted data in the cover medium so the fact that amessage that is being transmitted is concealed. One method is to convert image into cipher text by S-DES algorithm using a secret key and hiding this text in another image using steganographic method. Another method is encrypting the image directly by S-DES algorithm with the use of key image and then it is then concealed in another image.

Mohammad *et al*. (2010) [6] proposed a steganography technique used to hide the data in the cover media and a key is used to hide the data and the Diffie-Hellmann exchange Protocol is used to exchange the data between the sender and the receiver. Proposed method that described two steps for hiding secret information by using the public steganography based on matching method. The first step is to find the shared stego-key between the two communication parties (Alice and Bob) over the networks by applying Diffie Hellman Key exchange protocol. The second step in the proposed method is that, the sender uses the secret stego-key to select pixels that it will be used to hide. Each selected pixel is then used to hide 8 bits binary information.

Dipti*et al.*(2011) [7], cryptography entirely is not enough for secure and credible communication. Both cryptography and steganography provides security and confidentiality in its own way.

Srideviet *al.* (2011) [8] presented that the goal of the steganography is in concealing the secret data by beclouding. The secret data is hidden in the cover medium. Steganography is different from cryptography in an aspect that cryptography is used to make the data unreadable for the unwanted users but at the same time it cannot prevent the unwanted user from learning about their existence whereas steganography hides the very existence of the secret message. The success of the steganography depends holistically on the ability to conceal the secret data in the cover media such that observe do not suspect its existence. Steganography must ensure that the message is invisible until the receiver knows what to look for and how. The process of hiding the data depends upon the medium used for hiding the information. Capacity of hiding information or the amount of information that can be concealed in the medium before it becomes detectable, can be measured.

Niel*et al.* (2003) [9], presented subsistingsteganographicsystems and presents the current research in observing them through statistical steganalysis. This paper discussed about the practical applications and mechanisms of detection algorithms. This article discusses existing steganographic systems and presents recent research in detecting them viastatistical steganalysis. Other surveys focus on the general usage of information hiding and watermarking orelse provide an overview of detection algorithms. The article presented recent research and discussed the practical application of detection algorithms and the mechanismsfor getting around them.

Mark *et al.* (2003) [10] presented an image steganography software named “Chameleon”. It features an encoding algorithm for 24 bit true color images. This software for 24-bit true-colorimages features a novel adaptive encoding algorithm founded on the steganographic model conceived by Yeuan-Kwen Lee and Ling- Hwei Chen for grayscale images.

MATERIALS AND METHODS

Algorithm for the proposed approach

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: 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 accepting 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.

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

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.

III. 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.

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

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

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

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

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

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.

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:

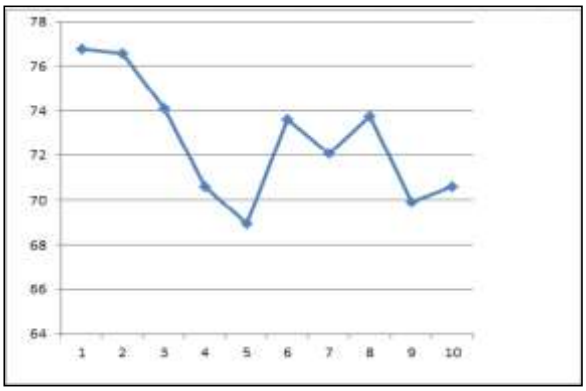

Fig 2: Graph of PSNR values

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.

ACKNOWLEDGEMENTS

Authors gratefully acknowledge to CSE Department JIS College of Engineering, for providing lab and related facilities for do the research

ISSN 2349-4506
Impact Factor: 2.265

Global Journal of Engineering Science and Research Management

REFERENCES

1. Vivek, J., Lokesh, K., Madhur, M. S., Mohd, S., and KshitizRastogi 2012. Public-Key Steganography Based on Modified LSB Method. Journal of Global Research in Computer Science, 3(4). ISSN: 2229-371X, pp. 26-29.
2. AbikoyeOluwakemi, C., AdewoleKayode, S., &OladipupoAyotunde, J. 2012. Efficient Data Hiding System using Cryptography and Steganography. International Journal of Applied Information Systems (IJAIS)–ISSN, 2249-0868,4(11).
3. Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011. Information Hiding Using Audio Steganography – A Survey. International Journal of Multimedia and Its Application, 3(3), pp. 86-96.
4. Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630.
5. Sujay, N. and Gaurav, P. 2010. Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions. Signal & Image Processing: An International Journal (SIPIJ), 1(2), pp 60-73.
6. Mohammad, A. A., and Abdelfatah, A. Y. 2010. Public-Key Steganography Based on Matching Method. European Journal of Scientific Research, 40(2). ISSN: 1450-216X. EuroJournals Publishing, Inc., pp. 223-231. Retrieved 21st August, 2012 from http://www.eurojournals.com/ejsr.htm.
7. Dipti, K. S. and Neha, B. 2010. Proposed System for Data Hiding Using Cryptography and Steganography. International Journal of Computer Applications. 8(9), pp. 7-10. Retrieved 14th August, 2012 from http://www.ijcaonline.org/volume8/number9/pxc3871714.pdf.
8. Sridevi, R., Damodaram, A., and Narasimham, S. 2009. Efficient Method of Audio Steganography By Modified LSB Algorithm and Strong Encryption Key with Enhanced Security. Journal of Theoretical and Applied Information Technology, pp. 768-771. Retrieved 21st August, 2012 from http://www.jatit.org.
9. Niels, P. and Peter, H 2003. Hide and Seek: An Introduction to Steganography. IEEE Computer Society. IEEE Security and Privacy, pp. 32-44.
10. Mark D. G. 2003. Chameleon Image Steganography- Technical Paper. Retrieved 14th July, 2012 from http://faculty.ksu.edu.sa/ghazy/Steg/References/ref13.pdf.