Crypt Arithmetic Stego based Encryption Algorithm for Secure Data Transfer

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

Abhipsa Kundu
B.Tech. Dept. of CSE
JIS College of Engineering
West Bengal, India

Ahana Pal
B.Tech. Dept. of CSE
JIS College of Engineering
West Bengal, India.

ABSTRACT

Information security is the most important issues in network communication in current days. Safe and sound data transfer become more essential and significant, as security is a major concern in the field of message transformation over internet in current years, Cryptography and Steganography are two significant areas of research that involve a number of applications. Cryptography is the technology that involves converting a message text into an unreadable cipher. Steganography is an art of hiding information in a cover image without causing statistically significant change to the cover image, so a carrier is needed to transfer information. In this proposed work the plain text is transformed to a cipher text using Cryptography technique where after changing the original text into its equivalent binary bits generally different kind of Boolean algebraic operations are used and in the succeeding step using Steganography technique this cipher text is hidden inside a gray scale image as a cover media with dimension 2^m x 2^m and a secure pictorial block steganography based encryptionalgorithm is proposed to execute the concept of secrecy for transferring text messagesbefore transmitting the information and also mentioned the Cryptanalysis and Steganalysis method for retrieving data at receiver side.The experimental result shows that the algorithm hasa high capacity and is better than the previous recommended PBST [5] techniqueFurthermore, satisfactory security is maintainedsince the secret message that is hidden inside the image cannot be extracted withoutknowing the cryptanalysis technique.

Keywords: Cryptography, Steganography, Plaintext, Ciphertext, Cryptanalysis, Steganalysis

1. INTRODUCTION

Cryptography is the technique where security engineering meets mathematics. It is probably the key enabling technology for protecting distributed systems. An encryption algorithm takes the original message and a key, and alters the original message mathematically based on the key bits to create a new encrypted message. Likewise a decryption algorithm takes an encrypted message and restores it to its original form using one or more keys. There are two general concepts of cryptographic keys:Private key and public key system.Public-keyencryption is also known as asymmetric-keyencryption. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicatesecurely with it. To decode an encrypted message, a computer must use the public key. In this paper, secure data transfer by using cryptography with Boolean algebra and key concept is focused.

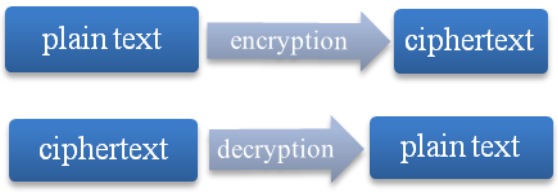
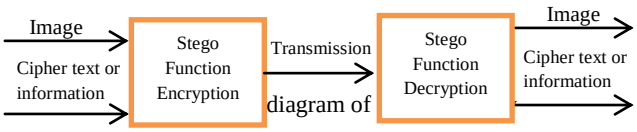


Fig 1: Block diagram of cryptography

Steganography is the process of invisible 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 operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media.



The paper is organized as follow. Section 2 describes thedifferent 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 decryptiontechnique 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.

2. 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

connections with deterministic encryption, hash functions protected on associated involvements.

InS.Malik, A. Sardana [2] 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.

In k. singla et al. [3] proposed a hash based Steganography approach for protected steganography using edge detection. The method accomplishes high embedding capacity and enhances the quality of the encoded image. This technique first detects 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.

In R. Zhang et al. [4] presents an upgraded data hiding technique based on BCH (*n*, *k*, *t*) coding. The suggested embedder hides data into a block of input data by altering some coefficients in the block in order to null the syndrome. The complexity of the suggested scheme is linear although that of other methods are exponential for any block size *n*. Thus, it is easy to extend this method to a large *n*. The BCH syndrome coding for steganography is now viable ascribed to the reduced complexity and its easiness of the embedder.

In P. Marwaha [6] proposed the Cryptography and Steganography are the most extensively used procedures, Both these procedures deliver some security of data neither of them solitary is secure enough for sharing information over an unsecure communication channel and are vulnerable to invader attacks. Although these procedures are often combined together to accomplish advanced levels of security but still there is a need of a highly protected system to transfer information over any communication media diminishing the threat of interruption

In A. Almohammad [7] projected the performance of both gray scale and color version of a given cover image when they are used with a specified Steganography process, The ability and impact of using the chrominance components 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 Q.HUANG [8] proposed the problem in LSB Matching revisited (LSBMR) ALGORITHM to make regions assortment on images to find fit zone. By counting on each pixel whether it is secured, decided. It can improve the visual inaudibility and deplorability of the LSB matching method.By adjusting the parameters of the neighbor pixels, the max embedding capacity can be increased as needed.

Liping et al [9] recommended a new Steganography method which uses the length of the messages to transfer the secret data. In this method, the sender and the receiver generate a Reference which is formed by collection of certain lengths of the ordinary traffic and the values in this reference are used to direct secret message. Liping's second scheme produced buckets and these buckets contain certain values. The number of buckets formed depends on the payload of the secret data per packet. Depending on the secret data, a value from a bucket is taken and the packet of that value is directed across the network.

3. ALGORITHM

In this section "Crypt Arithmetic Stego Based Encryption Algorithm for Secure Data Transfer" (CASE) is described. The encryption technique is used to convert plain text into cipher text and then considered a grayscale image, where the cipher text is concealed for transmission. In receiver section the cipher texts is retrieved and get the original message by decryption process.

3.1 Cryptography Technique:

Step 1: Taken an input string of information known as plain text. Calculate the length of each word of plain text.

Step 2: Taken an input string "EARTH" as a key.

Step 3: Convert this plain text string to ASCII value character by character including space and also convert the key string to corresponding ASCII value.

Step 4: Now perform bitwise XOR operation between each character of plain textand each character of key excluding plain space and tab or nbsp and If number of plain text characters is greater than the number of the characters of the key string,then repeat the key element.

Step 5: Convert each XOR result toequivalent binary value of 8 bits.

Step 6: Divide the 8bit binary value into 2 group having four bits binary value each and interchange the place of the left 4 bits with right 4 bits.

Step 7: Now operate right shift of left 4 bits and left shift of right 4 bits.

Step 8: Merge that two groupof 4 bit value and make it an 8bit value.

Step 9: Now divide the 8 bit value into 4 group of each of 2 bits and numbering these 4 parts from 1^{st} to 4^{th} as 1,2,3,4.

Step 10: Interchange the place of 1,2,3,4 as 1,4,2,3.

Step 11: Merge those 4 parts as a single 8 bits value.Perform 1's complement of the ODD bit positions of 8 bit value (i.e. 1, 3, 5, and 7).

Step 12: Now reverse the whole 8 bits i.e. the bits of 0 to 7 position will be now in 7 to 0 position

Step 13: Do XNOR operation between the data that is found in step 12 and 00001111.

Step 14: After doing the 13^{th} step convert each binary data to its corresponding decimal value and get the ASCII character of those value and this will be

the cipher text.

3.2Steganography Technique:

In this paper a gray scale image is considered first; where the cipher text (encrypted data after cryptography process) is hidden. At first the length of the cipher text is calculated and converted the text into its corresponding ASCII value. The initial gray scale image (256x256 i.e. $2^8 \times 2^8$) first converted into block size of(8x8) using block truncation coding(BTB). Then this will be converted into a binary format using binary conversion and merge the text into it by the following algorithm. Now this coded image is sent to the receiver end.

Step 1: Taken the cipher text as an input string and calculate the number of character which is stored it into a variable CT.

Step 2: Agray scale image with dimension $2^m x 2^m$ is taken.

Step 3: Add just one null character whose ASCII value is zero at the end of the CT.

Step 4: Convert the CT string to ASCII(decimal)value character by character whose last decimal value will be always 0 and convert each decimal value into m no. of it'sequivalent Binary bits.

Step 5: Apply the partial BTB technique on this image with mxm size block matrix and each cell of the matrix contain $2^{(m-n)}$ x $2^{(m-n)}$ (where, m= 2^n) matrix size.

Step 6: Convert this gray scale image to bit map image.

Step 7: The number of characters of the text is calculated already. If it is less than or equal to m then the 1^{st} bit of the 1^{st} character will be placed into 1^{st} image block (0,0 position),then2^{nd} bit will be placed into 2^{nd} image block(0,0 position) thus the process will continue less than or equal to m time

Step 8: If the number of character is greater than m then the 8 bit afterward positions will be considered so the m+1 character's 1^{st} bit will be placed into 1^{st} image block(7,7 position), 2^{nd}bit place into 2^{nd}image block (7,7 position) similarly 2m+1 character's 1^{st} bit will be placed into1^{st} image block (15,15 position), 2^{nd} bit will be placed into 2^{nd}image block(15,15 position),after that for the character set of 3m+1 to 4m (23,23 positions) will be considered and continued.

Step 9: Convert the entire changed binary image to gray scale image.

Step 10: Transfer this coded image to receiver side.

3.3 Steganalysis Technique:

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

Step1: Convert the gray scale image to binary image(bit map image).

Step 2: Apply the partial BTB coding for this image with mxm size block matrix where each cell contains ($2^{(m-n)}$ x $2^{(m-n)}$) size matrix.

Step 3: Then first take all the binary value of the position (0,0) from every block ($2^{(m-n)}$ x $2^{(m-n)}$) row wise.

Step 4: All the binary value is takenof the position (7,7) form every block ($2^{(m-n)}$ x $2^{(m-n)}$) row wisethen take binary value of the position form every (15,15) position then take (23,23) position then take (31,31) position until all the m bits of any row are zero. If all m bits are raised zero then stop to collect values.

Step 5: Convert the binary representation into equivalent decimal form block by block.

Step 6: Convert the decimal number or the ASCII value to character and discard last 0.

Step 7: This set of character is the Cipher text that is encrypted by the cryptography process.

3.4 Cryptanalysis Technique:

Step 1: Convert this cipher text string to ASCII value character by character and get the corresponding 8bits binary value of those decimal values.

Step 2: Do XNOR operationbetween the cipher text(8 bit value) and 00001111.

Step 3: Reverse the whole 8 bits number means the bits of 0 to 7 position will be now in 7 to 0 positions.

Step 4: Perform 1's complement of the ODD bit positions of 8 bit value(1, 3, 5, and 7).

Step 5: Now divide 8 bit value into 4 parts of each 2 bits and numbering these 4 parts from 1^{st} to 4^{th} as 1,4,2,3.

Step 6: Interchange the position of 1,4,2,3 as 1,2,3,4 merge those 4 parts as a single 8 bits value.

Step 7: Divide the 8bit binary value into 2 four bits binary value and operate left shift of left 4 bits right shift of right 4 bits.

Step 8: Now interchange the place of the left 4 bits with right 4 bits.

Step 9: Merge the 4 bit parts and again make it a 8 value.

Step 10: Now perform bitwise XOR operation between each character of Cipher text and each character of key excluding space or tab or nbsp and if number of plain text characters is greater thanthe number of the characters of the key stringthen repeat the key element.

4. EXAMPLE

4.1 Cryptography Technique:

Suppose "JIS" is a plain text i.e. it is required to transmit.

Length of the word "JIS" is 3. Key-EARTH

ASCII value of plain text

J-112, I-111, S-123

Binary value:

J-01001010, I-01001001, S-01010011

ASCII value of key element

E-105, A-101, R-122, T-124, H-110

Binary value

E-01000101, A-01000001, R-01010010, T-01010100, H-01001000

Now J XOR E-00001111, I XOR A-00001000, S XOR R-00000001

Now, dividing the result of each XOR operations of 8bit binary value into 2 parts of 4 bits and interchanging left 4 bits with right 4 bits the value will be 11110000, 10000000, and 00010000.

After right shifting left 4 bits and left shifting right 4 bits the following value is received

From 1111 0000→1111 0000

From 1000 0000→0100 0000

From 00010000→10000000

Now dividing each of these 8 bit value into 4 parts of each 2 bits and numbering these 4 parts from 1st to 4th as 1,2,3,4 and interchanging the place of 1,2,3,4 as 1,4,2,3 the following value is received,

1	2	3	4		1	4	2	3
11	11	00	00	→	11	00	11	00
01	00	00	00	→	01	00	00	00
10	00	00	00	→	10	00	00	00

Now 1's complement of odd position (1, 3, 5, 7) is performed-

01234567 01234567

11001100→ 10011001

01000000→ 00010101

10000000→11010101

Now calculate reverse of each 8 bits -

10011001 →10011001

00010101 →10101000

11010101 →10101011

Now performing XNOR gate with those 8 bits data and 00001111

10011001 XNOR00001111→ 01101001

10101000 XNOR 00001111→01011000

10101011 XNOR 00001111 → 01011011

Decimal values of those 8 bits:

01101001 → 105

01011000 → 88

01011011 → 91

Converting those decimal values to character

J→i I→XS→[

4.2 Steganography Technique:

Consider the value m=8 and n=3.Suppose the cipher text of word JIS that is **iX[**is wanted to transmit. Here number of characters in the word are 3add just one null character and make it 4 characters or with the ASCII value of those 3 characters add 1 zero value (as the ASCII value of null is 0). The original message takes form as:

105	88	91	0

Now each value is transformed to it's corresponding binary value as total length of message is now 32.and the matrix will be

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

Now a grey scale image is chosen in which this binary message is merged.

Fig 3: Gray scale image for data hiding

Then the image is converted to equivalent binary image matrix and the dimension of matrix will be 2^8x2^8 or 256x256. O it will be decomposed o 8x8 matrix as follows:

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

Each 8x8 block matrix contains 32x32 square matrices which is represent as follows:

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

The text is embedded within the gray scale image. Now according to the encryption algorithm all the a_{00} position of each 8x8 matrix will be replaced according to the message representation i.e.,the 1st row of character **i** value will be inserted as a_{00} of A_{00} will be 0, a_{00} of A_{01} will be 1, a_{00} of A_{02} will be 1, this way for character **X** value a_{00} of A_{10} will be 0, a_{00} of A_{11} will be 1,……a_{00} of A_{36} will be 1 a_{00} of A_{37} will be 1 and a_{00} of A_{40} to a_{00} of A_{47}will be 0 and the other values of a_{00} will be the binary values of original image. As the number of characters in the text is less than 8 so a_{77} positions are not considered at all. After getting the total matrix it is converted into its corresponding gray scale image for transmission

4.3 Steganalysis technique:

By using this technique all the bits are retrieved from the a_{00} position of 1st three rows and will get all 8 bits is zero of the 4th row.So stop collecting other binary valuesand omit the last row and convert the 1st three rows each 8 bits binary no to decimal. Then convert those to their ASCII character which is iX[, that is a cipher text.

4.4 Cryptanalysis technique:

The cipher text is iX[

i = 105 → 01101001

X= 88→ 01011000

]= 91 → 01011011

Now performing XNOR Gate with these 8 bits data and 00001111

01101001 XNOR 00001111 → 10011001

01011000 XNOR 00001111 →10101000

01011011 XNOR 00001111→10101011

Now performing the reverse of 8 bits data:

10011001 →10011001

10101000 → 00010101

10101011 → 11010101

Now performing 1's complement of odd position (1, 3, 5, 7) the value will be,

10011001 → 11001100

00010101 → 01000000

11010101 → 10000000

Now dividing each of these 8 bit value into 4 parts of each 2 bits and numbering these 4 parts from 1st to 4th as 1,4,2,3 and then interchanging the place of 1,4,2,3 as 1,2,3,4 -

1	4	2	3		1	2	3	4
11	00	11	00	→	11	11	00	00
01	00	00	00	→	01	00	00	00
10	00	00	00	→	10	00	00	00

Now merge 4 parts of two bits to a single 8 bits data. Divide the 8 bit binary value into 2 four bits binaryValue and operate left shift of left 4 bits right shift of right 4 bits.

11110000 → 1111 0000 →1111 0000

01000000 → 0100 0000 →1000 0000

10000000 →1000 0000 →0001 0000

Interchange the these left 4 bits with right 4bits.

1111 0000→ 0000 1111

1000 0000→ 0000 1000

0001 0000 → 0000 0001

Those are the value of after XOR GATE.

Suppose the key is EARTH. E= 01000101 A= 01000001 R= 01010010 T= 01010100 H = 01001000 SO,

01000101 XOR00001111 = 01001010 →74 → J

01000001 XOR 00001000 = 01001001 → 73→I

01010010 XOR 00000001 = 01010011 → 83 → S

So the plain text received is JIS

Notation	Description
ASCII	American Standard Code for Information Interchange
XOR	Exclusive OR operation
XNOR	Exclusive NOR operation
PT	Plain Text
CT	Cipher Text
BTB	Block Truncation Coding

Table 1: Data Dictionary

5. ANALYSIS WORK

In this paper the proposed CASE method is better than the previous recommended PBST [5] technique in many ways those are as follows:

- In PBST technique only the steganography method was suggested so if anybody is guessed that any information is hidden inside the image and if he is succeed to retrieve the data from the image then he will able to know the original secret information that was transmitted. But in the proposed method the hidden data inside the image is a cipher text so if anybody can retrieve the data is in an unreadable format. So a dual layered security system is proposedhere for data transmission.

- The steganography method is also better here than the PBST technique as because of in PBST technique only the (0,0) position of the 32x32 matrix was considered for data hiding, so very limited data can be send at a time if a huge information try to send together then this process will be failed. But in this proposed method a vast information is transmitted at a time and not only the (0,0) position but other like (7,7),(15,15) etc. this positions are also considered so it is very hard to understand in which position of 32x32 matrix the data is hidden by a third person.

- In PBST technique for less than 8 characters of data making it 8 characters so many zeroes are added and the cover image is greatly changed but in the proposed process only one zero is added at the end that does not considerably change the image.

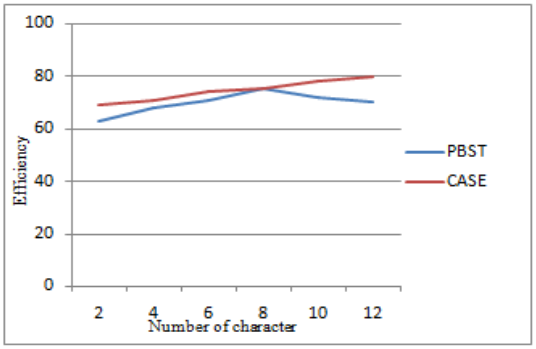


Fig 4: Efficiency Comparison between PBST & CASE

6. CONCLUSION:

In this paper namely CASE; a new method of utilizing the concept of cryptography and steganography together is proposed. Cryptography emphases in preserving the contents of a message as a secret to an unreadable format and on the other hand the steganography focuses on shielding the existence of a message to be secret that cannot be discovered 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] MihirBellare and SriramKeelveedhi and Thomas Ristenpart," Message-Locked Encryption and Secure Deduplication", Eurocrypt 2013, Volume 7881, 2013, pp 296-312

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

[3] KirtikaSingla and sumeetkar, "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.

[4] Rongyue Zhang," AN EFFICIENT EMBEDDER FOR BCH CODING FOR STEGANOGRAPHY" Information Theory, IEEE Transactions on vol. 58, December 2012.

[5] AnupamMondal, SudiptaSahana, Sainik Kumar Mahata "A Pictorial Block Steganography based Secure Algorithm for Data Transfer" International Conference on Computing, Communication and Sensor Network (CCSN) 2012

[6] PiyushMarwaha, PareshMarwaha, "Visual Cryptographic Steganography in images", 2nd International Conference

on Computing, Communication and Networking Technologies, 2010

[7] Adel Almohammad and GheorghitaGhinea, "Image Steganography and Chrominance components ", 10th IEEE International Conference on Computer and information Technology, 2010

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

[9] L. Ji, W. Jiang, B. Dai and X. Niu, "A Novel Covert Channel Based on Length of Messages", International Symposium on Information Engineering and Electronic Commerce,16-17 May 2009, Page(s):551-554.