Optimized Block Steganography based Crypt Encryption for Secured Data Transfer

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

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

Archisman Chakroborty
B.Tech. Dept of CSE
JIS College of Engineering
West Bengal, India

ABSTRACT
In this paper a new steganographic technique using an advanced cryptographic technique has been proposed. In the encryption part of this paper the concept of ASCII value of the English alphabets have been used. Besides this the binary conversion of those ASCII values and the concept of hamming distance measurement are also used here. Multiple Auxiliary keys are generated using one password and after the encryption, the steganographic part is done with the help of grey-scale concept.

Keywords
Cover image, Data hiding, Cryptography, Steganography, Stego-image, grayscale image definition, hamming distance.

1. INTRODUCTION
In this modern world the major concern is transmission of the information securely so that the messages are not intercepted by unauthorized users. To overcome this constraint techniques such as – Steganography and Cryptography are used. Steganography and Cryptography deals with hiding the information so that only the sender and the intended receiver can understand the hidden message. Even then security is a major concern and so in this paper a step has been taken forward in improving the security by making use of multiple passwords. The generation of these passwords and the process of utilizing them to embed the message have been effectively described by the Algorithm and the related example.

1.1 Cryptography
In cryptography a plain text is chosen which is a message that will be put into secret form and then transform this plain text to cipher text .This process of transformation of plain text to cipher text is known as encryption. The reverse process is known as decryption. The encryption is done in such as way that it is impossible for anyone to understand the cipher text without the means to decrypt. The strength of cryptography depends on the encryption and decryption techniques and the length of key.

Cryptography is:
–A tremendous tool.
–The basis for many security mechanisms.
Cryptography is not:
–The solution to all security problems.
–Reliable unless implemented and used properly.

Two basic types of cryptosystem exist: secret key and public key.
In a secret key scheme, the key for encryption must be the same as the key used for decryption. This scheme is also known as symmetric cryptosystem.

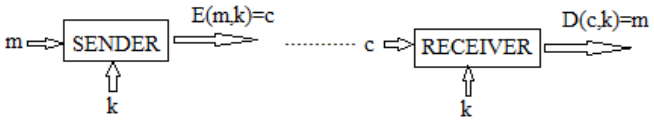


Fig 1: Block diagram of symmetric cryptosystem

Here m: plaintext
c: cipher text
E: Encryption algorithm
D: Decryption algorithm
k: Secret key

1.2 Steganography
Steganography is formally defined as the art and science of writing hidden messages in such a way that only the sender and intended recipient, can know about the presence of hidden information**.** Stenography can be traced all the way back to ancient Greece but it has recently seen a revival with the birth of the digital age, steganography has become much easier and it is commonly used to send hidden messages within a digital pictures or audio files. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot detect the presence of the hidden message. The carrier image in steganography is called the "cover image" and the image which has the embedded data is called the "stego-image".

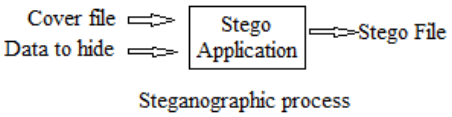


Fig 2: Block diagram of Steganographic process

1.3 The advantage of Steganography over Cryptography:
The advantage of steganography over cryptography is that in cryptography a third party can be suspicious about the presence of hidden information. Though cryptography protects the contents of a message, however it reveals the presence of secret message. Whereas in digital steganography, image file are used as carriers of the hidden message and in that process reduces the suspicion of hidden messages present within.

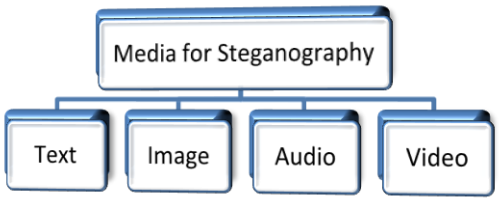


Fig 3: Different media for Steganography

1.4 Grayscale image definition:

In computer vision color images are not used very much. Mostly black and white images like gray scale image are used .Even though gray scale images misses' information from the original image, but it turns out that grey scale is more robust to lighting variations than color is. So a gray scale image is a matrix typically of several hundred rows and several hundred columns that have small values imprinted which corresponds to the gray scale of a pixel. These values scale between 0 and 255, where 255 is white and 0 is black.

Grayscale images are often the result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum (e.g. infrared, visible light, ultraviolet, etc.), and in such cases they are monochromatic proper when only a given frequency is captured. But also they can be synthesized from a full color image.

1.5 Converting color image to grayscale image

The red, green, blue variables should all be assigned to a gray level, which is computed as a weighted average of the original red, green, blue levels. The weights, corresponding to the sensitivity of the cone cells in human eye, are red: 0.2126, green: 0.7152, blue: 0.0722

Y= (0.2126*red+0.7152*green+0.0722*blue)

where Y is the weighted average of the original red, green, blue levels.

In this paper the data hiding mechanism has been ensured by using a new technique of password based pictorial block steganography. Here the grey scale image is divided into blocks as per the requirement and then the algorithm is used to generate multiple keys from the given password to embed the message. It ensures security in the sense that the location of the hidden message in the grayscale image can only be found with the help of password. The paper is ordered as follow. In Section 2 different types of steganography Techniques are specified. In Section 3 the encryption algorithms of cryptography, steganography and the decryption techniques are discussed followed by an example in Section 4. Finally, concluded in Section 5 with some references in section 6.

2. RELATED WORKS

Many research works have been carried out on Stego-Security. Different researchers employed different techniques for the purpose of secured secret image embedding. Following are the few related works carried out by various research groups.

Yicong Zhou et al. [1] proposed PLIP (Parameterized Logarithmic Image Processing) addition to embed the scrambled original image into a selected cover image via specific parameters using a new algorithm to generate an encrypted image.

K. Pramitha et al. [2] used the RSA encryption technique and Mod-4 Embedding algorithm to obtain secure stego image by embedding the encrypted message into groups of 2×2 block of non-overlapping spatially adjacent pixels of the cover image.

Ge Huayong et al. [3] review's steganography and steganalysis based on digital image by illustrating the important concepts, principle, present trends and future prospects of steganography and steganalysis.

S. M. Masud Karim et al. [4] improvises the present technique of LSB substitution of RGB true color image by using a secret key to store hidden information into different position of LSB of image. In general, in LSB methods, hidden information is stored into a specific position of LSB of image.

Lauretha Rura et al. [5] analyses the best possible available image steganography technique to be implemented in an electronic voting system, out of which F5 technique has been suggested as it creates smaller stego-image size, and it does not include a very complex mathematical calculation.

Rig Das et al. [6] 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.Karthigai Seivi at al. [7] 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 bern Jina Chanu at al. [8] describes a short survey on different types of steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image in spatial domain by mentioning the strong points and weak points of the techniques.

3. ALGORITHM

In this section different phases of security technique have been described. Before cryptography and steganography algorithm a Password Matrix and Auxiliary key generation phase is done.

3.1 Password Matrix

Step 1: Choose a password of 8 characters.

Step 2: Convert each character of the password into its corresponding ASCII value.

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

Step 4: Categorize the password matrix into 16 blocks each of 4 bits such that each row has two groups of 4 bits.

3.2 Generation of Auxiliary keys

Step 5: For that purpose the diagonal elements of password matrix is chosen as the first auxiliary key AK1.

Step 6: The second auxiliary password AK2 is generated by retaining the 0^{th} bit of AK1 as the 0^{th} bit of AK2 and doing XOR operation between the n^{th} bit and $(n+1)^{th}$ bit of AK1 to obtain $(n+1)^{th}$ bit of AK2.

Step 7: The third auxiliary key AK3 is generated by doing OR operation between the bits of AK1 and AK2.

Step 8: The remaining auxiliary keys are generated by xoring the AK (n) key and AK (n+1) key.

Step 9: The number of Auxiliary keys generated depends on the number of letters in the plain text.

3.3 Encryption

Step 1: Choose a plain text of variable length and calculate its length.

Step 2: Convert each character into its ASCII value and then into its corresponding binary representation.

Step 3: Categorize the binary value of each corresponding letter into three parts. The first part consists of 5^{th}, 6^{th}, 7^{th} and 8^{th} bits. The second part consists of 4^{th}, 5^{th}, 6^{th} and 7^{th} bits. The third part consists of 3^{rd}, 4^{th} , 5^{th} ,and 6^{th} bits.

Step 4: Convert part 1 to decimal value. Select the group from password matrix basing on the decimal value.

Step 5: Calculate the hamming distance (H.D) between part 2 and the particular group selected. If H.D is odd then 7^{th} bit is toggled. Else if H.D is even then the bit is retained as it is.

Step 6: Calculate the hamming distance (H.D) between part 3 and the particular group selected. If H.D is odd then 8^{th} bit is toggled. Else if H.D is even then the bit is retained as it is.

After this step the transformed binary values P1, P2,.., Pn. are obtained.

Step 7: If 'n' is the number of letters in the plain text then XNOR operation is performed between the transformed binary values P1, P2, P3,…,Pn and the auxiliary keys AK1, AK2, AK3, ….,AKn respectively.

Step 8: CT1, CT2, CT3, CT4 are combined to obtain the encrypted message.

3.4 Steganography

Step 1: Take a grayscale image with dimension 256 x 256.

Step 2: Apply the partial Block Truncation Coding on this grayscale image with 16 x 16 size block matrix, where every block is of size 16 x 16.

Step 3: Convert this gray scale image into bit map image.

Step 4: To embed the encrypted message into the image, consider the 1^{st} block of encrypted message CT1.

Step 5: Select the first auxiliary key AK1, then divide this key into two equal parts each of 4-bits.The first 4 bits of the AK1 is taken into consideration and inverted. Each set of bits is converted into decimal. These two decimal values are used as row number(r) and column number(c).

Step 6: The 1^{st} bit of 1^{st} message block is placed into 1st image block $(r,c)^{th}$ position. The 2^{nd} bit of 1^{st} message block is placed into 3^{rd} image block $(r,c)^{th}$ position and so on the 8^{th} bit of 1^{st} message block is placed into 13^{th} image block $(r,c)^{th}$ position. This step is performed recursively for all the message blocks, considering next row of the image block.

Step 7: After reaching the last block row, again the process is repeated from the 1^{st} block row considering the consecutive even image blocks i.e 2^{nd} block, 4^{th} block, 6^{th} block and so on in each row. Again after reaching the last block row, step 6 is repeated followed by step 7.

Step 8: If the length of plain text is L. Then After embedding the plain text, the $(L+1)^{th}$ row is embedded with zero.

Step 9: Send the grayscale image with the embedded message to the receiver.

3.5 Decryption:

Step 1: Generate the auxiliary keys from the password matrix which in turn is obtained from the password.

Step 2: After obtaining the auxiliary keys each key is divided into two equal parts each containing 4 bits. Invert the first 4 bits. Then the two parts are converted to their corresponding decimal values. These two decimal values are used as row number(r) and column number(c).

Step 3: Convert the gray scale image to binary image (bit map image).

Step 4: Apply the partial Block Truncation Coding on this gray scale image with 16 x 16 size block matrix, where every block is of size 16 x 16.

Step 5: Then take the binary value of the $(r,c)^{th}$ position from every odd 16 x 16 block row wise. i.e $(r,c)^{th}$ position of 1^{st} image block of 1^{st} row, $(r,c)^{th}$ position of 3^{rd} image block of 1^{st} row and so on.

Step 6: After reaching the last block row, again the process is repeated from the 1^{st} block row considering the consecutive even image blocks in each row i.e $(r,c)^{th}$ position of 2^{nd} image block of 1^{st} row, $(r,c)^{th}$ position of 4^{th} image block of 1^{st} row and so on.

Step 7: Then divide those bits in several blocks with 8 bits in each.

Step 8: Convert the binary representation into equivalent decimal block by block. If the decimal number is zero

a). discard that number

Else

b). XNOR operation is performed between the binary representation of each block and the auxiliary key.

Step 9: After the XNOR operation each Decoded Text (DT) is equivalent to the transformed binary value.

Step 10: Categorize the each transformed binary value into three parts. The first part consists of 5^{th}, 6^{th}, 7^{th} and 8^{th} bits. The second part consists of 4^{th}, 5^{th}, 6^{th} and 7^{th} bits. The third part consists of 3^{rd}, 4^{th} , 5^{th} ,and 6^{th} bits.

Step 11: Convert part 1 to decimal value. Select the group from password matrix basing on the decimal value.

Step 12: Calculate the hamming distance (H.D) between part 2 and the particular group selected. If H.D is odd then 7^{th} bit is toggled. Else if H.D is even then the bit is retained as it is.

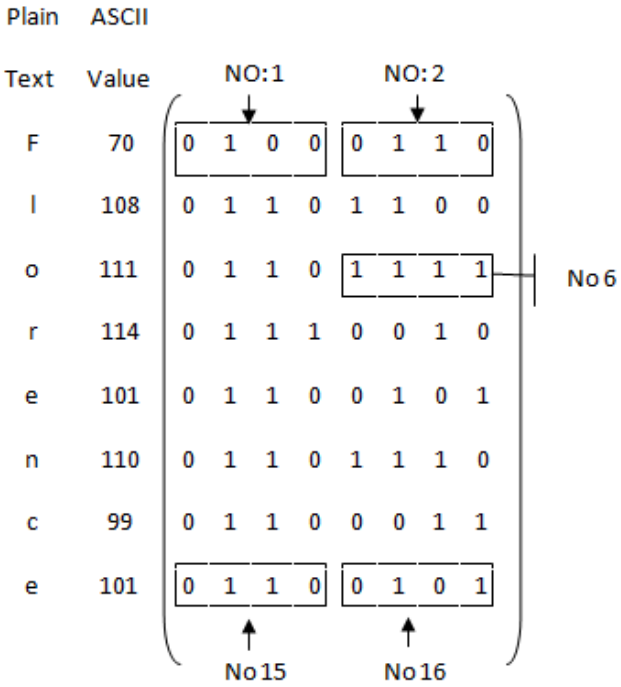
Step 13: Calculate the hamming distance (H.D) between part 3 and the particular group selected. If H.D is odd then 8^{th} bit is toggled. Else if H.D is even then the bit is retained as it is.

Step 14: After this step the binary values are obtained which are converted into its decimal value (i.e. ASCII value) to obtain the characters. These set of characters are the ultimate information which was forwarded by the sender.

4. EXAMPLE

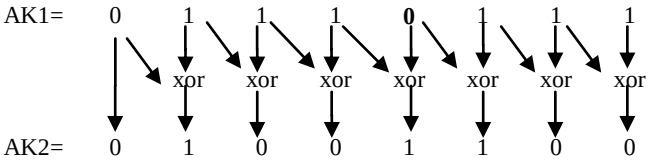
4.1 Password Matrix

Suppose password is Florence



4.2 Generation of auxiliary keys:

For that purpose the left diagonal elements of password matrix is chosen as the first auxiliary key;
AK1=01110111

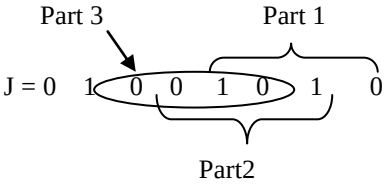


AK1=	0	1	1	1	0	1	1	1
AK2=	0	1	0	0	1	1	0	0
	OR	OR	OR	OR	OR	OR	OR	OR
AK3=	0	1	1	1	1	1	1	1

AK2=	0	1	0	0	1	1	0	0
AK3=	0	1	1	1	1	1	1	1
	xor	xor	xor	xor	xor	xor	xor	xor
AK4=	0	0	1	1	0	0	1	1

4.3 Encryption

Pain text	ASCII value	Binary value
J	74	01001010
I	73	01001001
S	83	01010011
C	67	01000011



Part1: 1010 =10 (decimal value)
Group No.10 from password matrix is selected.
Hamming distance between Part2 and group no 10 is calculated.

Group 10	0	1	0	1
Part 2	0	1	0	1
H.D.	0	0	0	0

H.D = 0 (in decimal) which is even so the 7th bit is not inverted.
Hamming distance between Part3 and group no 10 is calculated.

Group 10	0	1	0	1
Part 2	0	0	1	0
H.D.	0	1	1	1

H.D = 7(in decimal) which is even so the 8th bit is not inverted.
J becomes 11001010
Similarly proceeding in this way for the remaining letters in the word are obtained as:

Pain text	Transformed binary value
J (P1)	11001010
I (P2)	01001001
S (P3)	00001001
C (P4)	00000011

XNOR operation is performed between the new binary values P1, P2, P3, P4 and the auxiliary keys AK1, AK2, AK3, AK4 respectively.

P1	1	1	0	0	1	0	1	0
AK1	0	1	1	1	0	1	1	1
	xnor	xnor	xnor	xnor	xnor	xnor	xnor	xnor
CT1	0	1	0	0	0	0	1	0

P2	0	1	0	0	1	0	0	1
AK2	0	1	0	0	1	1	0	0
	xnor	xnor	xnor	xnor	xnor	xnor	xnor	xnor
CT2	1	1	1	1	1	0	1	0

P3	0	0	0	0	1	0	0	1

AK3	0	1	1	1	1	1	1	1
	xnor	xnor	xnor	xnor	xnor	xnor	xnor	xnor
CT3	1	0	0	0	1	0	0	1

P3	0	0	0	0	0	0	1	1
AK4	0	0	1	1	0	0	1	1
	xnor	xnor	xnor	xnor	xnor	xnor	xnor	xnor
CT4	1	1	0	0	1	1	1	1

CT1, CT2, CT3, CT4 are combined to obtain the encrypted message.

4.4 Steganography

Suppose dimension of the image matrix is 256x256.Then this matrix is completely logically decomposed into some 16x16 square matrices as follows:

B_{00} B_{01} B_{02} B_{03} ……..…….B_{011} B_{014} B_{015}
B_{10} B_{11} B_{12} B_{13} …….....B_{111} B_{114} B_{115}
B_{20} B_{21} B_{22} B_{23} ……..……B_{211} B_{214} B_{215}
. .
. . . . …… . . . .
. .
. . ..…….. . . . .
. .
B_{140} B_{141} $B_{142}B_{143}$ ……... ……B_{1414} B_{1415}
B_{150} B_{151} $B_{152}B_{153}$ ……..... B_{1514} B_{1515}

Each block matrix is of size 16x16 which is represented as follows:

b_{00}	b_{01}	……	b_{015}	b_{016}
b_{10}	b_{11}	……	b_{115}	b_{116}
. . . . .		……	. . . . .	
. . . . .		……	. . . . .	
b_{140}	b_{141}	……	b_{1414}	b_{1415}
b_{150}	b_{151}		b_{1514}	b_{1515}

The original message is embedded within the gray scale image. To embed CT1 block, the first auxiliary key AK1 is selected, then this key is divided into two equal parts each of 4-bits.The first part of the AK1 is taken into consideration and inverted .Each set of bits is converted into decimal.

AK1=0111 0111
8 7

The first bit of CT1 will be inserted in b_{87} of B_{00} . The second bit of CT1 will be inserted in b_{87} of $B_{03,}$ in this way the 8^{th} bit of CT1 is inserted in b_{87} of B_{013}
Similarly CT2, CT3, CT4 is embedded into image using the key AK2, AK3, AK4.

4.5 Decryption

The received encrypted message (EN) is broken down to equal parts of 8 bit as follows:

EN1	1	1	0	0	1	0	1	0
EN2	0	1	0	0	1	0	0	1
EN3	0	0	0	0	1	0	0	1
EN4	0	0	0	0	0	0	1	1

Since the number of parts happens to be four so four auxiliary keys AK1, AK2, AK3, and AK4 are generated. And then XNOR operation is performed between EN1, EN2, EN3, EN4 and the auxiliary keys AK1, AK2, AK3, and AK4 respectively.

EN1	1	1	0	0	1	0	1	0
AK1	0	1	1	1	0	1	1	1
	xnor	xnor	xnor	xnor	xnor	xnor	xnor	xnor
DT1	1	1	0	0	1	0	1	0

EN2	0	1	0	0	1	0	0	1
AK2	0	1	0	0	1	1	0	0
	xnor	xnor	xnor	xnor	xnor	xnor	xnor	xnor
DT2	0	1	0	0	1	0	0	1

EN3	0	0	0	0	1	0	0	1
AK3	0	1	1	1	1	1	1	1
	xnor	xnor	xnor	xnor	xnor	xnor	xnor	xnor
DT3	0	0	0	0	1	0	0	1

EN3	0	0	0	0	0	0	1	1
AK3	0	0	1	1	0	0	1	1
	xnor	xnor	xnor	xnor	xnor	xnor	xnor	xnor
DT3	0	0	0	0	0	0	1	1

Each Decoded Text (DT) is equivalent to the transformed binary value and is proceeded as in encryption to obtain the binary value which is then converted to ASCII values to obtain the original message sent.

5. CONCLUSION

In this paper the cryptography and steganography techniques has been combined to transmit messages over secure medium; by making use of one user defined password to generate multiple auxiliary keys. The process of data hiding is achieved by making use of these Auxiliary keys which makes the data hiding more secure. This new process is an improvement over the existing pictorial based steganography technique as the messages are embed in the pictorial blocks on the basis of a password.

6. REFERENCES

[1] Yicong Zhou, Sos Agaian, "Image Encryption Using the Image Steganography Concept and PLIP Model" International Conference on System Science and Engineering, Macau, China - June 2011

[2] K. Pramitha, Dr. L.Padma Suresh, K.L.Shunmuganathan "Image Steganography using MOD-4 embedding algorithm based on imagecontrast" International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011)

[3] Ge Huayong, Huang Mingsheng, Wang Qian "Steganography and Steganalysis Based on Digital Image" 2011 4th International Congress on Image and Signal Processing

[4] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key", International Conference on Computer and Information Technology (ICCIT 2011) 22-24 December, 2011, Dhaka, Bangladesh

[5] Lauretha Rura, Biju Issac, Manas Kumar Haldar "Analysis of Image Steganography Techniques in Secure Online Voting", 20 II International Conference on Computer Science and Network Technology

[6] RigDas , Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding", 2012 IEEE

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

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