A Pictorial Block Steganography based Secure Algorithm for Data Transfer

Anupam Mondal, Sudipta Sahana, Sainik Kumar Mahata
Asst. Prof. Department of CSE, JIS College of Engineering,
Kalyani, Nadia, India Pin – 741235

Abstract
The growth of high speed communication networks and that of the Internet, in particular, has increased the ease of Information Communication. Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Steganography is mainly used to embed important information within images for encryption. This approach is better than cryptography in secure data Transfer. Original message is being hidden within a carrier like images or video in such a way that the change in image or video is not observable. So the hidden message is difficult to detect without retrieval. In today's world, with the advancement of science and technology, we have plenty of security tools which are developed to protect the transmission of multimedia objects. But the development of security approaches for text messages are comparatively less. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. In this paper, a secure pictorial block steganography based encryption and decryption algorithm is proposed to impose the concept of secrecy over privacy for transferring text messages.

Keywords
Steganography, Security, Cryptography, Encryption, Decryption.

1. Introduction
Steganography is the art and science of invisible communication of secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. Steganography's aim is to make the secret communication undetectable, that is, to hide the presence of the secret message. It modifies the carrier in an imperceptible way only so that it reveals nothing neither the embedding of a message nor the embedded message itself. The recent development of the Internet has brought new attention to steganography. The interest in steganography has been enhanced recently by the emergence of commercial espionage and the growing concerns about homeland security due to terrorism. We mainly emphasized on the data security based on steganography concept. There are many types of data hiding and data security concept, but in this paper we have proposed a new concept of data hiding using steganography concept with minimum complexity. The primary concept of data hiding is through cryptography which is based on appending approach with original data and a key. But in this paper we have looked several different types of steganography approach based on image, audio and video other than the basic cryptographic concept. Here we have

considered the data hiding mechanism within an image by using a technique where we have ensured the transmission security by means of complicated manipulation over the actual information regarding the unauthentic access at the time of transmission from sender to receiver end. Here we have introduced our new secure algorithm named as, "Pictorial Block Steganography Technique (PBST)"
The paper is organized as follow. Section 2 describes the different types of steganography Techniques. In Section 3 we have introduced the Pictorial Block Steganography techniques followed by an example in Section 4. Section 5 shows the Performance Evaluation. Finally, in Section 6 we have concluded our paper.

2. Related Work
To maintain security for transferring a confidential data from sender to receiver end, several different types of approaches have been made. Now days we are mainly concerned about different types of encryption and decryption algorithm (RSA, DES, IDEA, MD5 etc.) for sending original information from sender to receiver end. Steganography is a different approach, by which we can send information from sender to receiver end as hidden data within a carrier, that can an image, an audio, a video and else.

A.Daneshkhah et al. [1] proposed the two bits of message is embedded in a pixel in a way that not only the Least Significant Bit (LSB) of picture element is allowed to change but also the second bit plane and fourth bit plane are allowed to be manipulated, but the point is in each embedding process only one alternation in one bit plane is allowed to happen. It is compared by the method LSB-Matching, the results shows this method has an acceptable capacity of embedding data and hardly is detectable for steganalysis algorithm.

Elham Ghasemi et al. [2] presented the application of Wavelet Transform and Genetic Algorithm in a steganography scheme by employing a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the message and the frequency domain is utilized to improve the robustness of steganography.

A. Nag et. al. proposed the embedding process [3] to hide the data under the transformation (DWT and IDWT) of cover image and to obtain privacy, they have used Huffman encoding.

Q.Huang et al. [4] proposed the problem in LSB Matching Revisited (LSBMR) algorithm to make regions selection on images to find suitable area. By counting on each pixel we can decide if it should be protected. It can improve the visual imperceptibility and detectability of the LSB matching method. By adjusting the parameters of neighbor pixels, the max embedding capacity can be increased as needed.
P.Marwaha et al. [5] proposed the Cryptography and steganography are the most widely used techniques. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an un secure communication channel and are vulnerable to intruder attacks.

Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion.

A.Almohammad et al. [6] proposed the performance of both gray scale and color versions of a given cover image when they are used with a given steganography method. The capability and impact of using the chrominance components for data hiding. There are two steganography methods are used as test methods, JSteg and JMQT. As a result, using color images is better than using gray scale images for data hiding. Sarreshtedari et al. [7] proposed a high capacity method for transform domain image steganography and algorithm works 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. Jung and Yoo [8] down-sampled an input image to half of its size and then used a modified interpolation method, termed the neighbor mean interpolation (NMI), to up-sample the result back to its original dimensions ready for embedding. For the embedding process the up-sampled image was divided into 2x2 non-overlapping blocks. Piyu Tsai et al. [9] divided the image into blocks of 5x5, where the residual image is calculated using linear prediction. Then the secret data is embedded into the residual values, followed by block reconstruction. Histogram-based data hiding is another commonly used data hiding scheme. Li et al. [10] propose lossless data hiding using the difference value of adjacent pixels.

Y. C. Li et al. and M. C Chen proposed an image (spatial) domain, transform (frequency) domain and cover image in quantization format [11, 12]. In general, transform domain is more robust compared to image domain technique and cover image in quantization format. It eliminates the possibility of message being destroyed during the compression process when the excess image data is removed (lossy compression) and has lower computational cost compared to images in quantization format. Some of techniques of image steganography are described in the following section in more detail. In this paper, we have focused on secure data transfer by using image steganography with BTC (Block Transform Coding). We have applied here the stegofunction and key for secure data transfer.

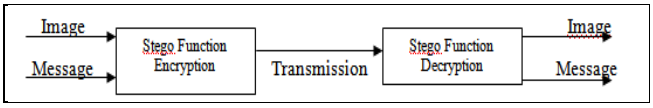

Fig 1: Functional Diagram

3. Pictorial Block Steganography Technique :

In this section we have described our Pictorial Block Steganography Technique (PBST). We have considered a grayscale image first, where we can encrypt the original information. In this paper the original information first converted into its corresponding ASCII value and the length of information have been calculated. After using binary conversion we have divided the binary number into 8 bit block segment. The initial gray scale image (256×256 i.e. 28×28) first converted into block size of (8×8) using block truncation coding (BTC). Then we have converted it into binary format using binary conversion and merge the original information into the decomposed matrices by the following encryption algorithm. Now we have sent this coded image towards the receiver end. At receiver section the reverse technique is followed to decompose the image matrix to easily retrieve the original information by the following decryption algorithm.

3.1 Encryption Technique:

Step 1: Taken an input string of information is known as a plain text.

Step 2: Calculate the number of character without Space stored in a variable of PT.

Step 3: Convert the PT string to ASCII value character by character and convert those characters to equivalent binary bits.

Step 4: Divide the binary bits in several blocks where every block was considering n numbers of bit.

Step 5: After that we were taken a gray scale image with dimension 2^n x 2^n.

Step 6: Apply the partial Block Truncation Coding on this gray scale image with n x n size block matrix, where every block of this matrix size $2^{(n-p)}$ x $2^{(n-p)}$ (where, n= 2^p).

Step 7: Convert this gray scale image to bit map image.

Step 8: After taking the 1^{st} block of the PT, we have considered the following steps.

Step 9: Now 1^{st} block 1^{st} bit placed into 1^{st} image block (0, 0 position), 1^{st} block 2^{nd} bit placed into 2^{nd} image block (0, 0 position) and continue this procedure for 1^{st} block of text with n time recursively. Next time for the rest of the text block we were considering next row of the image recursively with (0, 0 position).

Step 10: Convert the entire changed binary image to gray scale image.

Step 11: Forward this gray scale image along with the unique dimension of each logical decomposed matrix block to the receiver.

3.2 Decryption Technique:

Step 1: Convert the gray scale image to binary image (bit map image).

Step 2: Apply the partial Block Truncation Coding with this binary image with n x n size block matrix, where every block of this matrix size $2^{(n-p)}$ x $2^{(n-p)}$ (where, n= 2^p).

Step 3: Then taken the binary value of the 1^{st} position (0, 0) from every block ($2^{(n-p)}$ x $2^{(n-p)}$) row wise.

Step 4: Then divided those bits in several blocks with n numbers of bit.

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

Step 6: If the decimal number is zero
Discard the number
Else
Convert the decimal number (ASCII value) to character.

Step 7: These set of characters are the ultimate information was forwarded by the sender.

4. Example

Suppose a word "IT" is required to transmit. Here number of character in the message is 2 and it is less than 8. To adjust it as a message of character length 8 it turns into "IT000000". Now converting only the characters into the message to their ASCII values and store into an array. The original message takes form as:

73	84	0	0	0	0	0	0

Now again each and every array elements are transformed into equivalent 8 bit binary form as the total character length of the message is now 64. The matrix values will be formed as:

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

Now a gray scale image is chosen in which this binary message is merged:

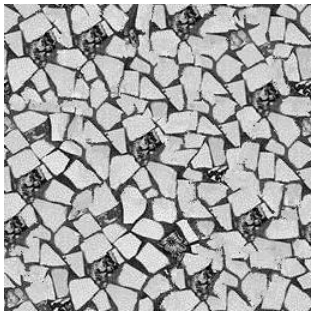

Fig 2: Gray scale image

Then that image is converted to equivalent binary image matrix. Suppose dimension of the image matrix is 256 x 256 (say). Then this matrix will be completely logically decomposed into some 8x8 square matrices as follows

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

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

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

We have to embed the original message within the gray scale image. Now according to our encryption algorithm we have replaced all b00 position of each 8x8 block matrix according to the message representation above. i.e. the first row our character matrix value will be inserted as b00 of B00 will be 0, b00 of B01 will be 1, b00 of B02 will be 0, b00 of B03 will be 0 in this way up to 7th Colum. For second row b00 of B10 will be 0, b00 of B11 will be 1, b00 of B12 will be 0, b00 of B13 will be 1 in this way up to 7th Colum. Rest of all b00 position of all 8x8 block will be 0. After getting the full matrix we convert it into its corresponding gray scale image for transmission. For the receiver section the original message can be fetched easily using the decryption algorithm.

5. Performance Evaluation:

For secure data transfer several different types of steganography techniques are present mainly based on logical invisibility attributes. Here in this paper we are mainly concerned the logical invisibility based on partial Block Truncation Coding (PBTC).

Logical invisibility means hide the data within a different of data format. In this section after embedding data in an image we have compared it with the original image and checked the visual differences. Based on Average Mean Squared Error (MSE) we have compared our PBST with Least Significant Bit (LSB) steganography technique with respect to size of the image. Moreover, measurement of the Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) of stego image with respect to the original image based on the following equation,

$$MSE= (1/(H \times W))\sum(O[i][j] - P[i][j])$$

Where, H= Height, W= Width, O[i][j]= Original image & P[i][j]= Stego image.

$$PSNR= 10\log10 (L2 / MSE)$$

Where, L= Peak signal label of gray scale image.

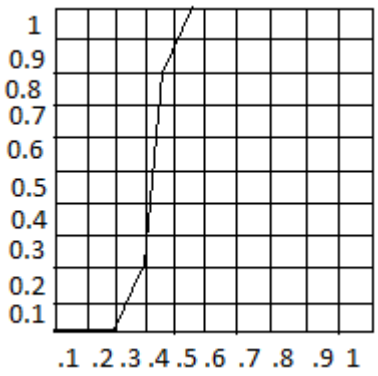

Fig 3: Average MSE mapping between LSB & PBTC technique

6. Conclusion:

In this paper, we have introduced a new method of utilizing the concept of image steganography for message encryption, namely Pictorial Block Steganography Technique for encrypting the original message by concealing it into a cover image using a specific encryption process. As an example of this new idea, we have introduced an encryption algorithm called the PBST image steganography algorithm. The main objective of this paper is given on the privacy of information to be transferred. So, to obtain this we have used the block steganography concept. The new algorithm is more efficient as the text is hidden within the image without any deformation of the image. No additional key is used here in this algorithm. The new approach can be available to use on any type of the character to work with it as the corresponding number system has to be chosen (ASCII).

References

[1] Ali Daneshkhah, Hassan Aghaeinia and Seyed Hamed Seyedi, "A More Secure Steganography Method in Spatial Domain", Second International Conference on Intelligent Systems, Modelling andSimulation, 2011.

[2] E. Ghasemi, J. Shanbehzadeh , N. Fassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm," International MultiConference of Engineers and Computer Scientists, vol. 1, 2011.

[3] A. Nag, S. Biswas, D. Sarkar, P. P.Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding," International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6),pp. 497-610,2011.

[4] Qinhua Huang and Weimin Ouyang, "Protect Fragile Regions in Steganography LSB Embedding", 3rd International Symposium on Knowledge Acquisition and Modelling, 2010.

[5] Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in images", 2nd International conference on Computing, Communication and Networking Technologies, 2010.

[6] Adel Almohammad and Gheorghita Ghinea, "Image Steganography and Chrominance Components", 10th IEEE International Conferenceon Computer and Information Technology, 2010.

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

[8] K.H. Jung, K.Y. Yoo, Data hiding method using image interpolation, Computer Standards and Interfaces 31 (2) (2009) 465-470.

[9] 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.

[10] Z. Li, X. Chen, X. Pan, X. Zeng, Lossless data hiding scheme based on adjacent pixel difference, in: Proceedings of the International Conference on Computer Engineering and Technology, 2009, pp. 588-592.

[11] Y. C. Li, P. Tsai, C. H. Lin, H. L. Yeh, C. T. Huang ,"Palette Partition Based Data Hiding for Color Images," Intelligent Information Hiding and Multimedia Signal Processing, 2009. lIH-MSP '09. Fifth International Conference, pp.620-623, 12- 14 Sept. 2009.

[12] M. C Chen, S. Agaian, P. Chen, "Generalized Collage Steganography on Images ", IEEE International Conference on Systems, Man and Cybernetics (SMC), IEEE, 2008.