Multilevel Data Encryption Using Hadamard Transform Based Image Steganography

Shweta Dahiya
Student
Dept. of Electronics & Comm., Bhagat Phool Singh Mahila Vishwavidalaya, Khanpur Kalan, Sonepat, India

***Abstract*— The major goal of this investigation is to design an effective and more secure image steganography algorithm using cryptographic algorithm named multi-level encryption. It is an improved report of existing single level encryption algorithm. In this investigation, the focus of concern is image because it is widely used in internet and also in mobile system. Enhanced Linear Significant Bit (LSB) algorithm can easily be executed and do not corrupt the image to the point of being noticeable. It would appear that improved LSB using Hadamard multi-level transform is more suitable algorithm of steganography due to its security. Using improved LSB algorithm we can exchange secret messages over public channel in a safe way. The proposed method is more secure than previous method which uses only simple encryption because it is totally relied on the number of 1's in the equivalent binary value of the key.**

***Keywords*— Steganography, Encryption, LSB, Hadamard Transform, Image Processing.**

I. INTRODUCTION

Steganography is a method of hiding one form of information into another form of information. It is way of encoding some important information in such manner that the existence of the information is invisible. When some important information is inserted then it is known as stego-medium. A stego-key is utilized for encoding/hiding process which is used to restrict detection or extraction of the embedded data [Al-Shatnawi Atallah et al., 2012; Gunda Sai Charan et al., 2015; Parmar Ajit Kumar Maganbhai et al., 2015].
Steganography consists of three elements:

1. cover image
2. the secret message and
3. the stegano-image

Cover image is used to hide the information and stegano image is used to help the cover object with message embedded inside it.
Steganalysis is a system to detect the existence of steganography [Asad Muhammad et al., 2011; Khan Muhammad et al., 2015]. In this method, sender should choose the suitable message carrier before the hiding process and then it chooses efficient secret information as well as password. The effective and suitable steganography algorithm should be chosen so that it will able to encode the message in more safe approach and this is why the sender can send the files by other modern approach such as email, chatting or by some other mean. [Al-Shatnawi Atallah et al., 2012].
The various steganography techniques are described below:

(i) Text Steganography: In text steganography, information is hidden in text file. This is the most common process of steganography. In this method, secret message is hidden into text message. Text steganography do not use digital file very often as text files have a very less amount of excess data [T. Morkel et al., 2005].

(ii) Image Steganography: In image steganography, image may be utilized as the cover medium. A message is inserted in digital image by utilizing an embedding algorithm using the secret key. The final resultant images are then sent to the receiver. On the other hand, it is then processed by the extraction algorithm utilizing the same key. On the transmission of image, person can only notice the image received but can't see the existence of the hidden message [Li Bin et al., 2011].

(iii) Audio Steganography: Audio steganography is troubled with inserting information in a safe cover speech in a protected and vigorous manner. Commonly used method for audio steganography are: LSB coding, parity coding, phase coding, spread spectrum and echo hiding [Gunda Sai Charan et al., 2015].

Image steganography has been used in this study:

Image steganography is a technique which is used to hide secret message within an image. The binary bits of secret message are hidden in the binary of image and this slightly affects the intensities of colour or brightness which is not detectable by naked human eyes [T. Morkel et al., 2005; Kulsoom Ayesha et al., 2016]. There are many algorithms which are used for image steganography but

some of them are very complex while some of them are simple. Images are the most popular cover objects used for steganography. A simple image steganographic model contains an original image called cover image (I), in which secret message/image (M) is hidden and a stego key (K) which is used to hide the information as well as to extract. The purpose of using stego key is to provide security. Finally, after the steganographic process, an image is obtained called stego-image (S) in which pixel value is different from the pixel value of original image but these changes are so minor that they cannot be easily detected by human eyes [Lionel Fillatre et al., 2012 ; Swain Gandharba et al., 2012].

A simple steganographic model is depicted in figure 1, where function 'f' indicates any image steganographic algorithm. Least Significant Bit (LSB) image steganography [Li Bin et al., 2011] algorithm is used to return the LSB of the image in which secret message is to be hidden called cover image with the Most Significant Bits (MSB) of secret message to be hidden without changing the statistical property of the cover image significantly [Khan Muhammad et al., 2015; B. Srinivasan et al., 2015].

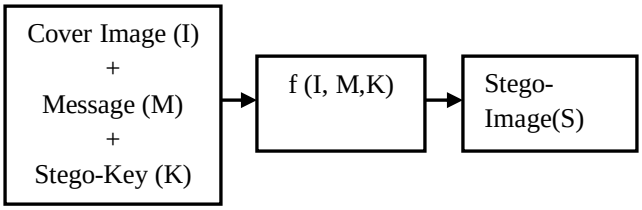

Figure 1: Simple Steganographic Model [Parmar Ajit Kumar Maganbhai et al., 2015]

A digital image utilize 2-dimensional matrix of the colour intestines at every grid pixel. Generally, grey images use only 8 bits but on the other side 24 bits is used for colour model like RGB model [Al-Shatnawi Atallah et al., 2012].

The steganography system that utilizes an image as cover, there are various approaches to hide information inside cover-image:

(a) Spatial Domain.

(b) Frequency Domain.

In the spatial domain approach, bit value of the cover image is manipulated to insert the secret message. The secret bits are written directly to the cover image pixel bytes. As a result, it can be concluded that the spatial domain approach is simple and easy to execute. [Hamid Nagham et al., 2012; Rig Das et al., 2012]

II. OBJECTIVES

The main purpose of this work is to design and develop an efficient and more secure image steganography algorithm using cryptographic algorithm named multilevel encryption, which is an enhanced version of existing single level encryption algorithm.

Efforts will be made to enhance and improve the existing LSB image steganography algorithm and to deduce a more secure combined approach of these two cryptography algorithm named multilevel encryption and image steganography algorithm improved LSB. Moreover comparative study of existing algorithms and analysis of the combined approach of cryptography and steganography will be carried out.

III. RELATED WORK

Following literature survey have been carried out in context of present study as depicted in Table 1.

Table 1: Related Work in Context of Present Study

Parameters	Researchers
LSB Substitution based image steganography	Chi-Kwong Chan and L.M. Cheng [2003]; Champakamala B.S et al.[2005]; Saeed R Khosravirad et al. [2009]; Yogendra Kumar Jain and R. R. Ahirwal[2010]; Luo Weiqi et al. [2010]; Ekta Walia et al.[2010]; Karim S. M. Masud et al. [2011]; Asad Muhammad et al.[2011]; Shailender Gupta et al.[2012]; Koushik Dasgupta et al.[2012]; Lionel Fillatre[2012]; Mandal J. K. and Debashis Das[2012]; Swain Gandharba et al.[2012]; Parisa Gerami et al.[2012]; Ankit Chadha et al.[2013]; Khan Muhammad et al.[2015]; Gunda Sai Charan et al.[2015]; Marghny H. Mohamed and Loay M. Mohamed [2016]
Pixel based color image steganography	Da- Cun Wu and Wen-Hsiang Tsai [2003]; Ko-Chin Chang et al. [2008]; Tomas Pevny et al.[2010]; Mandal J. K. and Debashis Das[2012]; Al-Shatnawi Atallah et al.[2012]; B. Srinivasan et al. [2015]
Huffman coding based image steganography	Amitava Nag et al.[2010]; Rig Das et al.[2012]
Multil level image steganography	Gunda Sai Charan et al.[2015]; Pallavi H. Dixit et al. [2015]; Arun

	K. et al. [2015]; Rani et al. [2016]
Bio-inspired methods based steganography	Ghasemi Elham et al.[2011]; Parisa Gerami et al.[2012]; Chakravarthy Sudharshan et al. [2016]; Kulsoom Ayesha et al. [2016]
Surveys and Comparisons	A. Martin et al. [2005]; Li Bin et al.[2011]; Hamid Nagham et al.[2012]; R. Amirtharajan et al.[2010]; Hariri Mehdi et al.[2011]
Image transposition based steganography	Muhammad Khan et al. [2015]

After a brief review of literature survey, in forthcoming section framework for present investigation is presented.

IV. FRAMEWORK FOR PRESENT INVESTIGATION

The Hadamard transform-based signature template satisfies the needs of inevitability and diversity for steganography. Also, the method is efficient for transforming resultant stego image and the parameter key in a less space. The proposed method is evaluated using the images. The proposed Hadamard transform-based approach can be argued as a special case of dynamic projection for the steganographys, however, compared to conventional projection, the method gives a simple yet effective way of secure transformation during retaining mostly recognition performance. Hadamard transform- based signature template design is presented in this section. Firstly, preliminaries on Hadamard transform are presented. Then, next apply the partial Hadamard transform to binary string's frequency-domains. So, wrap up the section with signature template matching in transformed domain.

The Hadamard transform is a orthogonal transformation non-sinusoidal whose base is created with walsh functions. These walsh functions are square or rectangular waveforms with the values of +1 or -1. The Hadamard transform contains no multipliers in real because the amplitude of walsh functions is only two values, +1 or -1. A Hadamard matrix is defined as a matrix having elements ±1 and row vectors pair wise orthogonal [Harwit M., 2012; Parvinder Kaur and Deepika, 2016].

(i) Chaos Theory

This theory relates to the system that has diverging outcomes for little variation in the initial conditions. In this method chaotic sequence is developed by using logistic map method. The chaotic maps are defined using equation (1):

$$X_{k+1} = \mu X_k(1- X_k) \qquad (1)$$

Where, Xk is current chaotic sequence and μ is the change coefficient.

(ii) Ceaser Cipher Technique

In this scheme, each alphabet is replaced with another alphabet which is placed at fixed distance. It is one of the substitution encryption techniques.

(iii) Chaotic Encryption

In chaotic encryption secret text of size LxB is divided into L parts of size 1 x B. In this algorithm, the colour images are considered. Each cover pixel has 3 bytes, hence each part has N=W*3 bytes. Now take each part at a time and consider some initial conditions for μ, x and generate chaotic sequence Xk, k=0, 1, 2 ... N-l for each part using chaotic maps developed using equation (1). Then find arithmetic mean (T) of chaotic sequence generated. Then generate binary bit sequence Bk for each part by comparing each Xk with T in such a way that if Xk > T then Bk =1 else Bk =0. Then each byte of secret is made XOR with its corresponding Bk. In this way each part is encrypted with different initial conditions of μ, x. Then all parts are merged into cipher text [Gunda Sai Charan et al. 2015].

(iv) XOR Algorithm

The combined approach of steganography and cryptography play an important role in information security because if someone detect the presence of secret message in any media file, then this information cannot be directly used due to its encryption form. So, neither steganography nor cryptography is alone better. Cryptography provides security to information. There are many algorithms, some of these take more space and some of these take less time such as XOR, AES, DES, TDES, Blowfish and RSA [A.K. Mandal and C. Prakash, 2012]. XOR algorithm is simple one and it takes less space but slightly more time than other. So, XOR algorithm can be used for enhancement because it has less time complexity. XOR encryption algorithm is simple algorithm because it performs only XOR operation between the bit of key and plain text. It first convert plain text and key to their equivalent binary value, then XOR operation is performed between binary value of key and plain text, called encryption. Decryption is same as encryption and it is performed again XORing of the binary value cipher text and key. In it, cipher text takes equal space as original plain text. XOR algorithm can work only on binary signals or values and encrypts each pixel separately because image is made up of a lot of pixels and each element (character, symbol, number etc) of information can be converted into binary value.

XOR algorithm is also suitable for multimedia data such audio, video and image but pixels which are in multimedia are highly correlated. Pixels values can be redistributed to different location by using affine transformation with XOR operation. Scrambling of

plain text/image can be performed using XOR encryption with Modulo-256 addition operations for two rounds independent of chaotic map and no iteration method is used in any chaotic map for scrambling [A. Nag et al., 2011].

Algorithm for Embedding:

1. Take the secret image of size LxB and divided into L parts of size 1 x B.
2. For each part generate binary bit sequence as described in chaotic sequence.
3. Apply XOR operation for each byte of secret text with bit of sequence generated for corresponding part.
4. Repeat step 3 for all parts of secret text.
5. Encrypted secret text is embedded using 3, 3, 2 LSB replacement technique.
6. Stego image is formed.

In 3, 3, 2 LSB replacement technique each 8 bits of secret text is embedded in one pixel of cover image. In RGB image, each pixel will consist of 3 bytes. Therefore, first 3 bits are replaced with 3 LSB bits of red byte, next 3 bits are replaced with 3 LSB bits of green byte and last 2 bits are replaced with 2 LSB bits of blue byte. This technique is based on the fact that if little amount of variation occurs in blue then it will have huge effect on human eye, in comparison to change in red and green pixels. For replacement, LSB positions are acquired by using hash function which is expressed using equation (2):

$$k = p \,\%\, n \qquad (2)$$

Where, 'k' represents LSB bit position of corresponding byte to be replaced;
'p' represents position of bit to be embedded in secret byte;
'n' represents no. of bits in RGB pixel.

Procedure for 3, 3, 2 LSB replacement technique is as follows:

1. Recognize the four LSB bits of each of red, green, blue bytes of each pixel of the cover image.
2. Embed eight bits of secret bits into the corresponding cover image pixel in the positions obtained by hash function.
3. Eventually, obtain stego image.

In 3, 3, 2 LSB technique odd numbered parts are considered first then even numbered parts are considered for encoding as well as decoding.

Secret bits are obtained from LSB bits of stego image pixel during the process of decoding. Then secret image is divided into parts and for each part binary bit sequences are generated as described in algorithm for embedding with their respective initial conditions for μ, x. Then, for each byte of secret image with single bit of binary bit sequence of corresponding secret part XOR operation is applied. For all parts of encrypted secret text this process is repeated. Each and every part of secret text are merged together to form original secret text.

In the forthcoming section the result and discussion is presented.

V. RESULTS

This section presents the experimental results based on various image quality assessment metrics for performance evaluation. LSB using Hadamard transform- based method is compared with simple LSB. We have embedded a text file in different standard colour images like Lena, Castle and Chilly. The results are demonstrated in terms of measuring parameters i.e. PSNR. This is used for the accuracy of the image Peak Signal to Noise Ratio (PSNR). Usually, the image steganography system should insert the unseen information in the image. It can be ascertained that the chances of visual attack by human eye decreases as the PSNR value increases. PSNR ratio is used as a quality measurement between the base image and the proposed image as shown in figure 2, 3 and 4 respectively. The images are of best quality if PSNR ratio is high.

PSNR is defined using equation (3) and (4) respectively:

$$PSNR = 10 \log_{10} \frac{(L-1)^2}{RMS} \qquad (3)$$

Where RMS is defined as,

$$RMS = \frac{1}{m.n} \sum_{i=1}^{m} \sum_{j=1}^{n} (X_{i,j} - X'_{i,j})^2 \qquad (4)$$

Here, 'm' and 'n' show image dimensions, 'i' and 'j' are loop counters, X' is the cover image and X is the stego image [Muhammad Khan *et al.*, 2015; B. Srinivasan *et al.* 2015].

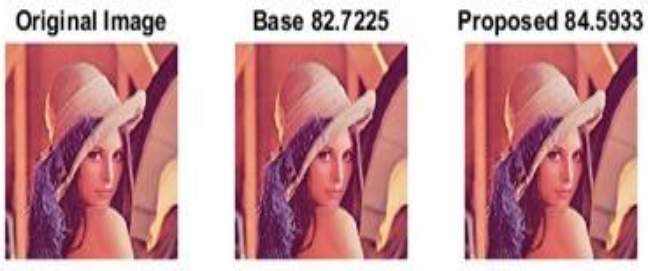

Fig.2: Lena Image steganography PSNR comparison between base and proposed methods

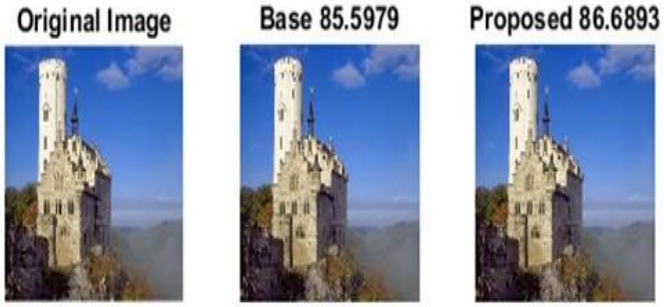

Fig.3: Castle Image steganography PSNR comparison between base and proposed methods

Fig. 4: Chilly Image steganography PSNR comparison between base and proposed methods

The proposed system test result for three different images with their PSNR values are shown in Table 2.

Table 2: PSNR Comparison of Simple LSB with proposed method

Secret Image	PSNR (dB) of Simple LSB	PSNR (dB) of Proposed method
Lena	82.7225	84.5933
Castle	85.5979	86.6893
Chilly	83.0037	84.465

VI. FINDING OF THE STUDY

The findings of study are as follows:

1. LSB using Hadamard transform- based method is more secure than simple LSB algorithm because it is an iterative version of base method and iteration is totally dependent on the numbers of 1's in the equivalent binary value of the key.
2. Hadamard transform- based method also uses modulo concept which makes it more secure but it takes more time than simple LSB method because encryption is done in one by one iterative process.

3. Basically, it is working for documents, so it can be further enhanced to encrypt image, audio, video and other formats of information.

VII. CONCLUSION

On the basis of the results presented, it can be observed that the value of PSNR has improved in comparison of existing LSB algorithm. Due to which, the process of detection of hidden information becomes difficult. And if someone is able to find it then it cannot be used further, because of its encrypted form which is performed by Hadamard transform- based encryption algorithm. So, combined approach of cryptography and steganography provides more security to information.

VIII. FUTURE SCOPE

Now days, image steganography is broadly used in steganography field. Processing time and complexity of Hadamard transform-based method can be reduced. Both the algorithms can be used, proposed method and improved LSB with other cryptographic algorithms and steganographic algorithms which can reduce the space and time complexity and increase the level of security.

REFERENCES

[1] Morkel, T., J.H.P. Eloff and M.S. Olivier, "An overview of image steganography," Proceedings of the Fifth Annual InformatioN Security South Africa Conference (ISSA), 2005.

[2] Asad, Muhhamad, Junaid Gilani and Adnan Khalid, "An enhanced least significant bit modification technique for audio steganography," International Conference on Computer Networks and Information Technology (ICCNIT), pp. 143-147, IEEE, 2011.

[3] Li, Bin, Junhui He, Jiwu Huang and Yun Qing Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142-172, 2011.

[4] Nag, A., Singh, J.P., Khan, S., Ghosh, S., Biswas, S., Sarkar, D. and Sarkar, P. P, "Image Encryption Using Affine Transformation and XOR Operation," International Conference of Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), pp. 309-312, 2011.

[5] Mandal, A. K., and Parakash, C, "Performance Evaluation of Cryptographic Algorithms: DES and AES," Students Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[6] Rig Das and Themrichon Tuithung "A novel steganography method for image based on Huffman Encoding," Emerging Trends and Applications in Computer Science (NCETACS), 3rd National Conference, IEEE, pp. 14-18, 2012.

[7] Al-Shatnawi, Atallah M, "A new method in image steganography with improved image quality," Applied Mathematical Sciences, vol. 6, no. 79, pp. 3907-3915, 2012.

[8] Fillatre, Lionel, "Adaptive steganalysis of least significant bit replacement in grayscale natural images," Transactions on Signal Processing, vol. 60, no. 2, pp. 556-569, IEEE, 2012.

[9] Swain, Gandharba, and Saroj Kumar Lenka, "LSB array based image steganography technique by exploring the four least significant bits," Global Trends in Information Systems and Software Applications, pp: 479-488, Springer Berlin Heidelberg, 2012.

[10] Hamid, Nagham, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi, "Image steganography techniques: an overview," International Journal of Computer Science and Security (IJCSS), vol. 6, no. 3, pp. 168-187, 2012.

[11] Harwit M. Hadamard "Transform optics," Elsevier, 2012.

[12] Charan, Gunda Sai, S. S. V. Nithin Kumar, B. Karthikeyan, V. Vaithiyanathan, and K. Divya Lakshmi, "A novel LSB based image steganography with multi-level encryption," International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1-5, IEEE, 2015.

[13] Muhammad, Khan, Muhammad Sajjad, Irfan Mehmood, Seungmin Rho, and Sung Wook Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimedia Tools and Applications, pp. 1-27, 2015.

[14] Srinivasan, B., S. Arunkumar, and K. Rajesh, "A novel approach for color image, steganography using nubasi and randomized, secret sharing algorithm," Indian Journal of Science and Technology, vol. 8, no. S7, pp. 228-235, 2015.

[15] Maganbhai, Parmar Ajit Kumar, Prof. Krishna Chouhan, "A Study and Literature Review on Image Steganography," International Journal of Computer Science and Information Technologies (IJCSIT), vol. 6, no. 1, pp. 685-688, 2015.

[16] Muhammad, Khan, Jamil Ahmad, Muhammad Sajjad, and Muhammad Zubair, "Secure Image Steganography using Cryptography and Image Transposition," NED University Journal of Research, 2015.

[17] Deepika, and Parvinder Kaur, "Non-invertible secure template generation for online signature verification," International Journal of Engineering Development and Research, vol. 4, no. 2, pp. 968-973, 2016

[18] Kulsoom, Ayesha, Di Xiao, and Syed Ali Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," Multimedia Tools and Applications, vol. 75, no. 1, pp. 1-23, 2016.