A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication

Kamaldeep Joshi[1], Rajkumar Yadav[2]
[1, 2]Department of Computer Science and Engineering
University Institute of Engineering and Technology, Rohtak, India
[1]kamalmintwal@gmial.com, [2]rajyadav76@rediffmail.com

***Abstract*— In this paper, a new method of image steganography in spatial domain on gray images blend with cryptography is present. Steganography and cryptography are used to hide message and its meaning respectively. By this method, the message is first encrypted using Vernam cipher algorithm and then the message (encrypted) is embedded inside an image using the new image steganography method i.e. LSB with Shifting (LSB-S). In LSB-S method we have used four LSB of the pixel and performed circular Left shift operation and XOR operation. The combinations of Cryptography and steganography method enhance the security of embedded data. After implementation the proposed method it is checked on the different parameter such as PSNR and MSE and got good results.**

Keywords LSB; LSB-S; Image Steganography; Cryptography; PSNR; MSE.

I. INTRODUCTION AND LITERATURE SURVAY

Steganography is the method of hiding the existence of data from others [1]. It is the art and science of secure communication [2]. The main purpose of steganography is secure data transfer over the internet [3]. Many different file carriers are used to hide the data in steganography like- image, audio, video, text[4]. In image steganography the cover media is an image. In audio steganography the cover media is any audio file, In text steganography the cover media is text file and in video steganography technique the cover media is video file [5]. For hiding the data in images different steganography technique are existed with low complexity than others and respective weak and strong points [6]. For more secure data transfer cryptography is used with steganography. In cryptography the message is encrypts with encryption algorithm with secret key and transfer it to the other end then receiver decrypt it and get original message by using decryption algorithm[7]. There are many algorithms presented in the literature. LSB is one of the most popular and easiest methods of data hiding. LSB (Least significant Bit) algorithm [8], replaces the least significant bit in the cover file according to the message bit. This is most popular technique used in steganography to hide the message. This is usually an effective technique, as LSB substitution doesn't cause significant quality degradation [9].The main disadvantages of the LSB method is that if the intruder extracts the entire LSB bits, he can get the full message as the message is hidden in the LSB bit. Parvinder et al. propose a scheme which used 6^{th} and 7^{th} bit for hiding the data. This method removes the disadvantage of LSB as data is not hidden on LSB. But the capacity of hiding the data was only 50% [10]. After that Rishi et al. proposed a method which removed the limitation of the method proposed by Parvinder et al. but it has also limitations i.e. the capacity if this method is 85.93[11]. Rajkumar et al. proposed another method based on parity of the pixel. In that method the message is hidden on the bases of parity i.e. if the parity is odd hide zero and if the parity is even hide one. The data hiding capacity of this method is capacity of this method is 98.82 [12]. Also this method is easy to break by hit and trail method. Only one gauss is required for breaking the algorithm i.e. whether the value of pixel is having odd parity or even parity. If the parity is odd extract zero otherwise retrieve one.

II. THE PROPOSED METHOD

This proposed work consists of two steps, first the data is encrypted using vernam cipher [13], secondly hide the encrypted data using LSB-S method given by the algorithm section. This paper consists of a structure of hiding the message in two layers. First layer hides the data using cryptography (Vernam cipher) and the second layer hides data, the scrambled data received from previous layer, using the new LSB-S algorithm with the benefits of perceptual degradation and message capacity. The new steganography method is combined with the existing cryptographic method so that it increases the security of the data. In this structured work, first encrypt the data with transposition cipher then the encrypted message is hidden inside an image using our LSB with shifting embedding method (given by the algorithm below). Hiding data by simple LSB is not very secure. The grouping of these two approaches enhances the security of data. The combination of these two methods will satisfy the requirement such as capacity and security for data transmission over an open channel. If the attacker were able to detect the steganography technique, he would still have to require the cryptographic decoding way to de-cipher the encrypted message and vice versa.

A. Proposed Architecture

In this section, architecture of the proposed work has been given. This architecture shows the operations performed on the secret message. Figure 1 shows the proposed architecture.

B. Assumption

- Sender and receiver share the same one time pad key for Vernam cipher algorithm.
- Receiver knows the algorithm for encryption.

978-1-5090-0148-4/15/$31.00© 2015 IEEE

- Cover media in which message will be hidden is chosen on mutual consent of sender and receiver.
- Receiver knows the algorithm for steganography using which sender hides the message.
- Receiver knows the length of the hidden.

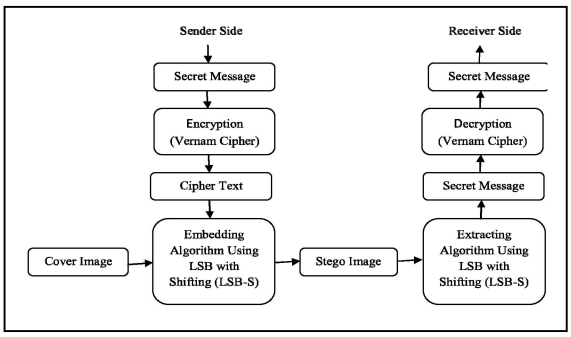

Fig. 1. Architecture of the proposed work

C. *Proposed Algorithm*

This section contains the insertion as well as retrieval algorithm for proposed method.

Insertion Algorithm

- Take a gray scale image i.e. I.
- Take the message and convert it into cipher text by Vernam cipher and store it in the form of bit in M.
- perform the followings

  1. Extract the four LSB Bits in a Temporary matrix T1 of pixel and perform 1-Bit circular left shift over these bit and again store them in Temporary matrix T1. Shift on next element of T1 by increasing 1 in present location.

  2. Get the LSB of first element in T1 from and perform XOR with 1st message bit from message matrix. Decrease the length of message by 1.
- Store the result obtained previous step in I at first pixel's LSB and Shift on next element of I by increasing 1 in present location.
- Repeat step 3 till length of M=0;
- Stop

Retrieval Algorithm

- Take Stego-Image and extract all the pixel i.e. embedded pixels
- Perform 1-Bit circular left shift operation over 4-LSB bits of these pixels and get the rotated pixel. Store these shafted pixels in a matrix T2.
- Perform XOR of

  1. LSB bit of 1st embedded pixel of Stego image with LSB bit of corresponding shifted pixel from T2.
- Repeat step 3 for whole message, as receiver knows the message length.
- After XOR operation, the corresponding message bit will be got. Which is the required encrypted message? Convert this message into character form.
- Apply Vernam cipher decoding algorithm to decrypt the received message.
- Finally the secret message will be received.

D. *Simple Example of the Proposed Method*

The The LSB-S method is explained using a simple example. Consider an image 2*2 image I and a decrypted message after Vernam cipher is M1*4. = [1010]. To embed M into I, we have to follow the insertion algorithm.

Let $I=\begin{bmatrix}106 & 122\\ 201 & 103\end{bmatrix}$. the binary equivalent of I is

$I_{BIN}=\begin{bmatrix}01101010 & 01111010\\ 11001001 & 01100111\end{bmatrix}$.

Last 4 bit of I_{BIN} i.e. $T1=\begin{bmatrix}1010 & 1010\\ 1001 & 0111\end{bmatrix}$.

1-bit circular left shift of $T1=\begin{bmatrix}0101 & 0101\\ 0011 & 1110\end{bmatrix}$.

LSB of $T1=\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}$. The result of T1 is XORed with M can be given as $S=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$.

Replace the LSB of I by S we get the Stego pixels i.e. $\begin{bmatrix}01101010 & 01111011\\ 11001011 & 01100110\end{bmatrix}$.

The value in decimal is=$\begin{bmatrix}106 & 123\\ 202 & 102\end{bmatrix}$.

For getting [1010] the retrieval algorithm is followed.

III. Experimental Results

The proposed algorithm was implemented in MATLAB. For this experiment four standard image having size 256*256 were taken from USC-SIPI-ID [14] database. For simplification these images have been converted into 256*256 sizes. The size of the message was taken as 1KB, 2KB and 4 KB. PSNR and MSE were calculated for every cover and Stego image by the formula given by the equation 1 and 2 respectively.

A. *PSNR and MSE*

The PSNR (Peak Signal to Noise Ratio) is the parameter that accesses the quality of Stego image with respect to the original image. It calculates the imperceptibility of the Stego image. In simple form we can say that it calculates and analyzes that how much similar two images are i.e. the similarity between Stego image and original image [15]. Higher the value of PSNR of stego image higher will be the quality of Stego image or we can say that higher will be the

imperceptibility of hidden message behind the pixels of an image. The formula for PSNR calculation is described below

MSE (Mean Square Error) is the parameter that calculates the magnitude of average error between the original image and stego image. The difference between the observed values of original and stego image are squared and then their average is calculated [16]. RMSE is used mainly in case of large errors because it provides relatively high weight to these errors. So, RMSE is very demanding when large errors are undesirable in carrier file. The small we get the value of RMSE higher will be the quality of system. The formula for calculation of MSE is depicted below.

$$PSNR = 10\log_{10}\left[\frac{I^2}{MSE}\right] \quad (1)$$

$$MSE = \frac{1}{[R \times C]^2}\sum_{i=1}^{N}\sum_{j=1}^{M}(X_{ij} - Y_{ij})^2 \quad (2)$$

Where:

Here, I, represents the maximum possible value of the pixel in the image. For example for a gray scale image the maximum value is 255. MSE is the mean square error. R and C are the no of rows and no of columns in cover image. Xij, is the intensity of Xij th pixel in cover image. Yij is the intensity of Yij th pixel in Stego image.

B. Peformance Analysis

After performing implementation of the proposed work, the algorithm was analysed on the bases of PSNR MSE and Imperceptibility. Figure 2, 3 and 4 show the cover image of Lena and its corresponding Stego image with their histograms. Table 1 shows the performance of the method with respect to PSNR and MSE. Similarly the figure 4, 5, and 6 and table 2 show the performance of the method on Baboon image. This method was also tested on peppers and triffy images and the result is given in the figure 7, 8, 9 and 10, 11, 12 respectively. The table 3 and 4 show the PSNR and MSE of Peppers and Triffy images.

C. Result of Lena image

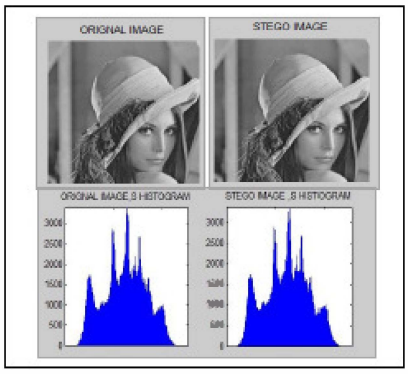

Fig. 2. Original and Stego Image for message size 1024 bits, Histogram for message size 1024 bits

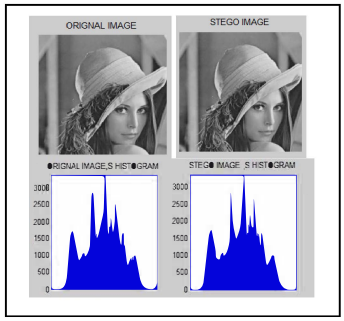

Fig. 3. Original and Stego Image for message size 2048 bits, Histogram for message size 2048 bits

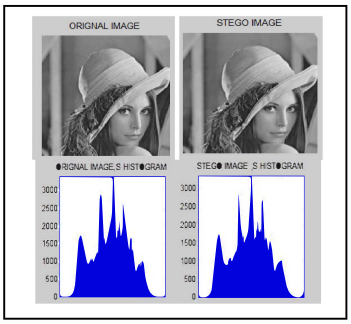

Fig. 4. Original and Stego Image for message size 4048 bits, Histogram for message size 4048 bits

D. Result of Baboon image

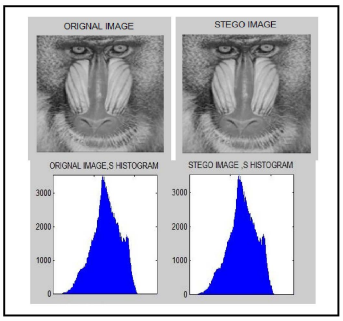

Fig. 5. Original and Stego Image for message size 1024 bits, Histogram for message size 1024 bits

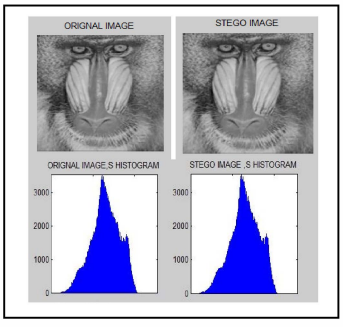

Fig. 6. Original and Stego Image for message size 2048 bits, Histogram for message size 2048 bits

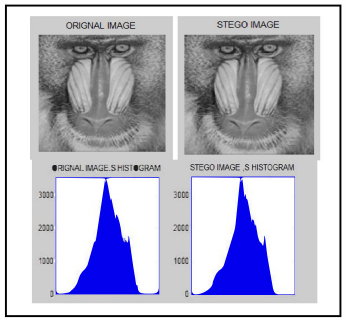

Fig. 7. Original and Stego Image for message size 4048 bits, Histogram for message size 4048 bits

E. Result of Peppers image

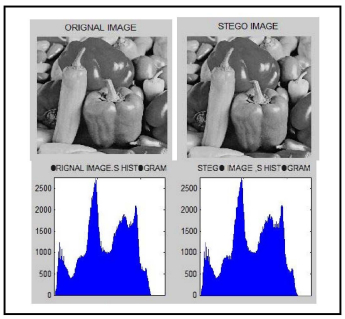

Fig. 8. Original and Stego Image for message size 1024 bits, Histogram for message size 1024 bits

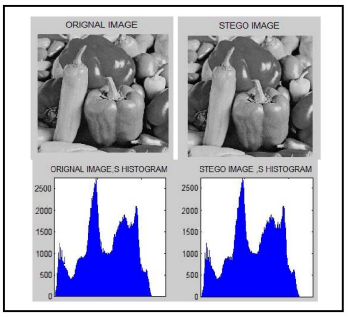

Fig. 9. Original and Stego Image for message size 2048 bits, Histogram for message size 2048 bits

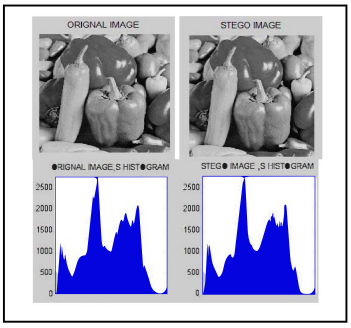

Fig. 10. Original and Stego Image for message size 4048 bits, Histogram for message size 4048 bits

F. Result of Triffy image

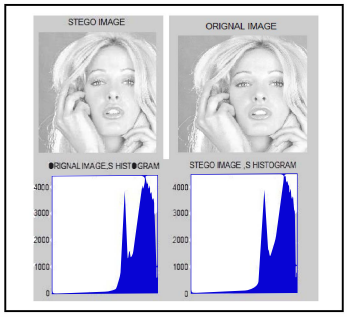

Fig. 11. Original and Stego Image for message size 1024 bits, Histogram for message size 1024 bits

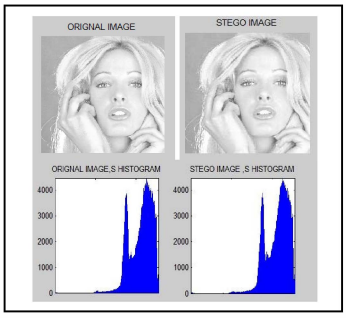

Fig. 12. Original and Stego Image for message size 2048 bits, Histogram for message size 2048 bits

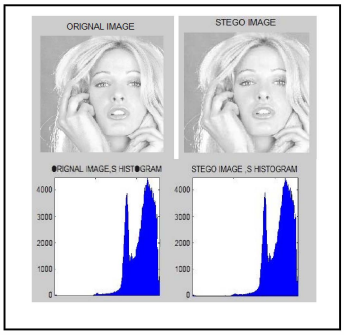

Fig. 13. Original and Stego Image for message size 4048 bits, Histogram for message size 4048 bits

TABLE I. PERFORMANCE ANALYSIS OF THE PROPOSED METHOD USING LENA IMAGE

Image Size	**Message Size**	**PSNR**	**MSE**
256*256	1024bits	60.3614	0.0625
256*256	2048bits	57.3380	0. 1255
256*256	4096bits	54.2455	0. 2523

TABLE II. PERFORMANCE ANALYSIS OF THE PROPOSED METHOD USING BABOON IMAGE

Image Size	Message Size	PSNR	MSE
256*256	1024bits	59.342	0.7124
256*256	2048bits	57.786	0.1367
256*256	4096bits	53.864	0.2623

TABLE III. PERFORMANCE ANALYSIS OF THE PROPOSED METHOD USING PEPPERS IMAGE

Image Size	Message Size	PSNR	MSE
256*256	1024bits	60.5456	0.0684
256*256	2048bits	57.4587	0. 1278
256*256	4096bits	54.4578	0. 2545

TABLE IV. PERFORMANCE ANALYSIS OF THE PROPOSED METHOD USING TRIFFY IMAGE

Image Size	Message Size	PSNR	MSE
256*256	1024bits	59.342	0.7124
256*256	2048bits	57.786	0.1367
256*256	4096bits	53.864	0.2623

IV. CONCLUSION

In this paper, a new data hiding method is proposed which overcomes the limitation of the existing methods. In this technique first the message is encrypted with the help of transposition algorithm after that the cipher text is hidden in the gray image using our new method (LSB-S). The beauty of this method is that it, overcomes the limitation of the existing method. The data hiding capacity of proposed method is 100% as all the pixel can carry data bit. The total number of pixels in an image are 256*256 i.e.65536 and the total no of bit can be hidden are 65536. If the intruder extracts all LSB bits, he does not get the message. Also the change in the pixel value is only plus one or minus one which results good PSNR and MSE. The cover and original image was shown to number of persons and asked for the difference, but they did not find any difference. The experimental result shows the good values of PSNR and MSE of the proposed scheme.

REFERENCES

[1] N. F Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer, pp 26-34, Feb 1998. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] S. Atawneh and P. Sumari, "Hybrid and blind steganographic method for digital images based on DWT and chaotic map," J. Commun., vol. 8, no. 11, pp. 690–699, 2013.

[3] K. Macrakis, "Confessing Secrets: Secret Communication and the Origins of Modern Science," Intell. Natl. Secur., vol. 25, no. 2, pp. 183–197, 2010.

[4] X. Luo, F. Liu, C. Yang, S. Lian, and Y. Zeng, "Steganalysis of adaptive image steganography in multiple gray code bit-planes," Multimed. Tools Appl., vol. 57, no. 3, pp. 651–667, 2012.

[5] F. a P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - a survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, 1999

[6] A. Almohammad, "Steganography-Based Secret and Reliable Communications˜ : Improving Steganographic Capacity and Imperceptibility by," 2010.

[7] I. V. S. Manoj, "Cryptography and Steganography," Int. J. Comput. Appl., vol. 1, no. 12, pp. 63–68, 2010.

[8] A. C. Ã, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography˜ : Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

[9] C. H. Yang and S. J. Wang, "Transforming LSB substitution for image-based steganography in matching algorithms," J. Inf. Sci. Eng., vol. 26, no. 4, pp. 1199–1212, 2010.

[10] S. Parvinder, B. Sudhir and H. R. Sharma, "Evaluating the Performance of Message Hidden in First and Second Bit Plane, W SEAS Transaction on Information Science and Technology, Vol. 2, No. 89, PP 1220- 1222, Aug. 2005

[11] B. Sudhir, R. Rahul, and Y. Rajkumar "Insertion of message in 6th, 7th and 8th bit of pixel values and its retrieval in case intruder changes the least significant bit of image pixels" International Journal of Security and Its Applications, Vol. 4, No. 3, July, 2010

[12] Y. Rajkumar, R. Rishi, and S. Batra, "A New Steganography Method for Gray Level Images using Parity Checker," Int. J. Comput. Appl., vol. 11, no. 11, pp. 18–24, 2010.

[13] K. R. Babu, D. S. U. Kumar, and D. A. V. Babu, "A Survey on Cryptography and Steganography Methods for Information Security," Int. J. Comput. Appl., vol. 12, no. 3, pp. 13–17, 2010.

[14] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimed. Tools Appl., 2015.

[15] K.-H. Jung and K.-Y. Yoo, "Data hiding method using image interpolation," Comput. Stand. Interfaces, vol. 31, no. 2, pp. 465–470, 2009.

[16] M. Aziz, M. H. Tayarani-N, and M. Afsar, "A cycling chaos-based cryptic-free algorithm for image steganography," Nonlinear Dyn., vol. 80, no. 3, pp. 1271–1290, 2015.