C. Immaculate Mary* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.4, Issue No.2, February - March 2016, 2832 – 2835.

An Effective Approach for Hiding Encrypted Messages with Neural Key using LSB Image Steganography

Dr.C.IMMACULATE MARY
H.O.D &Associate Professor
Department of Computer Science
Sri Sarada College for Women (Autonomous)
Salem-16. Tamil Nadu, India.

P. ROSHNI MOL
Assistant Professor
Department of Computer Applications
Shri Sakthikailassh Women's College
Salem-16. Tamil Nadu, India.

Abstract — **The network security is becoming more essential as the number of data being exchanged on the Internet increases. The data transmitted over the network may be detected, altered or hacked by the intruder. Therefore, privacy and data consistency are required to protect against unauthorized access and use. To overcome these problems, techniques such as Steganography and Cryptography can be adapted. This has resulted in an explosive development of the field of information hiding. This research work is a combination of Steganography and Cryptography, which provides a strong backbone for its security. In this research work, the secret message is encrypted before the actual embedding process starts. The main goal of this work is to hide a text of a secret message in the pixels of the image so that the Human Visual System is not able to distinguish between the original and the stego image. For this Image Steganography, We focus on the Least Significant Bit (LSB) technique in hiding messages in an image. This LSB technique embeds the bits of the message in the image and thus making it harder for unauthorized people to extract the original message encryption is used to protect the confidentiality of messages. Here, the sender sends the encrypted message by embedding using LSB technique with neural key. On the other end the receiver decrypts the message with the same key. The hidden message is encrypted using an encryption algorithm using secret key and hence it will be nearly impossible for the intruder to unhide the real secret message from the embedded cover file without knowing secret key. This present work focuses on enhancing the technique to secure data or message with authenticity and integrity**

Keywords- **Steganography; Cryptography; Encryption; Least Significant Bit (LSB) Technique; Neural Key**

I. INTRODUCTION

The quick growth of data transfer through internet made it easier to send the data precise and faster to the destination. There are many transmission media to transfer the data to destination like e-mails; at the same time it is easier to change and mishandling the important information through hacking. So, in order to transfer the data securely to the destination without any changes, there are many approaches like cryptography and steganography. This paper deals with the image steganography and cryptography using neural key and Least Significant Bit (LSB)[3] technique.

II. COMBINED CRYPTO-STEGANOGRAPHY

Steganography is not the similar as cryptography. Data hiding techniques have been commonly used for transmission of hiding secret message for long time. Data security is a big challenge for computer users. Every user has some important data that they want to secure from others. Though Cryptography and Steganography[5] provide security, it is better to make use both of them together. By combining, the data encryption can be perfomed by using an encryption algorithm and then embed the cipher text in an image with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined technique will assure the requirements such as capacity, security and robustness for secured data transmission over the network.

A pictorial representation of the combined concept of cryptography and steganography is depicted in Figure 1.

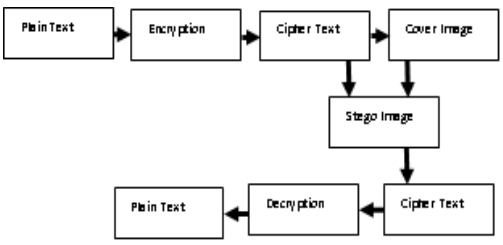

Figure 1. Combined Crypto-Steganography

III. ENCRYPTION

Encryption is the process of making the text into unreadable format. The intruder may not be able to read the message. In this paper we make use of Caesar cipher algorithm for encryption. It is one of the simplest substitution cipher algorithm. In this

algorithm a left shift of 3 letters and substitution takes place. For example letter D is replaced with A, letter E is replaced with B and so on. In this paper we have made use of Difie Hellman Key Exchange Algorithm and Neural Key for key exchange.

A. Diffie Hellman Key Exchange Algorithm:

Diffie Hellman Key Exchange is an asymmetric key algorithm. It makes use of both public and private key for exchanging. Both sender and receiver must generate private and public keys. For example the sender makes use of private key to generate a new public key and send it to receiver. The receiver obtains the key and issues a new public key. At the end they will receive the same shared key values. In this research we make use of diffie hellman key exchange algorithm to generate a key and it is passed as weights in neural network.

B. Neural Key Generation

The key which is generated by Diffie Hellman Key Exchange algorithm is again treated with neural network to generate a Neural key. For this we make use of Tree Parity Machine (TPM). The key generated by diffie hellman algorithm is passed as weights for neural network. The input of hidden units is calculated and output bit is generated so that it is passed between the sender and receiver. After the synchronization is completed, the weights of both neural network will be the same. These weights can now be used as secret key that is neural key.

IV. LEAST SIGNIFICANT BIT (LSB) INSERTION TECHNIQUE

LSB is one of the simplest techniques used for steganography. Images are composed of pixels. The pixel values can be digitally expressed as 0's and 1's. For example, RGB 24-bit image has 8 bits representing each of the red, green and blue components. To insert an A (binary value 10000011) into a 24-bit image which uses the RGB color model. Each pixel uses eight bits for the intensity of red, green and blue. Three pixels are needed for hiding the letter A.

TABLE I. BEFORE EMBEDDING TEXT

	Red Component	Green Component	Blue Component
pixel 0	00100111	11101001	11001000
pixel 1	00100111	11001000	11101001
pixel 2	11001000	00100111	11101001

The changed sequence with the letter A (bit sequence 10000011) embedded would look like this.

TABLE II. AFTER EMBEDDING TEXT

	Red Component	Green Component	Blue Component
pixel 0	00100111	11101000	11001000
pixel 1	00100110	11001000	11101000
pixel 2	11001001	00100111	11101001

The embedding process is done in a sequential manner.

V. PROPOSED ALGORITHM

Existing Combined Crypto-Stegaography makes use of symmetric or asymmetric approach for key exchange. In this proposed algorithm we make use of asymmetric key as well as neural key for exchanging.

Step 1: Read the cover image.

Step 2: Enter a random number to generate a key.

Step 3: Pass the key as weights to neural network.

Step 4: A neural key is generated.

Step5: Get the secret data. Convert the data from decimal to binary.

$$[message] \xrightarrow{Dec2Bin} [1000001]$$

Step 6: Break the byte to be hidden into bits.

$$Thus\ [1000001] \xrightarrow{is\ divided\ into\ 8\ bits} [10000001]$$

Step 7: Find the length of the secret data or message.

Step 8: Find the Least Significant Bit for each pixel of the cover image. This can be done by taking modulus of the pixel with 2.

Step 9: Compare the LSB bit of each pixel with the secret data bits. The LSB insertion technique is done based on two conditions.

Condition 1: If LSB bit equals to zero and secret data bit equals to one then 1 is added to each and every pixel of the cover image

Condition 2: If LSB bit equals to one and secret data bit equals to zero then 1 is subtracted from each and every pixel of the cover image.

Step 10: The modified image is the stego image with the secret data in it.

Step 11: The reverse process is done for extracting the secret data from the stego image.

Step 12: Secret data bits are finally converted to text format

Step 13: After extraction the stego image is converted to extracted image which is similar to the original image.

VI. EXPERIMENTAL ANALYSIS

We have implemented Image Steganography in MATLAB R2012a. We have implemented both bmp and jpg images for our experiments. The following Figures 2,3 &4 shows the cover , stego and extracted images.

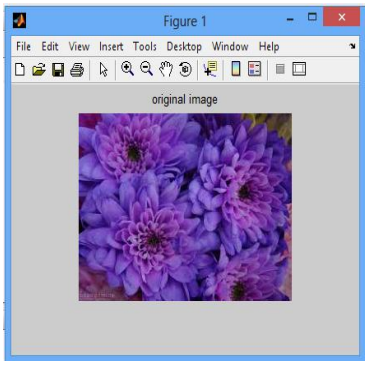

Figure 2. Reading and displaying jpg cover image. (RGB image)

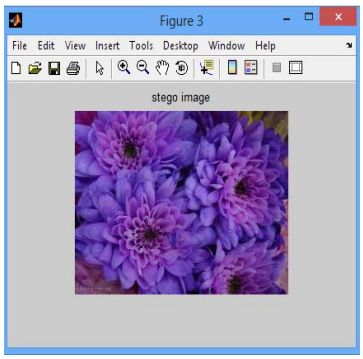

Figure 3. Displaying the stego image with message embedded

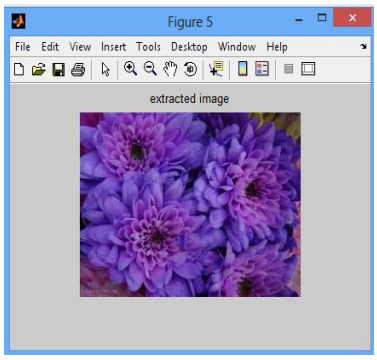

Figure 4. Displaying the extracted image where the message is extracted separately

VII. PERFORMANCE ANALYSIS OF JPG IMAGES

We have tested many images with various dimensions and we have calculated the MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio). The PSNR ratio is used as quality measurement of the images. The higher PSNR represents better quality of the reconstructed image. The lower value of MSE represents lower error. The following Table 3, 4 &5 show the results of the proposed technique.

Table 3: Performance Analysis of jpg images (Hidden message= 7 characters)

Image (uint8)	Message size	Payload (bits)	MSE	PSNR (dB)	Embedding Duration (seconds)
68x118	7	56	1	48.1648	0.289712
194x259	7	56	1	48.1648	1.753096
194x25	7	56	1	48.1648	1.798537

Table 4: Performance Analysis of jpg images (Hidden message= 12 characters)

Image (uint8)	Message size	Payload (bits)	MSE	PSNR (dB)	Embedding Duration (seconds)
68x118	12	96	1	48.1648	0.496995
194x259	12	96	1	48.1648	3.001386
194x25	12	96	1	48.1648	3.101297

Table 5: Performance Analysis of jpg images (Hidden message= 1509 characters)

Image (uint8)	Message size	Payload (bits)	MSE	PSNR (dB)	Embedding Duration (seconds)
68x118	12	96	1	48.1648	62.667100
194x259	12	96	1	48.1648	380.83510
194x25	12	96	1	48.1648	391.363631

When the dimension of the cover image is small i.e. when a small image is taken, the embedding duration of secret message is less. The error rate is less because the message is hidden in the LSB of the pixels.

VIII. HISTOGRAM ANALYSIS

Histograms show the distribution of data values. It is used to know the characteristics of data and to know the distribution of the data. Following figures are the histograms of cover image, stego image and the extracted image of JPG image. The result shows that there is no significant difference in the pixel values of stego image when compared to cover image.

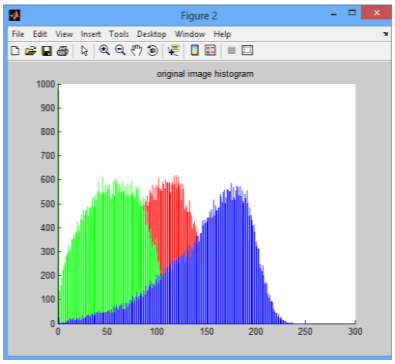

Figure 5. Histogram for Original image

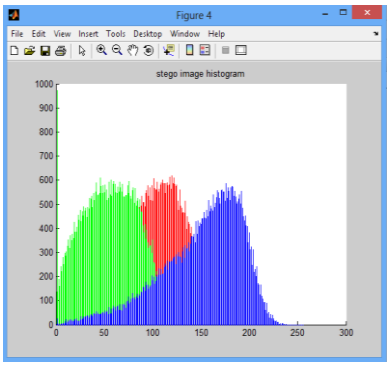

Figure 6. Histogram for Stego image

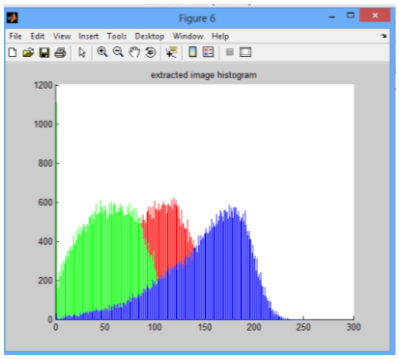

Figure7. Histogram for Extracted image

IX. CONCLUSION

The proposed approach in this research work uses a steganographic approach called LSB Image Steganography. The application creates a stego image in which the personal data is embedded and is protected with encryption and DECRYPTION along with a key exchange, which is highly secured. The main purpose of this research work is to develop a steganographic application that provides good security. The resolution of image doesn't change much and is slight when we embed the encrypted message into the image and the message is protected. So, it is not possible to damage the data by unauthorized person. We are using the Least Significant Bit algorithm for developing the application which is faster and reliable and compression ratio is rational compared to other algorithm. The Human Visual System may not able to identify the changes made in the image.

X. FUTURE ENHANCEMENT

The future work on this research work is to improve the compression ratio. The security using Least Significant Bit Algorithm along with neural key is good but we can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption. We can improve this algorithm by training with other neural networks.

XI. REFERENCES

[1] Domenico Daniele Bloisi , Luca Iocchi: "Image based Steganography and cryptography", Computer Vision theory and applications volume 1 , pp. 127-134 .

[2] Jammi Ashok , "Steganography: An Overview" International Journal of Engineering Science and Technology Vol. 2(10), 2010, 5985-5992

[3] A. E.Mustafa , A.M.F.ElGamal , M.E.ElAlmi , Ahmed.BD "A proposed algorithm for steganography in digital image based on least significant bit", Research Journal Specific Education, Faculty of Specific Education, Mansoura University, Issue No. 21, April. 2011

[4] Lee, Yeuan-Kwen and Ling Hwei Chen. "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement."Ninth National Conference on Information Security (1999): 8-15.

[5] A. Joseph Raphael, Dr. V. Sundaram," Cryptography And Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630

[6] JHP Eloff T Morkel and MS Olivier." An overview of image steganography". Fifth Annual Information Security South Africa Conference (ISSA2005), 2005

[7] Bijoy Bandyopadhyay Sugata Sanyal Soumyendu Das, Subhendu Das. "Steganography and steganalysis: Different approaches."

[8] Sushil Jajodia. Neil F. Johnson. "Exploring steganography: Seeing the unseen". Computer Practices: IEEE Journal, 1998.

[9] Karen Bailey. Kevin Curran. "Evaluation of image based steganography methods". International Journal of Digital Evidence, 2, September 2003.

[10] Khosravi, Sara,Abbasi Dezfouli, MashallahA New Method to Steganography Whit Processing Picture in Three Colors (RGB) , Int. J. Comp. Tech. Appl., Vol 2 (2), 274-279

