Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.804 – 808

RESEARCH ARTICLE

Enhance Two-Tier Secure Model of Modern Image Steganography

Ms. Tanuja Mahajan[1], Ms. Bhakti Kurhade[2]

[1]Department of Computer Science and Engineering

G.H. Raisoni Academy of Engineering and Technology, Nagpur, India

[2]Assistant Professor, Department of Computer Science and Engineering

G.H. Raisoni Academy of Engineering and Technology, Nagpur, India

[1] tanujamahajan24@gmail.com; [2] bhaktikurhade4@gmail.com

ABSTRACT:- ***In revolutionary stage, network Security is one of most significant problem . To pause this problem as well as to protect data we use cryptography and steganography. Steganography hide our data within image and looks like original image so anyone can't understand other data hide behind image. Secrete writing is cryptography. Cover writing is known as steganography. Two tier securities are provided to secret data by our proposed method. In cryptography we use RSA algorithm to encrypt secret message and Hash function with least-significant-bit (HLSB) technique is used to hide encrypted message into true color RGB image. Our proposed method gives cavalier quality stego images.***

Keywords — Cryptography, Steganography, LSB, Hash-LSB, Encryption, Decryption, PSNR, MSE

I. INTRODUCTION

We use internet for data communication but while communication hackers hack our data or data lost to avoid these problems we must provide security. Image Steganography allows two parties to communicate securely. Cryptography is a technique which convert message in unreadable form during communication of data whereas steganography conceals the existence of the message. Steganography is the art and science of hide the message or secret data into an image and send it to the destination securely without any modification.

Steganography word comes from the Greek word *Steganos*. The meaning of steganos is covered or secret and *graphy* mean writing or drawing. Therefore, steganography means covered writing. Steganography is the art and science of hiding information such way that its presence cannot be detected with necked eyes and a communication is happen.

There are so many kinds of Data hiding methods for images some of them are

1) spatial-domain technique
2) frequency-domain.

In the spatial domain the secret message is embedded in the image pixels directly. It is easy and safe. In the frequency-domain the secret image is first transformed to frequency-domain, and then the messages are embedded in the transformed coefficients.

Major objective of this project are as follows

1) availability
2) Improve the security of the data hiding technique.
3) Enhances the security of data and data hiding technique.
4) Confidentiality
5) Authenticity
6) Integrity

II. RELATED WORK

Least significant bit (LSB) insertion technique is discuss in paper[1]. It is simple method for embedding information in a cover image. In this method we embed 8th bits of data at (LSB) of each pixel in the cover image. We place this data in order of 3,3,2 respectively. The altered image is called stego-image. This is simple method of implementation.

Pixel-value differencing image steganography is presented in paper [5].This method increases the capacity of the hidden secret information and to provide a stego-image. This method uses the largest difference value between the other three pixels close to the target pixel.

Masud [3] has proposed new approach of LSB technique for RGB true color image by enhancing the existing LSB substitution techniques. This new approach improves the security level of hidden information. In paper [4] designing of robust and secure image steganography based on LSB insertion technique is discuss. In [15] a security analysis on spatial domain steganography for JPEG decompressed images has been presented.

III. PROPOSED SYSTEM ARCHITECTURE

Proposed system model is shown below

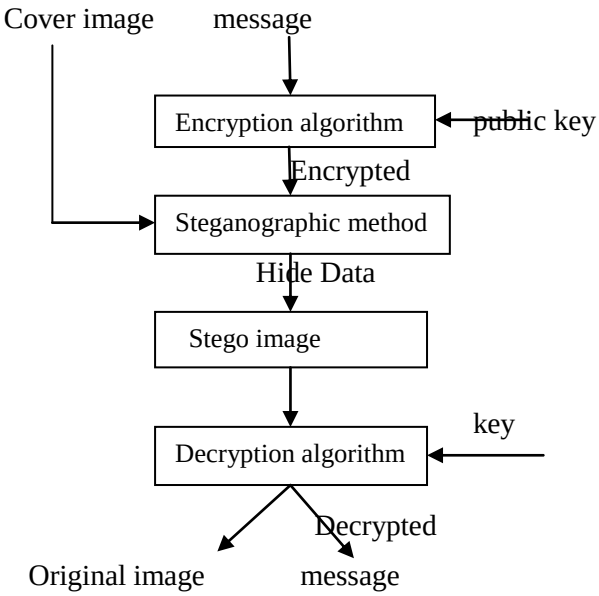

Fig.1 Flowchart of proposed system

First we take cover image then we enter secrete mess. Message is encrypted with encryption algorithm. We use steganographic method (hash function with LSB) which hides encrypted message into cover image new image is formed called stego image. When stego image is extracted decryption of message is done and we get message and original image separately. Proposed system consist of encryption and decryption phase.

A. ***Encryption Phase*** –

The Encryption phase uses two types of files. One is the secret file which contain secrete message which is to be transmitted securely, and the other is a carrier file (image) in which secrete message is hidden. a cover image split into three matrices i.e(RGB). The hidden information is converted from decimal to binary. Each pixel is converted into 8 bit binary value. Then the 2D array is reshaped into a 1D array. This 1D array matrix is called as bit stream of hidden information.

Encryption phase uses RSA algorithm to encrypt the secret data. Encryption process converts plaintext into the cipher text. Encryption process will use public key to encrypt secret data. It is very difficult for any intruder to decrypt data without private key. We take cipher text encrypted from the secret message to be embedded in the cover image. In this process first we converted cipher text into binary form to convert it into bits. We use hash function to select the position of insertion of bits and then 8 bits of message at a time will be embedded in the order of 3, 3, and 2 in red, green and blue matrices. The process is continued till entire message of bits will got embedded into the cover image

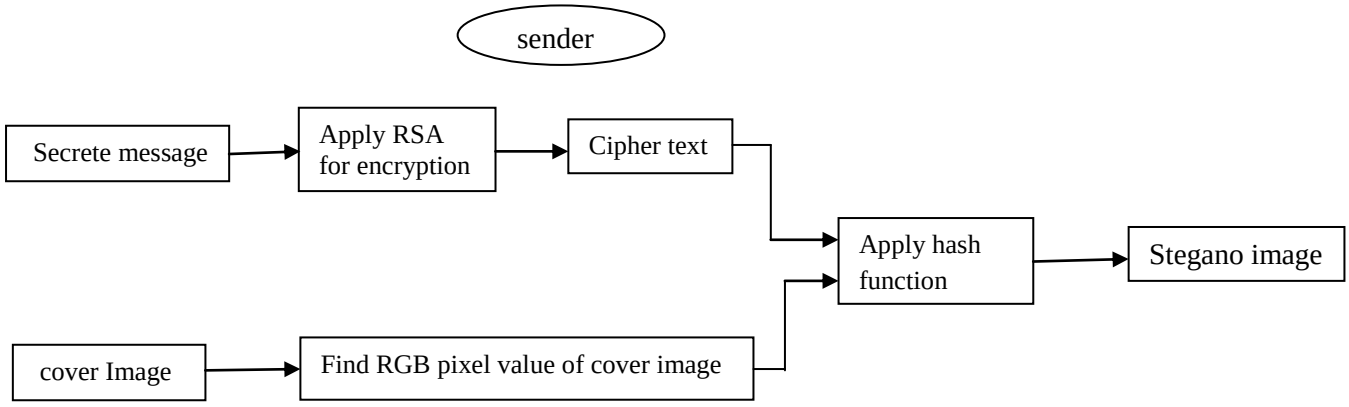

Fig.2 Encryption Phase

Form fig.2 it is clear that sender first select cover image and secrete message and then Apply RSA algorithm for encryption. Find position of insertion by hash function and hide message into that position finally Stegano image is formed.

B. ***Decryption Phase*** –

Decryption phase is exactly reverse of the encryption phase. In the decryption process we again used the hash function to detect the positions of the LSB's where the data bits had been embedded. Bits are then extracted from the position.

We will get the message which again converted from binary to decimal form, and by same process we got the cipher text message. Retrieve the positions of LSB's that contain secret data, the receiver will decrypt secret data using RSA algorithm. T receiver will use private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable form. Finally we got original image and secrete message

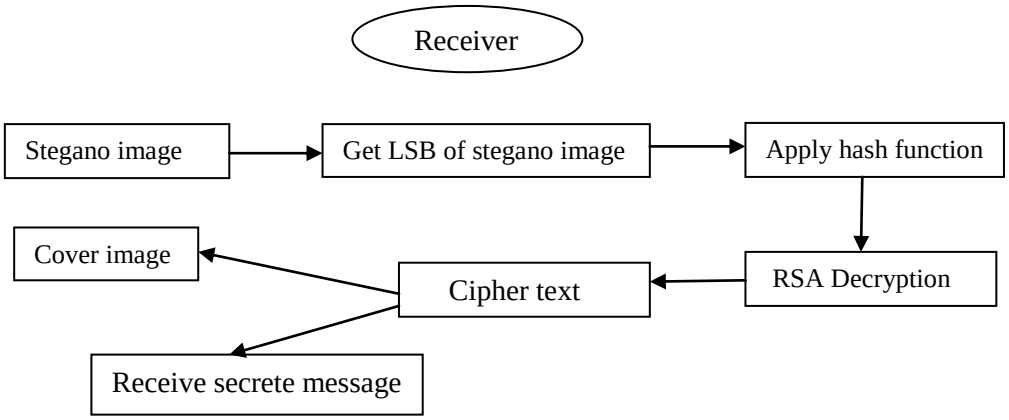

Fig 3. Decryption Process

Decryption process is discussed in fig.3 in this process first we select a stego image then find 4 LSB bits of each RGB pixels from stego image. Apply hash function to find the position of hidden data in LSB bits. Retrieve the bits in order of 3, 3, and 2 respectively. Apply RSA algorithm to decrypt the retrieved data. Finally we got the secret message and original image.

IV. PERFORMANCE ANALYSIS AND RESULT

The performance of Steganographic tech. has been evaluated and graphically represented on the basis of two measures are – Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR)

Mean Square Error (MSE) can be calculated as follows

$$MSE=1/H* \sum_{i=1}^{H} (P(i,j)-S(i,j))^2$$

Where, H and W are height, width and P (i, j) which represents the cover image and S (i, j) represents stego image.

Peak Signal to Noise Ratio (PSNR) can be calculated as follows

$$PSNR=10log\ 10\ L2/\ MSE$$

Where, PSNR is peak signal to noise ratio, L is peak signal level for a color image which is 255.

We take color image of size 512* 512 as cover image and then perform all process as given above we get stego image finally analysis performed through PSNR and MSE.

Name of Image	**Results of LSB method**		**Results of proposed method**	
	PSNR	**MSE**	**PSNR**	**MSE**
Barbara	51.1655	0.4972	64.2271	0.0246
Lenna	51.0728	0.5097	64.4518	0.0233
Tulips	51.3453	0.4770	65.0921	0.0201
Baboon	51.1490	0.4991	65.3640	0.0189

Table 1. Comparative Study

If we compare result obtained by LSB method with our proposed method as shown in Table 1 then it is clear that our proposed method gives more PSNR value and less MSE than LSB method. More PSNR value indicates best quality of image. If we carefully seen table then Baboon image quality is best because PSNR is highest and MSE is lowest. There is improvement in embedding capacity with preserving quality of the image. More secured transmission possible due to protection of RSA cryptosystem.

V. CONCLUSION

Analysis has been conducted through number of observations .It works fine. It is impossible for intruder to steal the data because embedding bit positions are decided by Hash function with LSB approach. After the cipher text is embedded, changes in image not seen to normal human eye. This steganography is a strong information security technique, especially when combined with encrypted embedded data. Experimental results show that proposed method obtains both larger capacity and higher image quality. Finally we can conclude that the proposed technique is effective for secret data communication.

ACKNOWLEDGEMENT

It is our privilege to acknowledge with deep sense of gratitude towards our seminar co-guide Prof. Bhakti kurhade for their valuable suggestions and guidance throughout course of study and timely help given in completion of project work.

REFERENCES

1] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-JengWang , Hun Min Sun ,"Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems", in *IEEE Information Transactions On Forensics And Security,* Vol. 3, No. 3.,September 2008 .

2] Souvik Bhattacharyya, Avinash Prasad Kshitij, Gautom Sanyal , "A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform", *International Conference on Recent Trends in Information, Telecommunication and Computing*, Vol 51 ,pp- 173-178, 2010 .

3] Han-ling ZHANG, Guang-zhi GENG, Cai-qiong Xiong, "Image Steganography using Pixel-Value Differencing", *Second International Symposium on Electronic Commerce and Security*, pp- 109 - 112, 2009.

4] Jinsuk Baekl, Cheonshik Kim, Paul S. Fisherl, and Hongyang Cha, "(N,1) Secret Sharing Approach Based on Steganography with Gray Digital Images", Wireless Communications, Networking and Information Security (WCNIS), *IEEE International Conference*, 2010, pp-325 – 329

5] Wuling Ren, Zhiqian Miao, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", *Second International Conference on Modeling, Simulation and Visualization Methods, IEEE*, 2010, pp-221-225.

6] Han-ling ZHANG, Guang-zhi GENG, Cai-qiong Xiong, "Image Steganography using Pixel-Value Differencing", *Second International Symposium on Electronic Commerce and Security*,2009, pp- 109 - 112.

7] R. Ji, H. Yao, S. Liu and L. Wang , "Genetic Algorithm Based Optimal Block Mapping Method for LSB Substitution", *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*,2011, pp. 215-218

8] Sunny suchdeva and Amit Kumar, "Color Image Steganography Based on Modified Quantization Table", *in 2nd international conference on advance computing and communication tech*, vol 51, 2012, pp. 534-538

9] Yi Luo, Xiaolong Li, and Bin Yang (2011) , "Locating steganographic payload for LSB Matching embedding " , *IEEE transaction on computers* , vol 2 , no 1,pp.214-218

10] N.Raftari, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", *Sixth Asia Modeling Symposium.*, 2012, pp. 523-527

11] Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge adaptive image steganography based on LSB matching revisited," in *IEEE Transactions on Information Forensics and Security,* vol.5, no.2, June 2010

