ISSN:0975-9646

Secure Secret Key Transfer Using Modified Hash Based LSB method

Aniket G. Meshram[1], Prof. Rahul Patil[2]

Department of Computer Engineering, Savitribai Phule Pune University, PCCOE, Akurdi, Pune – 411040, India.

***Abstract*— Recent advancements in computer security have shifted the focus of security officials from, using only the cryptography techniques to using steganography as well, or the combination of both. In steganography the most widely used technique is the LSB method, but this technique being the simplistic of all, is well known and hence is vulnerable to attacks. However, modifying the LSB method to the point where it would be difficult or impractical to find the hidden message is a domain where an extensive work and research is required. Due to the simplistic nature of the LSB method, this technique can be modified easily. But the main crux lies in the way this modification is done. Therefore, in this paper we discuss a modified version of the LSB, a Hash Based LSB technique and a hiding method that further hides the existence of the message into the cover image. We call this hiding method as the 'XOR Feed' method.**

***Keywords*— Modified Hash Based LSB, XOR Feed, Image Steganography, Spatial Domain, Grayscale Image.**

I. INTRODUCTION

Since ancient Greek and Roman rulers, the steganography technique has been widely used for hiding secret information. Steganography is a blend of two greek words, *steganos* and *graphein*, which means secret or covered and writing or drawing respectively. Now when it comes to hiding the secret information, a definitive medium is required that can carry the secret message, without getting noticed by anyone easily. This medium is called the cover medium, that covers the secret, intended only to the recipient with whom the secret is to be shared.

With regards to a computer system there are four mediums in which a person can hide the data, viz. The *text* medium itself, that can be used to hide information with some logic, for example, hiding information in a text by scripting some text so that the message be recognized only by the Initial letter of the words created. The *image* medium is used to hide both text as well as secret messages in the form of an image. This gives images the power over hiding not just the messages but also the images inside another images. Next is the *audio* medium and the *video* medium, where again the data can be hidden with the proper audio and video steganography techniques.

The Least Significant Bit method is used in the Image steganography to hide data in the least significant bit of the image pixels. Consider a grayscale image with pixel value ranging from 0 to 255. Now since, there are 256 possible values for each pixel, manipulating the least significant bit, would hardly be noticed by anyone observing the image. For a color image however, one has to consider the intensity of the RGB values since, each color has a different effect on the human eye.

II. RELATED WORK

Many modifications in the LSB technique have been suggested by different authors which mostly relate to the spatial domain. Alike the Video steganography, the Image Steganography can also be classified into spatial domain and frequency domain. The frequency domain transforms the image into components that can be manipulated by changing their frequencies. These images are transformed using the techniques like the Fourier Transform, DCT and DWT. Hashing scheme can be used in the LSB methods[1], where the position for hiding are chosen by a hash function. This hash function can further be made complex, however the nature of the algorithm remains the same.

Another technique described as in [2] can be used, where a combination of Fibonacci as well as the Lucas Transforms are used for selecting the hiding locations. This method can be effective when used with frequency domain methods like the dct and Fourier transform.

III. PROPOSED SCHEME

A. Modified Hash Based LSB Method

i. *Hash Function*

The technique we propose is based on the Hash Based LSB technique [1] with some major modifications applied on the Image Steganography. The proposed technique works on the hash function given by,

$$x_i = k^p \bmod x,$$

where, k is the LSB byte position of the image pixel, p is the bit position of the secret message in reverse order and x is the size of image i.e. (mxn), where, m is the height and n is the width of the image matrix. x_i, thus, gives the location to hide the secret data. Now, the value of k can either begin from the first pixel, i.e. 1, or a seed value can be supplied so that the hashing can work from the seed. For example, a seed of 11, and a secret message size of 7 will give the first x_i value as,

$$x_i = 11^7 \bmod x$$

B. 'XOR Feed Hiding Method

In order to further hide the data, a technique called the 'XOR Feed' Hiding Technique can be used, which simply

makes use of an XOR function to hide the data into an image. This technique can be explained as below:

i. *Hiding Method.*

To hide the data inside the image we use the 'XOR Feed' method as follows:

Consider that the location selected by using the Hash function for some bit *p* in the secret message which has the value '0', to hide in a 160x160 pixel image with some x_i value say 515, let the value of the pixel at this location be 225, which is represented in the binary as,

1110 000**1**

Now, the LSB bit has the value '1'. We use the XOR Feed method, to find a bit that when xor'ed with this value gives the secret 0, and that bit is nothing but the XOR'ed value of 1 and 0 i.e. 1.

ii. *Header*

The design of a header can be shown as below:

Fig. 1 Header Structure for hiding in image

The 'Seed Value' as mentioned above is an initial value given to the hash function, the 'Size' gives the size of image and the 'XOR Feed' gives the XOR'ed values of the secret and the actual bits in the positions given by the hash function.

The overall operation of the proposed method can be shown as below:

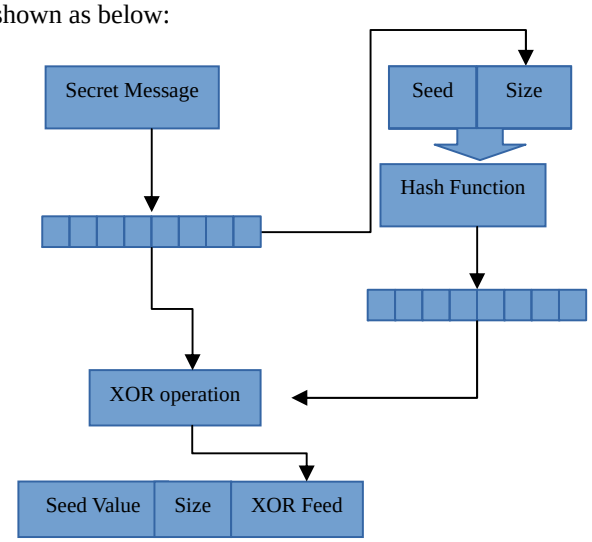

Fig. 2 Overall Modified Hash-based LSB Operation

IV. Performance Evaluation

The proposed scheme was evaluated with the two most widely used methods, the mean square error (MSE) and the Peak Signal to Noise Ratio (PSNR), which helps to evaluate the difference between two images.

A. MSE

The Mean Square Error is a measure of the average of the squares of the errors. It is used to measure the error difference of two images by calculating the mean error value. The formula for mean square error (MSE) is given by,

$$MSE = \frac{1}{ROW * COL} \sum_{i=1}^{H} (O(i,j) - C(i,j))^2$$

Where, *ROW* gives the number of rows in the image matrix, while *COL* gives the number of columns in the image matrix. The *O(i,j)* value gives the original image and *C(i,j)* gives the changed imaged.

B. PSNR

Peak Signal to Noise Ratio (PSNR), represents the ratio between the maximum value of an image pixel and the mean error difference of two images in consideration. This ratio helps to differentiate between the images based on their pixel values. For a peak value *PSL*, (for gray scale images the maximum value is 255) and the mean square error (MSE) we have,

$$PSNR = 10 \log_{10} \frac{PSL^2}{MSE}$$

Where, PSNR gives the Peak Signal to Noise Ratio of the two images under consideration.

TABLE I. Details of Image Test Files

Sr. No.	Name of Image	Resolution
1.	gray1.jpg	150 x 200
2.	gray2.jpg	300 x 308
3.	gray3.jpg	300 x 300
4.	gray4.jpg	500 x 500
5.	gray5.jpg	400 x 400

Five images were considered for testing the proposed system along with comparison of the LSB method. The images considered are all gray scale images with the resolution not exceeding 500 by 500 pixels.

TABLE II. Evaluation Results of LSB and MHLSB methods

Image File	LSB method Evaluation		Seed	MHLSB method Evaluation	
	MSE	PSNR		MSE	PSNR
gray1.jpg	8181.57	9.0364	11	8176.27	9.0392
gray2.jpg	6109.44	10.304	23	6001.25	10.382
gray3.jpg	11485.95	7.563	12	11189.89	7.676
gray4.jpg	25378.46	4.1199	27	22378.46	4.666
gray5.jpg	23076.75	4.533	17	22076.75	4.725

V. Conclusion and Future Scope

The LSB method that manipulates only the lsb bits can easily fall pray to detection, since one can easily retrive the bits from the lsb. But, however our proposed system provides a better hiding mechanism that cannot be detected easily using simple lsb methods. Further the XOR Feed method adds another layer of security to the proposed method complicating the detection process. This method, thus can be useful for applications where secret information is required to be communicated between two authorized parties.

References

[1] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash Based Least Significant Bit Technique For Video Steganography (HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No. 2, April 2012.

[2] Minati Mishra, Priyadarsini Mishra, M.C. Adhikary and Sunit Kumar, "Image Encryption Using Fibonacci – Lucas Transformation", International Journal on Cryptography and Information Security (IJCIS), Vol. 2, No. 3, September 2012.

[3] Luis von Ahn and Nicholas J. Hopper, "Public-Key Steganography", Carnegie Mellon University.

[4] Vivek Jain, Lokesh Kumar, et. al. "Public-Key Steganography Based On Modified Lsb Method", Journal of Global Research in Computer Science (JGRCS),Volume 3, No. 4, April 2012.

[5] Masoud Nosrati, Ronak Karimi and Mehdi Hariri , "Embedding Stego-Text in Cover Images Using linked List Concepts and LSB Technique", World Applied Programming, Vol. 1, No. 4, October 2011.

[6] Harshavardhan Kayarkar and Sugata Sanyal, "A Survey on Various Data Hiding Techniques and their Comparative Analysis".

[7] Eltyeb E. A bed Elgabar, "Comparison of LSB Steganography in BMP and JPEG Images", International Journal of Soft Computing and Engineering (IJSCE) , Vol. 3, Issue-5, November 2013.

[8] Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm ", Journal of Computer Science 3 (4): 223-232, 2007.

[9] Tanmoy Sarkar and Sugata Sanyal, "Reversible and Irreversible Data Hiding Technique ".

[10] Rucha Bahirat and Amit Kolhe, "Overview of Secure Data Transmission Using Steganography ", International Journal of Emerging Technology and Advanced Engineering (IJETAE), Volume 4, Issue 3, March 2014.

[11] R.M. Goudar, Aniket G. Meshram, Prashant N. Patil, et. al., "Secure Data Transmission by using Steganography", International Institute for Science, Technology and Education (IISTE), Information and Knowledge Management , Vol 2, No.1, 2012.