Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Enhanced LSB Steganography Algorithm for Data Hiding

Akash Modi, Manu Bansal
Department of E.C.E
Thapar University
Patiala, India

Abstract— In steganography, the secret message can be concealed inside any other medium like audio, video, image and text with the improvement in both security and quality of the medium. In this paper, we propose an algorithm to hide an image or data in cover image by using image steganography. The proposed algorithm is an improved version of LSB based image steganography. In this method, we modify the data image and then XORing the data image pixel with the cover image pixel. The obtained results show that the proposed algorithm provides an improved values of MSE and PSNR than LSB based image steganography method. This technique could be combined with other method to improve steganography.

Keywords— Image steganography, Peak Signal to Noise Ratio (PSNR), Mean Square Error(MSE), Least Significant bit(LSB)

I. INTRODUCTION

With the rising usage of computers and internet, the exchange in data as increased tremendously. Sometimes this data, which is being exchanged, might be confidential and private. This has further led to increase in the demand of security of such data. Earlier, cryptography and watermarking were designed to protect the information. Before the invention of these methods, traditional methods were being used for sending and receiving of message. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In the Second World War the Microdot technique was developed by the Germans [1].

Cryptography scrambles the data, so that it becomes unpredictable. The problem with the cryptography is that, it shows that the transmitted information is encrypted and it should not be read by the any random user. So, if any one wants to read it can deduce the information. Hence if some important data has to be transmitted on the unsecure channel such as internet, steganography provides an additional protection to the data. Where cryptography tries to completely change an image, but steganograpy tries to hide the information in the same image. This presents the image as if no changes have done in it. Steganography is an art of hiding data in another medium like audio, video, image and text file.

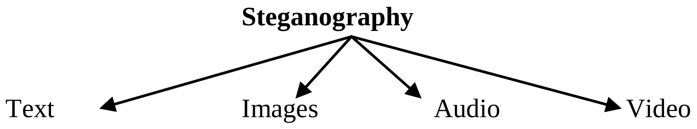


Figure 1: Classification of steganography

The hiding is typically parameterized by a key. It is difficult to detect the hidden material by the third party without this key. The combination of cover object and secret message is called stego object [2].

There has been a rapid growth of interest in this subject due to two main reasons. First, the publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books, and multimedia products; an appreciation of new market opportunities created by digital distribution is coupled with a fear that digital works could be too easy to copy. Secondly, moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages. The ease with which this can be done may be an argument against imposing restrictions [3].

In this paper we use Image steganography, in which each pixel of cover image has some integer value; in which data hiding can be done. Number of pixels in any image depends upon the size of the image. If the size of cover image is 512x512 then there are 262144 pixels available for data hiding. If we use a color image then each pixel of cover image have 24 bit of information in which first 8 bit shows the red color, next 8 bit shows the green color and last 8 bit shows the blue color of that pixel.

II. LITERATURE REVIEW

In this paper we introduce a new algorithm, which is based on least significant bits (LSB) method and Modified LSB method [5] [6]. In LSB method first of all we convert the data (image) in the binary format, after that each bit of data is replace by LSB of each pixel of cover image. In this method only LSB bit of cover image is change, due to this there is very few change in cover image which is not visible by human eyes. That's why this method is very popular. Example:

Let cover image pixels are

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

Data values are

11001001

Output of LSB method

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

The output of steganography is called stego image. The visibility or quality of stego image depends of many factors. In which two main factors are MSE (mean square error) or PSNR (peak signal to noise ratio).

Mean Squared Error: MSE is computed by performing byte by byte comparisons of the cover image and stego-image. The computation can be expressed as follows:

$$MSE = \frac{1}{m*n}\sum_{1}^{m}\sum_{1}^{n}(\mathrm{Fij} - \mathrm{Gij})^2 \qquad 1$$

m: number of rows of cover image
n: number of column in cover image
Fij: pixel value from cover image
Gij: pixal value from stego image
Higher value of MES indicates dissimilarity between cover image and stego image.

Peak signal-to-noise ratio: PSNR measures in decibels the quality of the stego-image compared with the CVR. The higher PSNR indicates the better the quality of the image or lower distortion. The larger the PSNR value the smaller the possibility of visual attack by human eye [4] . The PSNR is computed using the following equation:

$$PSNR = 10log_{10}\frac{255^2}{MSE} \qquad 2$$

Correlation Factor: Correlation factor is one of the performance parameter. Correlation coefficient 'r' is the measure of extent and direction of linear combination of two random variables. If two variables are closely related, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related.

$$r = \frac{\sum_i(Xi - Xm)(Yi - Ym)}{\sqrt{\sum_i(Xi - Xm)^2}\sqrt{\sum_i(Yi - Ym)^2}} \qquad 3$$

Where
Xi - pixel intensity of original image
Xm- mean value of original image intensity
Yi- pixel intensity of encrypted image
Ym - mean value of encrypted image intensity

III. PROPOSED METHOD

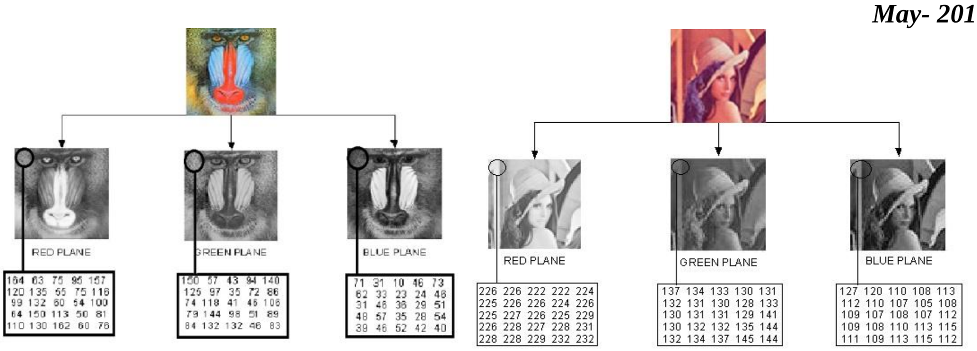
In proposed algorithm, we have taken the binary representation of the data image and hide into cover image. Here we introduced a new function before hiding the data image. The following formula, we have used in our proposed method is:

cover image + (data image – min. pixel value of each plane) = stego image

The data image that we need to hide in cover image is converted from decimal to binary form. In case of one bit LSB method, each pixel of data image is converted into 8 bit binary value. Then 8 sub pixels are formed using one pixel of data image. The LSB of each sub pixel is the bit value of the data image as shown in example:-

Let us take an example:
10110011 --- One pixel of Data image
00000001,00000000,00000001,00000001,00000000,00000000,00000001,00000001 --- Sub pixels of data image.

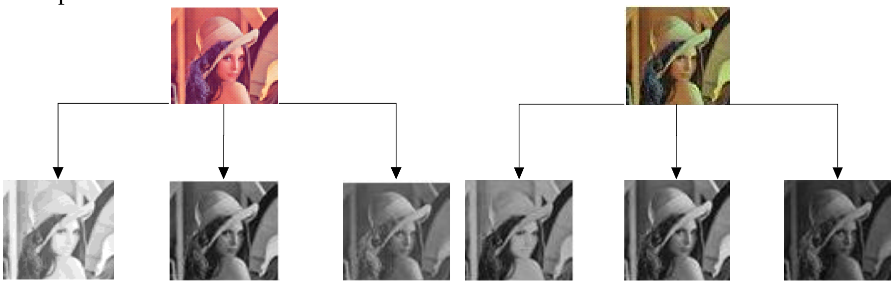
The maximum size of data image required is 64x64 pixels for 512x512 pixels cover image because each pixel of data image requires 8 pixels of cover image for hidding. Similarly, for 2 bit and 4 bit LSB method, the required pixels are 128x128 and 256x256 respectively. In case of 2 bit LSB method, each pixel of data image in converted into 4 sub pixels. Firstly, we obtain the pixel values of cover image and data image and then break the images into three planes red plane, green plane and blue plane. The three planes signifies three different matrices called RGB Matrix. RGB matrix representation of cover image and data image is shown in the following figure 2.



(A) (B)

Figure 2: (A) cover image with pixel vales, (B) data image with pixel vales

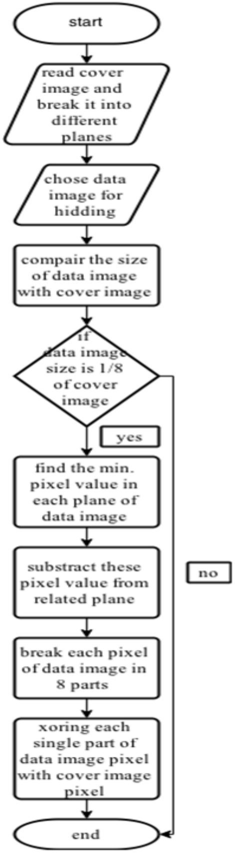
After breaking the data image in RGB plane, we find the pixel which have minimum value in each plane and subtract these values from each pixel of related plane.
Min. pixel value in red plane =64
Min. pixel value in green plane =0
Min. pixel value in blue plane =42



(A) (B)

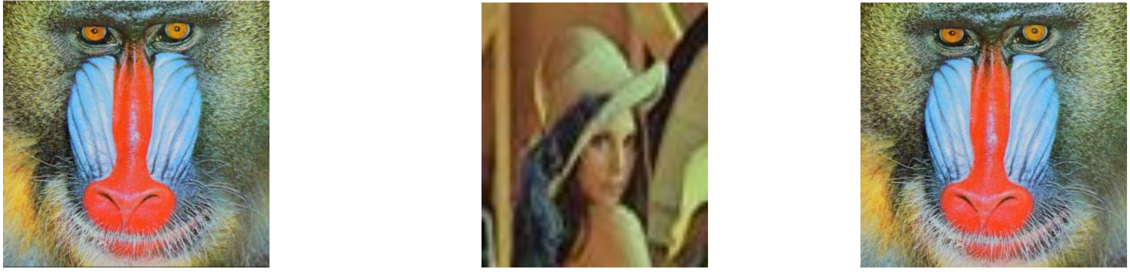
Figure 3: (A) Data image, (B) Data image after proposed method

Hiding Technique: To hide the data image we need the RGB matrix of both images. Then XORing technique is used. XORing of each data image pixel of RGB plane is done with each cover image pixel of RGB plane. For example, XORing of red plane of data image is done with red plane of cover image. After Xoring of both the image we get stego image, which is similar to cover image. After finding the stego image we compare this stego image with cover image and find out the value of MSE and PSNR. Flow chart of proposed method for 1-bit is shown below:


start
read cover image and break it into different planes
chose data image for hidding
compair the size of data image with cover image
if data image size is 1/8 of cover image
yes
no
find the min. pixel value in each plane of data image
substract these pixel value from related plane
break each pixel of data image in 8 parts
xoring each single part of data image pixel with cover image pixel
end

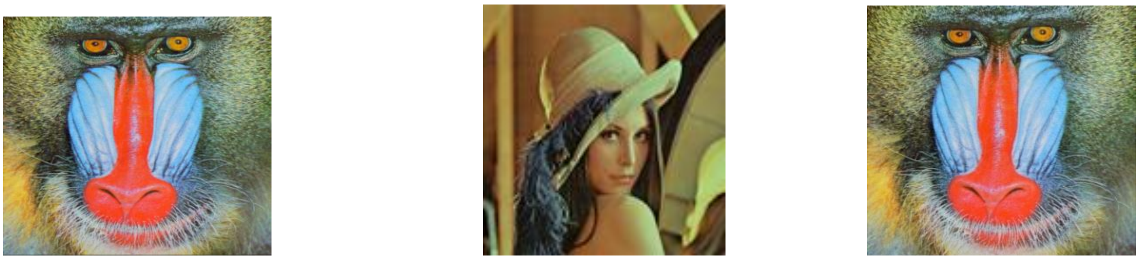
IV. EXPERIMENTAL RESULT AND DICUSSION

The results of our proposed algorithm are shown in this section. The MSE and PSNR values for modified n-bit LSB algorithm are shown in Table 2. Table 1 represents the previous results of paper [7].



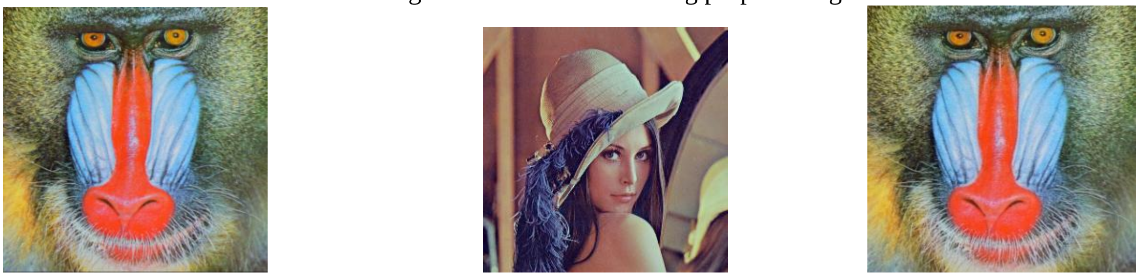
Cover image (512x512) Secret image (64x64) Stego image (512x512)

Figure 4: 1-bit method using proposed algorithm



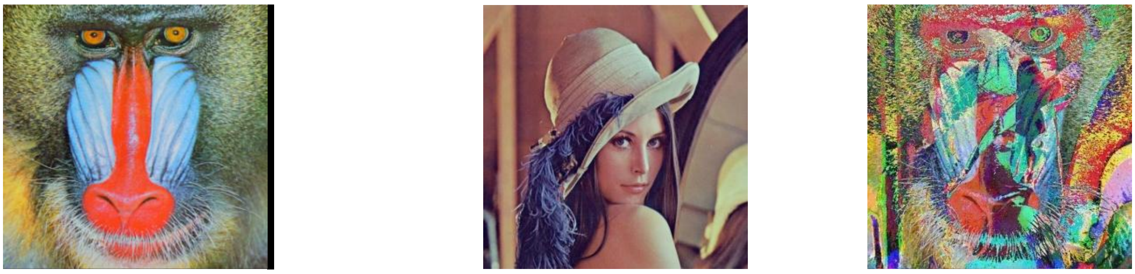
Cover image (512x512) Secret image (128x128) Stego image (512x512)

Figure 5: 2- bit method using proposed algorithm



Cover image (512x512) Secret image (256x256) Stego image (512x512)

Figure 6: 4-bit method using proposed algorithm



Cover image (512x512) Secret image (512x512) Stego image (512x512)

Figure 7: 8-bit method using proposed algorithm

After obtaining the output image we can say that, when we jump from 1-bit LSB method to higher LSB method the quality of stego image is distorted and due to this the MSE value will increase and the PSNR value will decrease.

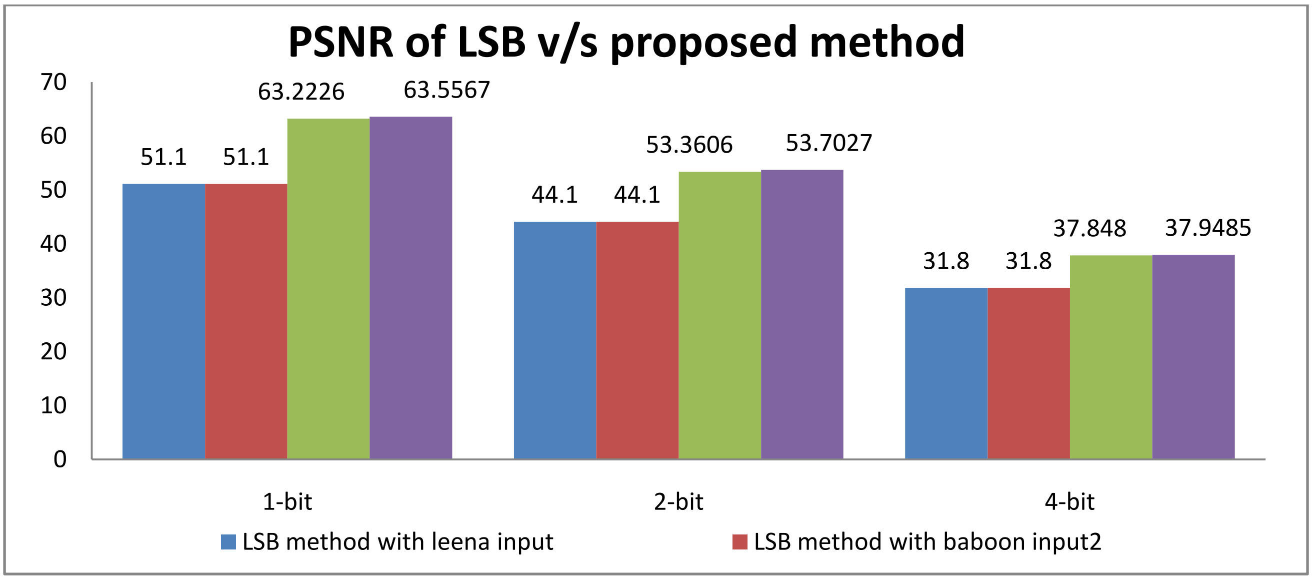
The output of 1 bit, 2 bit or 4 bit LSB method according to reference paper [7] is

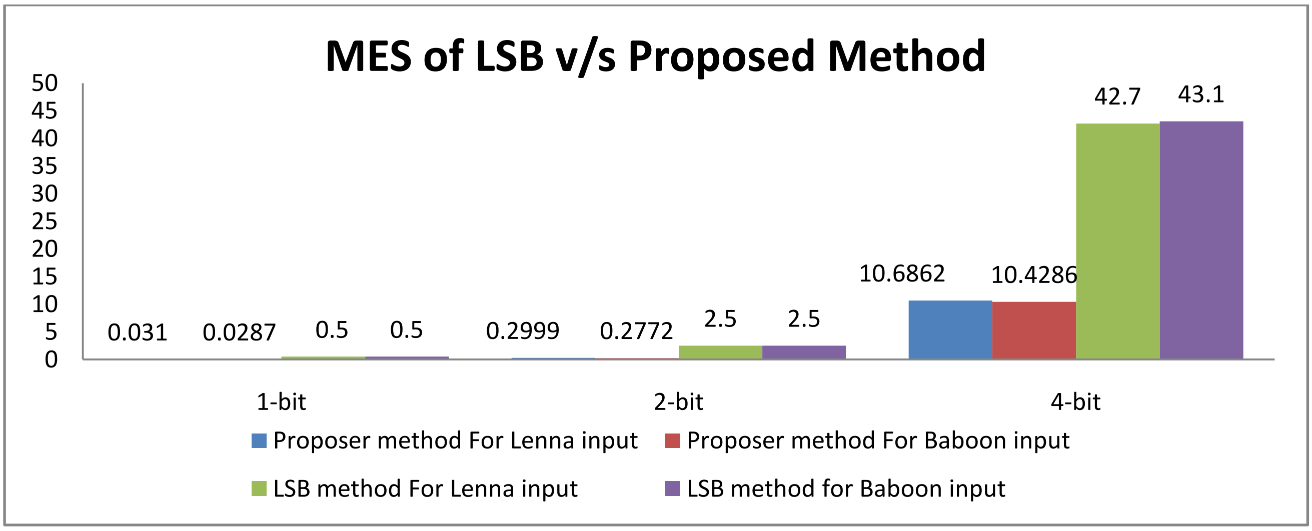
n-bit LSB	MSE		PSNR	
	Lenna	Baboon	Lenna	Baboon
1-bit	0.5	0.5	51.1	51.1

2-bit	2.5	2.5	44.1	44.1
4-bit	42.7	43.1	31.8	31.8

The output of 1bit, 2 bit or 4 bit proposed algorithm according to our study and analysis

n-bit LSB	MSE		PSNR	
	Lenna	Baboon	Lenna	Baboon
1-bit	0.0310	0.0287	63.2226	63.5567
2-bit	0.2999	0.2772	53.3606	53.7027
4-bit	10.6862	10.4286	37.848	37.9485





IV. CONCLUSION

In this paper we have implemented a new technique of data hiding using LSB algorithm in which we subtract the minimum pixel value of each plane from data image and then XORing of data image RGB matrix is done with the cover image RGB matrix. The experimental results show that the modified n-bit LSB algorithm is an effective way to hide the data image. and it is very difficult for the unauthorized user to identify the change s in stego image. This processes provides a new dimension for image steganography. Our proposed method provides better PSNR value where large PSNR indicates better quality of the image or in other terms lower distortion.

REFERENCE

[1] Atallah M. Al-Shatnawi. A New Method in Image Steganography with Improved Image Quality. *Applied Mathematical Science*,2012, 6(79), 3907 – 3915.

[2] B. Pfitzmann. Information hiding terminology. *Information Hiding Springer Lecture Notes in Computer Science*, 1996, 1174, 347–350.

[3] E. Franz, A. Jerichow, S. Moller, A. Pfitzmann, & I. Stierand. Computer based steganography. *Information Hiding Springer Lecture Notes in Computer Science*. 1996 1174, 7–21.

[4] M. Hossain, S.A. Haque & F. Sharmin. Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation. *Proceedings of 2009 12th International Conference on Computer and Information Technology*. 2009, 21-23.

[5] Ali K. Hmood & B.B Zaindan. An Overview on hiding information techniques in images. *Journal of applied Science Asian Network for scientific information*, 2010, 10(18).

[6] Mohammad Tanvir Parvez & Adnan Abdul-Aziz Gutub. RGB intensity based variable bits image steganography. *IEEE Asia Pacific Services Computing Conference*,2008.

[7] Bassam Jamil Mohd, Saed Abed & Thaier Al-Hayajneh. FPGA Hardware of the LSB Steganography Method. *IEEE potentials*, 2012.

[8] Youssef Bassil. Image Steganography Method based on Brightness Adjustment. *Advances in Computer Science and Application (ACSA)*, 2012, 2(2).

[9] Dr. Sudeep D. Thepade & Smita S. Chavan. Cosine, walsh and Slant Wavelet Transforms for Robust Image Steganography. *International Conference on wireless and Optical Communication Networks*,2013, 26-28.

[10] Fangjun Huang. New Channel Selection Rule for JPEG Steganography. *IEEE Transactions on Information Forensics and Security*, 2012, 7(4).