International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2020 International Journals of Sciences and High Technologies
http://ijpsat.ijsht-journals.org
Vol. 18 No. 2 January 2020, pp. 83-87

An Improved Quality and Security of LSB Based Steganography Technique Using XOR Bitwise Operation in 24 Bit Color Image

Serhat Cihangir[1] and Huseyin Canbolat[2]

[1,2] Electric and Electronics Engineering
Ankara Yildirim Beyazit University
Ankara-TURKEY

Abstract — **Information privacy has become the overborne issue today with the increasing use and efficiency of electronic data processing. The main purpose on privacy of communication is to provide secure connection with target without being captured by the third persons or by bringing them in such a way that they cannot understand. In the most general sense, steganography is the study and practice of concealing information to provide security of communication. The classic LSB (least significant bit) technique and methods which are derived from classic lsb, are used in steganography techniques on spatial domains. For the case of security, the classic LSB technique is very weak because it is very simple and predictable. Also, it causes distortion of image. In this paper, we propose an improved LSB Steganography technique to increase security and decrease the distortion of image. The proposed method is based on hiding two bits of secret data in one color (rgb) pixel with only one least significant bit change in one of the layers. LSB value of red layer is used in XOR operation with both LSB values of green and blue layers respectively. Only with one LSB bit change, 2 bits of secret data can be hidden, because nature of XOR bitwise operation. XOR operation provide the more secure and unpredictable communication than classic LBS. This method performed on to different images. Furthermore, it observed that the improved method reveals good result as the "Peak Signal to Noise Ratio (PSNR)" and "Mean Square Error (MSE)" than classic LSB method.**

***Keywords* — Color Image, LSB (Least Significant Bit), MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), Security, Steganography, XOR Bitwise Operation.**

I. INTRODUCTION

Along with increasing use of digital technology and the ease of access to the wide storage options including cloud storages, a new avenue for digital communication, called steganography, was emerged. If the technique term ‘’steganography’’ is not given, it may be confused with cryptography. Although both technique aims to carry information to a specific receiver or group of receivers as camouflaged, the existence of cryptographic communication is mostly evident while transferred information in steganography is concealed. In other words, while both techniques camouflage the chosen content, steganography is much more difficult to detect and process depending on the developed steganographic system which supposed to provide some features to embed data imperceptibly such as, promoting high information rate or payload, and impedance for removal [1].

Widespread use of computer, the internet, and perceiving of its incredible processing power, development of digital signal processing (DSP) carried the concept of steganography in the digital world. Carrying the steganography to the digital world resulted with an environment of corporate vigilance that has spawned varieties of applications which assure its proceeding evolution is to be able to hide contemporary information in digital atmosphere.

Image steganography methods consist of two groups which are time domain and frequency domain. In time domain also known as spatial domain [2], message bits are hidden directly intensity of pixel despite of in frequency domain message bits are hidden after transform of image [3].

Least significant bit (LSB) steganography [4] is the common and simple approach to embed information in a cover file. It needs no complex operation. It changes to number of some the least significant bits from pixel. It embeds bits of a payload into the LSB plane of a cover image.

K. Joshi,et.al.[5], used to XOR operation on spatial domains as an approach of steganographic method. Insertion method is least and most two bits are performed with XOR operation respectively on the gray scale image.

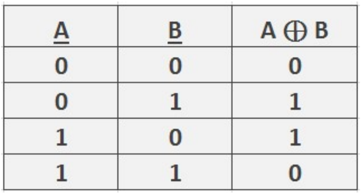
Hamzeh Hajizadeh et al. [6] introduced new method which provides high data capacity method in spatial image steganography. The proposed method based on extended lock based system from of Zhang and Wang's EMD eight directions multiple bits hide method in group of pixels in time domain. Also, this method combined with the Yang's Inverted Pattern (IP) approach as well as personally defined XORed pattern (XORP) and XNORed pattern (XNORP) approaches to achieve further enhancement.

II. Proposed Method

In this part, a new improved LSB technique with XOR operation is explained down to the last detail. In this method, two bits of secret messages is hidden one color pixel which is consist of three layers; red, green and blue. This method based on XOR operation advantage. Red layer least significant bit is performed XOR operation for green and blue layer least significant bits respectively. In order to equal result of two operations with two bits of secret message, only one bit is changed. This is the natural advantage of the XOR process.

A. *Natural advantage of XOR Operation*

Basically, XOR operation gives the true only when one input is true and other is false. Given table in Fig. 1 is the truth table of XOR operation. (A ⊕ B)



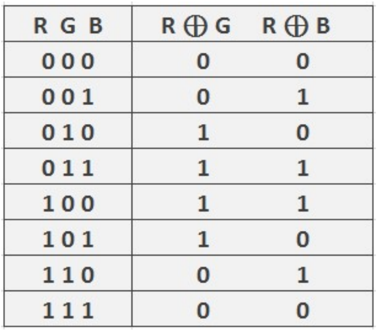
A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Fig. 1. Two bits XOR operation result

B. *Proposed XOR Operation on LSB of Red, Green and Blue Layers*

Given table in Fig. 2. shows all three bits combination of least significant bit of red, green and blue layer. In addition, exhibited table gives the result of XOR operation between red-green and red-blue layers.

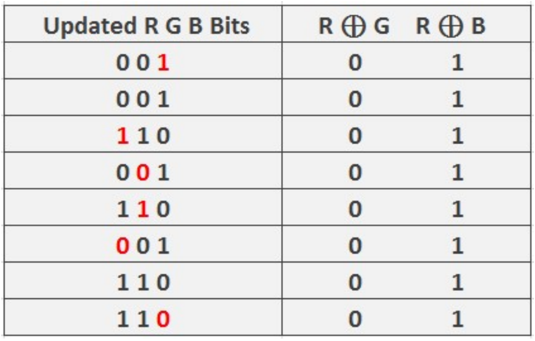
For example, two secret bits of message is equal "01" means one bit change, and the result of XOR operations can be equal to "01".



R G B	R ⊕ G	R ⊕ B
0 0 0	0	0
0 0 1	0	1
0 1 0	1	0
0 1 1	1	1
1 0 0	1	1
1 0 1	1	0
1 1 0	0	1
1 1 1	0	0

Fig. 2. One bit changed result for XOR Operation

Given table in Fig. 3. shows example of one bit change on all possibilities of three bit to obtain output result of "01".



Updated R G B Bits	R ⊕ G	R ⊕ B
0 0 1	0	1
0 0 1	0	1
1 1 0	0	1
0 0 1	0	1
1 1 0	0	1
0 0 1	0	1
1 1 0	0	1
1 1 0	0	1

Fig. 3. One bit changed result for XOR operation

C. *Insertion Algorithm*

- Take the image I.
- Read the all pixels which are consist of red, green and blue layer.
- Get the Pixel P and location (P = I(x,y)).
- Convert the all layer of pixel value into its binary equivalent.
- Get R1, G1, B1, Where;
- R1 is the Least Significant Bit (LSB) of Red Layer in pixel
- G1 is the Least Significant Bit (LSB) of Green Layer in pixel
- B1 is the Least Significant Bit (LSB) of Blue Layer in pixel.
- Two secret bits are represented by S2, S1
- Result of XOR operation respectively X2 and X1, where X2=R1⊕G1 and X1=R1⊕B1.
- To provide equal result of XOR operation and secret bits (S2=X2 and S1=X1), loop is shown below;

➢ If R1=0 then

- If G1=0 and B1=0 then

  If S2=0 and S1=0 then → No Change.

  If S2=0 and S1=1 then → Set B1=1.

  If S2=1 and S1=0 then → Set G1=1.

  If S2=1 and S1=1 then → Set R1=1.

- If G1=0 and B1=1 then

  If S2=0 and S1=0 then → Set B1=0.

  If S2=0 and S1=1 then → No Change.

  If S2=1 and S1=0 then → Set R1=1.

  If S2=1 and S1=1 then → Set G1=1.

```
        ▪ If G1=1 and B1=0 then
          If S2=0 and S1=0 then → Set G1=0.
          If S2=0 and S1=1 then → Set R1=1.
          If S2=1 and S1=0 then → No Change.
          If S2=1 and S1=1 then → Set B1=1.
        ▪ If G1=1 and B1=1 then
          If S2=0 and S1=0 then → Set R1=1.
          If S2=0 and S1=1 then → Set G1=0.
          If S2=1 and S1=0 then → Set B1=0.
          If S2=1 and S1=1 then → No Change.
➢ If R1=1 then
        ▪ If G1=0 and B1=0 then
          If S2=0 and S1=0 then → Set R1=0.
          If S2=0 and S1=1 then → Set G1=1.
          If S2=1 and S1=0 then → Set B1=1.
          If S2=1 and S1=1 then → No Change.
        ▪ If G1=0 and B1=1 then
          If S2=0 and S1=0 then → Set G1=1.
          If S2=0 and S1=1 then → Set R1=0.
          If S2=1 and S1=0 then → No Change.
          If S2=1 and S1=1 then → Set B1=0.
        ▪ If G1=1 and B1=0 then
          If S2=0 and S1=0 then → Set B1=1.
          If S2=0 and S1=1 then → No Change.
          If S2=1 and S1=0 then → Set R1=0.
          If S2=1 and S1=1 then → Set G1=0.
        ▪ If G1=1 and B1=1 then
          If S2=0 and S1=0 then → No Change.
          If S2=0 and S1=1 then → Set B1=0.
          If S2=1 and S1=0 then → Set G1=0.
          If S2=1 and S1=1 then → Set R1=0.
```

D. Retrieval Algorithm

- Obtain the stego image **got** after the insertion of secret message by insertion algorithm.
- Trace out location.
- Get the R1, G1, B1 bits of selected pixel. (LSB bits of Red, Green and Blue layer)
- Then, calculate XOR operation between R1-G1 and R1-B1.
- Result of XOR operation gives the two secret message bits.

E. Flow Chart of Insertion and Retrieval of Message

Information about insertion and retrieval method given as flowcharts in Fig. 4, and Fig.5, respectively.

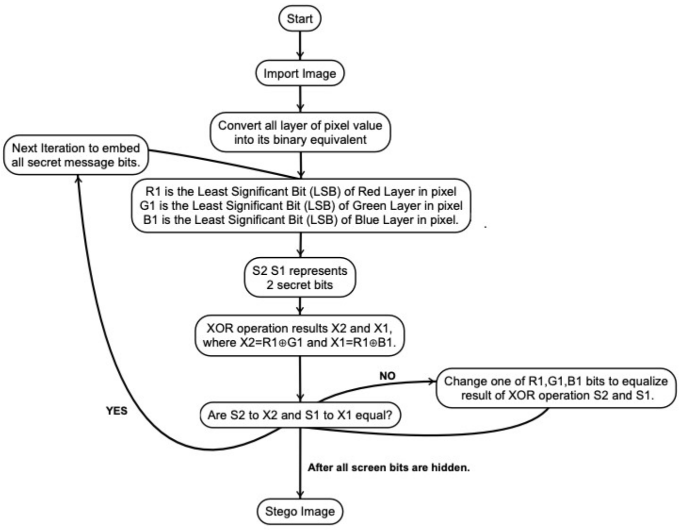

Start
Import Image
Convert all layer of pixel value into its binary equivalent
Next Iteration to embed all secret message bits.
R1 is the Least Significant Bit (LSB) of Red Layer in pixel
G1 is the Least Significant Bit (LSB) of Green Layer in pixel
B1 is the Least Significant Bit (LSB) of Blue Layer in pixel.
S2 S1 represents 2 secret bits
XOR operation results X2 and X1, where X2=R1⊕G1 and X1=R1⊕B1.
NO
Change one of R1,G1,B1 bits to equalize result of XOR operation S2 and S1.
YES
Are S2 to X2 and S1 to X1 equal?
After all screen bits are hidden.
Stego Image

Fig. 4. Flow chart for insertion of message

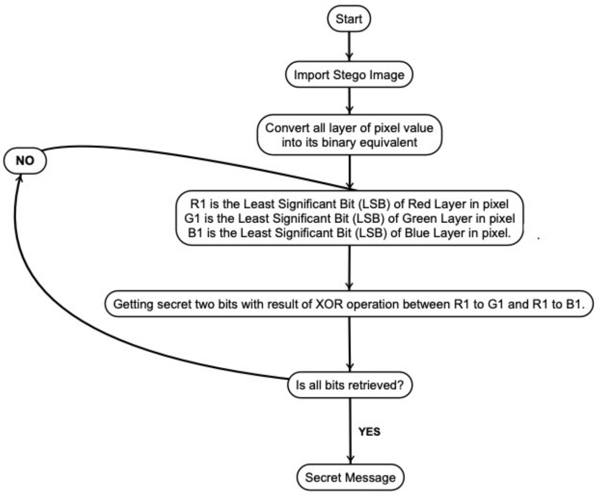

Start
Import Stego Image
Convert all layer of pixel value into its binary equivalent
NO
R1 is the Least Significant Bit (LSB) of Red Layer in pixel
G1 is the Least Significant Bit (LSB) of Green Layer in pixel
B1 is the Least Significant Bit (LSB) of Blue Layer in pixel.
Getting secret two bits with result of XOR operation between R1 to G1 and R1 to B1.
Is all bits retrieved?
YES
Secret Message

Fig. 5. Flow chart for Retrieval of message

III. Experimental Result

This section compares experimental results of the proposed method. This improved LSB method was tested on four color images “Lenna”, “Baboon”, “Barbara”, “Boots” in all size of 480x480. As a comparison parameter, security issue, MSR and PSNR are selected. In the experiment, three different size 1024, 2048 and 4096 bits secret message are hidden in all color picture and compared on the parameter.

A. MSE

Mean Square Error give the information about differences between two images. The value of MSE should be as possible as low to confirm the reliability of method. The formula of MSE is given in Eq (1).

$$MSE = \frac{1}{R \times C}\sum_{i=1}^{R}\sum_{j=1}^{C}(x_{ij} - x'_{ij})^2 \qquad (1)$$

Where xij and x'ij is the original and stego images respectively.

B. PSNR

Peak signal to noise ratio reveals how two images are similar. It measures peak error between two images. PSNR should be as possible as high for obtaining quality method of steganography. The PSNR of any image can be calculated by using Eq (2) [9].

$$PSNR = 10\,log_{10}[\frac{I^2}{MSE}] \qquad (2)$$

Where I is the dynamic range of pixel values, or the maximum value that a pixel can take, for 8-bit images: I=255. MSE is the mean square error.

C. Results for Improved XOR Based Steganography Method

1. Result for Image Lenna

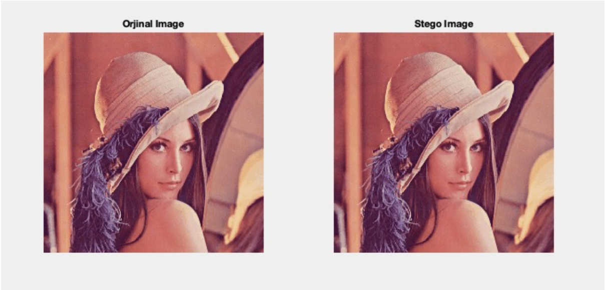


Fig. 6. Original and Stego Images

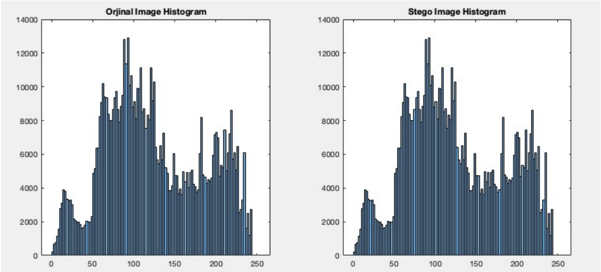


Fig. 7. Histogram for message size 512 bits

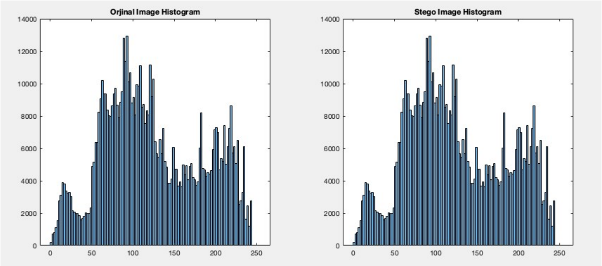
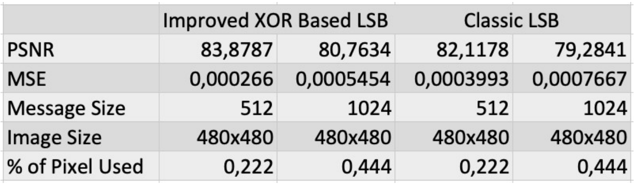


Fig. 8. Histogram for message size 1024 bits



	Improved XOR Based LSB		Classic LSB	
PSNR	83,8787	80,7634	82,1178	79,2841
MSE	0,000266	0,0005454	0,0003993	0,0007667
Message Size	512	1024	512	1024
Image Size	480x480	480x480	480x480	480x480
% of Pixel Used	0,222	0,444	0,222	0,444

Table 1. Performance analysis of the proposed method using various parameters.

2. Result for Image Baboon

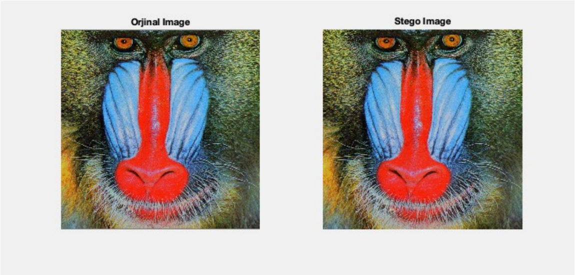


Fig. 9. Original and Stego Image

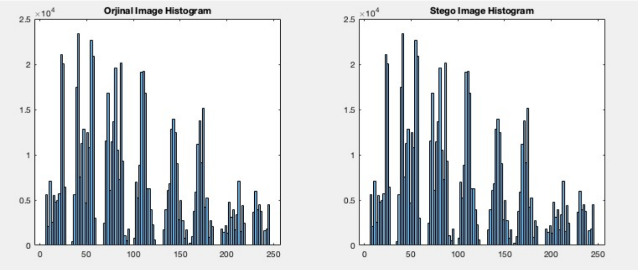


Fig. 10. Histogram for message size 512 bits

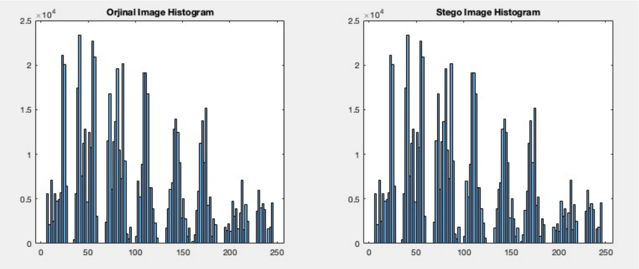
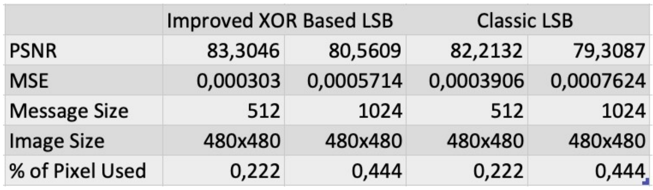


Fig. 11. Histogram for message size 1024 bits



	Improved XOR Based LSB		Classic LSB	
PSNR	83,3046	80,5609	82,2132	79,3087
MSE	0,000303	0,0005714	0,0003906	0,0007624
Message Size	512	1024	512	1024
Image Size	480x480	480x480	480x480	480x480
% of Pixel Used	0,222	0,444	0,222	0,444

Table 2 Performance analysis of the proposed method using various parameters.

3. Results for Image Boats

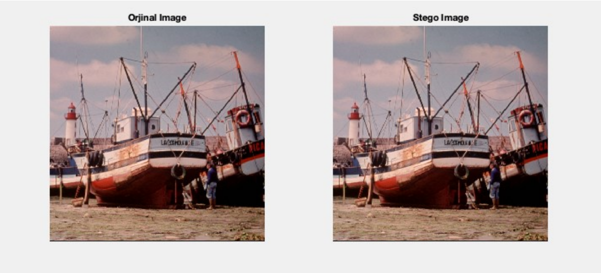


Fig. 12. Original and Stego Images

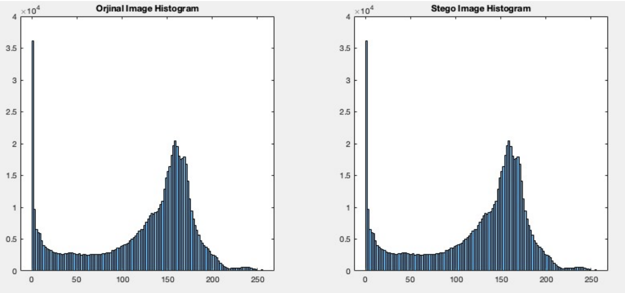


Fig. 13. Histogram for message size 512 bits

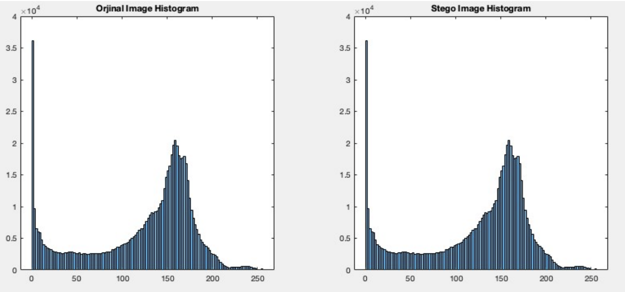
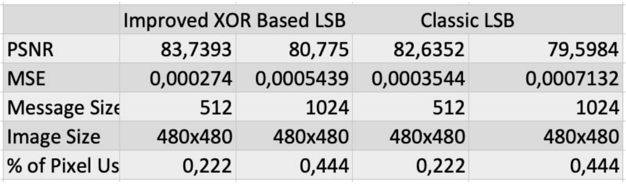


Fig. 14. Histogram for message size 1024 bits



	Improved XOR Based LSB		Classic LSB	
PSNR	83,7393	80,775	82,6352	79,5984
MSE	0,000274	0,0005439	0,0003544	0,0007132
Message Size	512	1024	512	1024
Image Size	480x480	480x480	480x480	480x480
% of Pixel Us	0,222	0,444	0,222	0,444

Table 3. Performance analysis of the proposed method using various parameters.

V. Conclusion

Improved XOR based LSB operation is proposed in this article. PSNR and MSE values for all three images are better than traditional LSB method as demonstrated in the tables Experimental result shows that proposed XOR based LSB method provides low image distortion which means that high PSNR value and low MSE value and high communication security. XOR operation used in this method is not predictable.

References

[1] L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, Publisher, City, 1999.

[2] V.M. Potdar, S. Han, E. Chang, "Fingerprinted secret sharing steganography for robustness against image cropping attacks", in: Proceedings of IEEE Third International Conference on Industrial Informatics (TNDIN), Perth, Australia, 10-12 August 2005, pp. 717-724.

[3] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[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 (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.

[5] K. Joshi, P. Dhankhar and R. Yadav, "A New Image Steganography Method in Spatial Domain Using XOR," in Annual IEEE India Conference (INDICON), New Delhi, 2015.

[6] H. Hajizadeh, A. Ayatollahi, and S. Mirzakuchaki, "A new high capacity and EMD-based image steganography scheme in spatial domain," 21st Iran. Conf. Electr. Eng. ICEE 2013, 2013.