International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9 (2017) pp. 1950-1955

A New Image Steganography Depending On Reference & LSB

Saher Manaseer[1*], Asmaa Aljawawdeh[2] and Dua Alsoudi[3]

[1]King Abdullah II School for Information Technology, Computer Science Department, The University of Jordan, Amman, 11942, Queen Rania Street, Jordan.

[2]The University of Jordan, Amman, 11942, Queen Rania Street, Jordan.

[3]The University of Jordan, Amman, 11942, Queen Rania Street, Jordan.

[1]Scopus Author ID: 24473138700, Researcher ID: C-8197-2015

Abstract

Steganography is the science of hiding information using a digital media carrier in a way that prevents attackers and Intruders from revealing information and sharing it with others. Digital images are the most popular carrier for steganography. This paper presents a new technique used by embedding the secret message into colored images. Two versions of the proposed algorithm, named standard LSB and Condition Based LSB respectively, are proposed and tested in this paper. The experiment measures PSNR (Peak Signal to NOISE Ratio) and MSE (Mean Squared Error) for the two versions show that the standard LSB version outperforms the second proposed version.

Keywords: *Steganography, PSNR, MSE, Information Hiding*

INTRODUCTION

Most systems suffer the problem of hacking actions that change and allow the modification of restricted data by intruders. To solve this issue those systems need to hide real information in a way that keeps them secured, Encryption and Steganography are the most well-known ways used to secure the secret message during transmission; Encryption is concerned with encoding and decoding using the suitable key. Steganography is the concept of hiding information using a digital media carrier Emam, et alin[1].

Steganography as a word origin come from Greek and it means "Covered Writing", Emam, et al in[1]. In general, Steganography focusses on how to hide the secret message using the digital carriers with unnoticed and less attractive way, Emam, et al in [1]. The carrier can be images, audio files or video files, but the most widely used carriers are the digital images. Digital images are the most popular media used over Internet. Digital images are best used for they can hide acceptable amount of data without being visible to the human eye, due to the high redundancy of data. Thenmozhi & Menakadeviin [3], Shabnam & Hemachandran in [4].

The main four types of steganography according to Pandit, et al. in [6]:

a. Image- Steganography:

   The image steganography is about hiding data within an image, taking into consideration the change should not be visible into original image.

b. Audio- Steganography:

   Audio Steganography is hiding information in an audio file. The stego audio file should be undetectable.

c. Video- Steganography:

   Video Steganography is to hide information in a video file. The stego video file should be undetectable by attacker.

d. Text files- Steganography:

   Text Steganography is hiding information in a text file.

The most known image steganography algorithm is Least Significant Bit embedding (LSB). Mainly, there are two techniques for embedding images in Steganography: spatial domain and transform domain (frequency domain). Spatial domain techniques, involves direct modifications to the pixel values, whereas the transform domain technique modifications depend on the transform domain coefficients that are obtained. Emam, et al. in[1], Shabnam & Hemachandran in [4] and Datta, et al. in[5].

The basic model of steganography is shown in Figure 1:

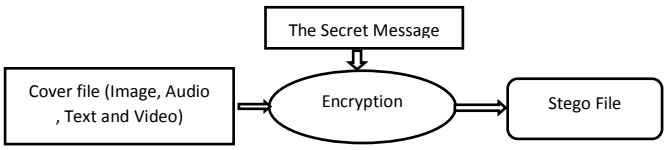

Figure 1: Basic model of steganography

Steganography process consists of the Carrier (cover object), Message (it can be any type of data) and Password (stego key) [1]. The main goal of stenographic system is the image quality. The Peak Signal to Noise Ratio (PSNR), and Mean Squared Error (MSE) metrics are the most common measures used to evaluate the quality of the image [1][4]. PSNR to determine the degradation in the embedding image with respect to the cover image [1]. PSNR & MSE equations as below [1]:

$$MSE = \left(\frac{1}{MN}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - X_{ij}^{\backprime})^2 \qquad (1)$$

$$PSNR = 10log_{10}\frac{I^2}{MSE} \quad (2)$$

Where X_{ij} is the i is the row, j is the column for the pixel in the original image (cover image), X_{ij}^{1} is the i is the row , j is the column for the pixel in the stego image, MN are the size of the image where M is the height and N is the width and I is the range pixel value. For 8 bit images, $I = 255$.

Steganography faces three challenges as Shabnam&Hemachandran found in[4] and Datta, et al. in[5]; Robustness of steganography is defines how strong the used stenographic technique exhibits against the changes. The second challenge is Imperceptibility, which is the power to hide data without being notice by human senses. The third challenge is Capacity, which is the size of the data that being hided depend on the size of carrier.

RELATED WORKS

LSB (Least Significant Bit) steganography has been widely used to embed information within image due to its simplicity and more imperceptible technique. Different Authors used the simple LSB techniques to hide data by replacing the pixels with secret data bits according to Artz in[7]. Thenmozhi&Menakadeviin[3], worked on hiding the secret image into cover image, where both images should have the same size. Their technique first compresses the secret message using Set Partitioning in Hierarchical Trees (SPIHT) algorithm, then the output of this compression is embed into the cover image using default LSB technique. The compression is made by wavelet transform and then by using the SPIHT coding. Image quality is retained with high PSNR values. Shabnam, S. ,&Hemachandranin[4], embed the secret message file into the covered image, the image should be colored and transformed into 3 matrices (R, G, B). The message convert to binary, depending on the secret message bit using OR or AND operation, sequentially (RGB, BGR, RGB, BGR…). Their results showed better performance in terms of quality of the stego image obtained. On the other handKaur, G., &Kochharin[2], used two different techniques LSB and DCT to perform steganography. It gives a good result according to the PSNR values comparing with previous works and the security was increased by using DCT. Emam, et al.in [1], embedded the message by hiding the byte of the message in three pixels only based on randomization in the cover image using Pseudo Random Number Generator (PRNG) of each pixel value. In the embedding technique (2-1-2) layer is used (two layers Blue and green) and the byte of the message being embedded in three pixels only in this form (3-2-3). They found that their method achieved a very high Maximum Hiding Capacity and Higher visual quality as indicated by PSNR.

Guptain [9], tried to overcome the disadvantage of the LSB method by appending encrypted data in image in place of plain textual data. To encrypt the data RSA and Diffie Hellman algorithms were used. To check the efficacy of the proposal, they calculated the number of instructions executed at sender and receiver site since the number of instructions executed is a measure of time complexity of the process. The result showed that the use of encryption in Steganalysis does not affect the time complexity if Diffie Hellman algorithm is used instead of RSA algorithm.

Al-Shatnawiin [8],used a methodology that hide the secret message based on searching for the identical bits between the secret messages and image pixels' values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hides the secret message directly in the least two significant bits of the image pixels. This paper concludes that the proposed method is more efficient, simple, appropriate and accurate than LSB method, it searches for the identical bits then starts hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure.

Mandal& Dasin[10], used Pixel-Value Differencing (PVD) method as image steganography scheme; the pixel values in the stego image may exceed the range 0 … 255. Therefore, they have eliminated this overflow problem of each component pixel. Moreover, for providing more security, they have used different number of bits in different pixel components. It was very difficult to trace how many bits are embedded in a pixel of the stego image. The results obtained in proposed method provides better visual quality of stego-image compared to the PVD method.

THE PROPOSED METHOD:

The proposed method of encoding is shown in Figure 2:

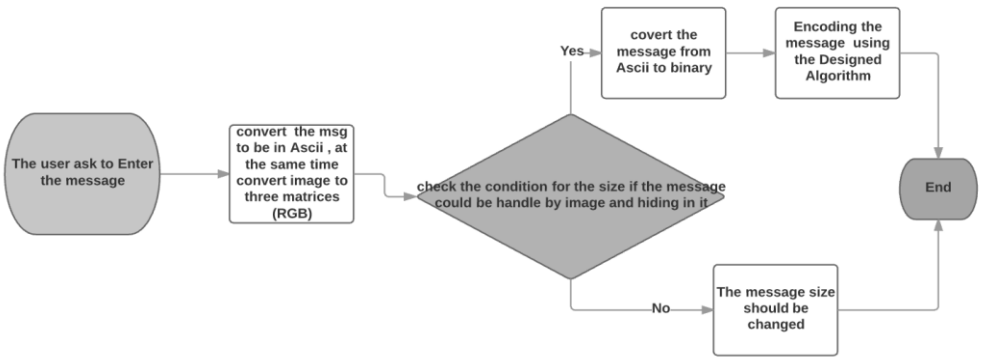

Figure 2: Encoding process according to the proposed method.

Figure 3 explains the Encoding steps of the proposed algorithm:

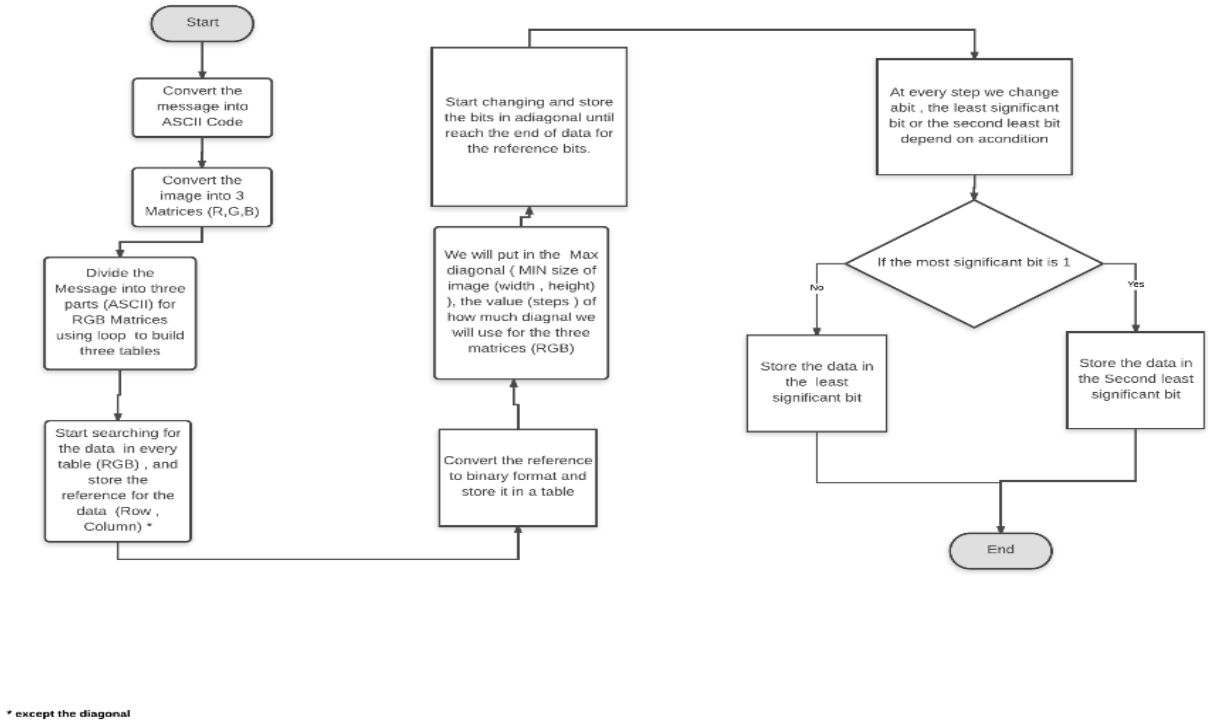

Figure 3: Encoding process according to the proposed method in details

Algorithm :

The main core of this paper is how to hide data in an image (.jpg) after converting it into 3 matrices (R, G,B), then searching for the reference of the data and use it in hiding information.

The Algorithm in details:

1- The message: "hello", converted in to ASCII code = "104 101 108 108 111"

2- Convert the Image (.jpg) into 3 matrices (R, G, B)

3- Build a table after searching for the message ASCII code (Using loop).

Table 1: Reference Table in three matrices (R, G, B)

1- For R matrix 2- For G matrix 3- For B matrix	Message ASCII	Row Reference	Colum Reference
1	**104**	**4**	**24**
2	**101**	**3**	**11**
3	**108**	**2**	**20**
1	**108**	**6**	**24**
2	**101**	**5**	**34**

- Note that while searching, the diagonal is skipped because the algorithm uses it.

4- Build a table for the total for the whole data:

Table 2: Total data found for the secret message in three matrices (R, G, B)

Matrix	Data found
R	2
G	2
B	1

5- The value of Data found in the table above is multiplied by 8 to calculate the number of steps and bits are going to be used later. Then, the results are used to fill the diagonal of the matrix.

Table 3: Calculating bits that are needed to be changed in three matrices (R, G, B)

Matrix	Data Found	CALCULATIONS	Final data to be used
R	2	2*8=16*2 =32	32
G	2	2*8=16*2 =32	32
B	1	1*8=8*2 =16	16

6- The algorithm places "Final data to be used" in the diagonal (Start from the maximum size of the image). It is worth mentioning that the last column will not be used

for the three matrices R, G, B. Moreover, the minimum between columns and rows (e.g. size 33*34) which equals (33*33) is the maximum size of the image.

7- The algorithm starts to change the data reference (row reference and column reference) from decimal to binary (into 8 bits), as shown in the Table 4:

Table 4: Data reference (row, column) with binary in three matrices (R, G, B)

1-For R matrix 2-For G matrix 3-For B matrix	Message ASCII	Row Reference	Column Reference	Row Reference binary	Column Reference binary
1	104	4	24	00000100	00011000
2	101	3	11	00000011	00001011
3	108	2	20	00000010	00010100
1	108	6	24	00000110	00011000
2	101	5	34	00000101	00100010

For whole data, we will need (16*5 = 80) numbers in the diagonal to be changed.

8- Next is changing the data, starting from R matrix:

Table 5: Start to change bits in R matrix

1-For R matrix 2-For G matrix 3-For B matrix	Message ASCII	Row Reference	Column Reference	Row Reference binary	Column Reference binary
1	104	4	24	00000100	00011000
2	101	3	11	00000011	00001011
3	108	2	20	00000010	00010100
1	108	6	24	00000110	00011000
2	101	5	34	00000101	00100010

9- In LSB, changing the least significant bit in the diagonal. The proposed method changes the least significant bit or the second least significant bit based on the condition as follows: If the most significant bit is 1, the algorithm changes the second least Significant bit. Otherwise, the algorithm changes the least Significant bit. For example, R (32, 32) = 156, converted to binary: 156 = 10011100, the algorithm considers the most significant bit, which is 1 here. Consequently, the algorithm applies the change 1001110**0** and the bit should be stored here is 0, so it will not be changed. However, if 1 should be stored, then 0 is changed to 1 and after changing the number will have the following result in 1001111**0**. If the message size = K, the message size should follow the below condition (Mathematically):

$$(\text{Ceiling } [k/3] * 16) + 1 \leq \text{Min } (m, n), \quad (3)$$

while m and n is the size of image.

EXPERIMENTAL RESULTS

The proposed system has been implemented using MATLAB Environment (R2010a), using the known three pictures (Lena, pepper and baboon) with size (512*512) and measures the MSE, PSNR and the total bits changed. The message that embedded in whole Experiments is "HelloWorld".

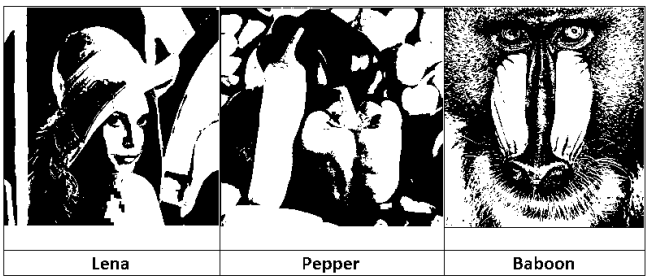

Figure 4: Pictures used in the Experiment

The results that have been collected are shown in the following tables and figures:

Table 6: MSE and PSNR for the method with the rule condition in the last step.

Picture	Bit1 change	Bit2 change	Total bit change COND	MSE COND	PSNR COND
Lena	55	24	79	0.00015259	86.2956
Pepper	14	64	78	0.00024414	84.2544
Baboon	64	8	72	0.00097275	78.2508

Table 7: MSE and PSNR for the method using default LSB in the last step.

Picture	Bit change LSB	MSE LSB	PSNR LSB
Lena	82	0.000049591	91.1768
Pepper	76	0.000045776	91.5244
Baboon	74	0.00097275	78.2508

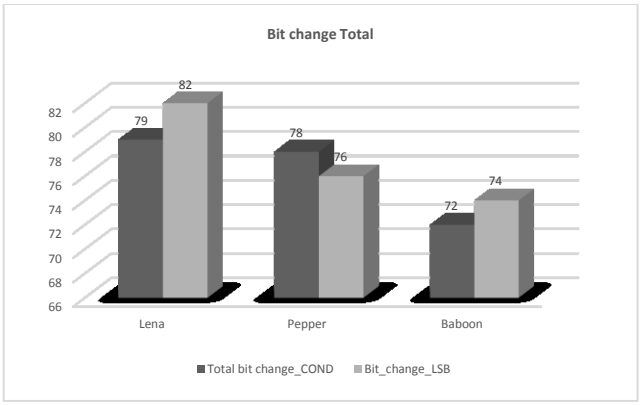

Figure 5: Total Bit Changed in both two methods.

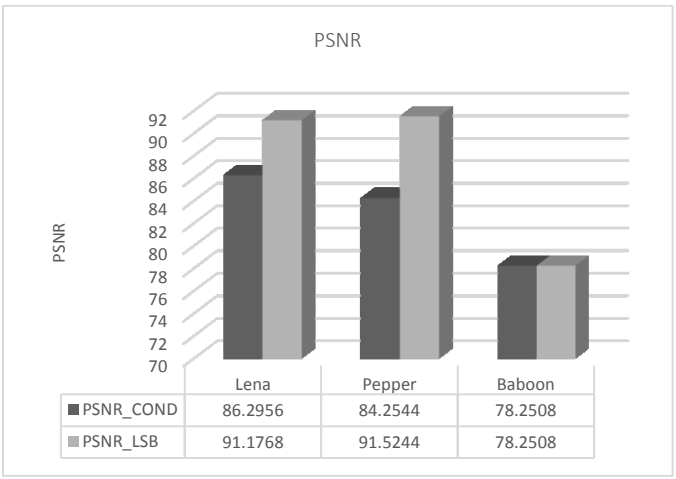

Figure 6: PSNR for both methods.

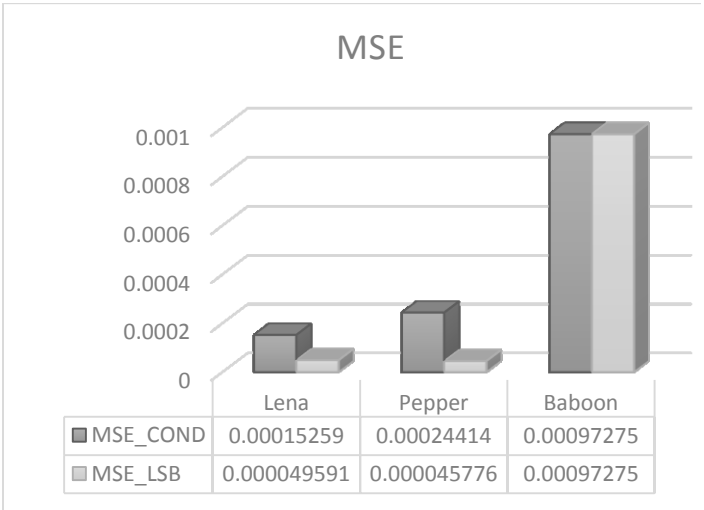

Figure 7: MSE for both methods.

Figure 8 displays the histogram that elustrates that the difference exists even if both have the same total number in changing bits. which depends later on MSE and PSNR values.

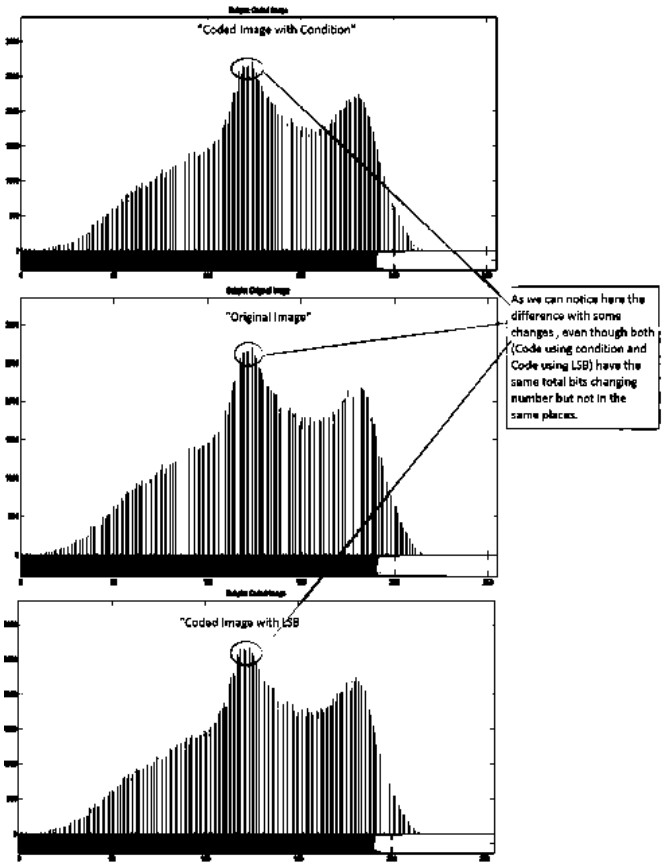

Figure 8: Histograms for Baboon Picutre

CONCLUSION

The experiment measures PSNR (Peak Signal To Noise Ratio) and MSE (Mean Squared Error) for the technique with two versions in last step to choose target bits. The standard LSB shows best performance than the condition based version which depends on the most significant bit value.

This technique is more secure compared with others due to depending on the reference of data, so we hide the reference not the real data. In addition, the way that used in diagonal and the condition that depend on the most significant bit value increase the security in this technique.

REFERENCES:

[1] Emam, M. M., Aly, A. A., &Omara, F. A. *An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection*. International Journal of Advanced Computer Science & Applications, *1*(7), pp. 361-366, (2016).

[2] Kaur, G., &Kochhar, A. *A steganography implementation based on LSB & DCT*. International Journal for Science and Emerging Technologies with Latest Trends, *4*(1), pp.35-41, (2012).

[3] Thenmozhi, M. J., &Menakadevi, T. *A New Secure Image Steganography Using Lsb And Spiht Based Compression Method*. International Journal of Engineering, 16(17), (2016).

[4] Shabnam, S. ,&Hemachandran , K. *LSB based Steganography using Bit masking method on RGB planes.* (IJCSIT) International Journal of Computer Science and Information Technologies*,* 7 (3) , pp.1169-1173, (2016) .

[5] Datta, B. , Mukherjee, U. , &Bandyopadhyay, S. *LSB Layer Independent Robust Steganography using Binary Addition*. International Conference on Computational Modeling and Security (CMS 2016), Elsevier Pub, (2016).

[6] Pandit, A. S., Khope, S. R., & Student, F. *Review on Image Steganography*. International Journal of Engineering Science, 6115, (2016).

[7] Artz, D. Digital steganography: hiding data within data. IEEE Internet computing, 5(3), 75-80, (2001).

[8] Al-Shatnawi, A. M. *A new method in image steganography with improved image quality*. Applied Mathematical Sciences, *6*(79), 3907-3915, (2012).

[9] Gupta, S., Goyal, A., &Bhushan, B. *Information hiding using least significant bit steganography and cryptography*. International Journal of Modern Education and Computer Science, *4*(6), pp.27, (2012).

[10] Mandal, J. K., & Das, D. *Colour image steganography based on pixel value differencing in spatial domain*. International journal of information sciences and techniques, *2*(4), (2012).