Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/100126

High Capacity Image Steganography Technique based on LSB Substitution Method

Marghny H. Mohamed[1,*] *and Loay M. Mohamed*[2]

[1] Department of Computer Science, Faculty of Computers and Information, Assiut University, Egypt
[2] Department of Computer Science, Faculty of Science, Assiut University, Egypt

Received: 26 Jun. 2015, Revised: 24 Aug. 2015, Accepted: 25 Aug. 2015
Published online: 1 Jan. 2016

Abstract: Steganography is the art of hiding important data by embedding secret message within other file. The least significant bit (LSB) is one of the most important considerations when one want to solve such problems. LSB substitution method exchanges some LSB of the cover-image with the secret data. In this paper, data hiding method using simple LSB substitution is proposed. The main goal of the presented method is to increase the embedding capacity and improve the image quality of the stego-image. The experimental results show better performance of the proposed method compared to the corresponding methods, in terms of PSNR and the capacity. The effectiveness of the model is estimated from the viewpoint of both the amount of data hidden and the image quality of the cover image.

Keywords: Steganography, LSB substitution, cover-image, stego-image, effectiveness

1 Introduction

The rapid development of the Internet offers great efforts to the transmission of secret data over networks. Secret data is candidate to unauthorized access. Therefore, transmission data secretly by internet needs much effort and becomes an essential topic. To keep the unauthorized user away, many different approaches have been proposed. Encryption and data hiding are two major methods to secured communication.

Encryption is the process of transforming data (plaintext) into a cipher text via cipher algorithms. The only user that has keys can decrypt the secret message from the cipher texts, as shown in Figure 1. The cipher text will look like meaningless and unreadable code for any unauthorized user does not have a key. The data encryption still has some weaknesses although it is a respectable way to secure data. It makes the messages suspicious enough and streams of meaningless to attract unauthorized attention and give an impulse to recover them. Moreover, when the unauthorized users have trouble recovering the cipher text out of range, they might simply destroy them so that the authorized users cannot get the data in time. That is the reason why data hiding is a hot topic and has been under consideration of researcher recently [1] and [6]

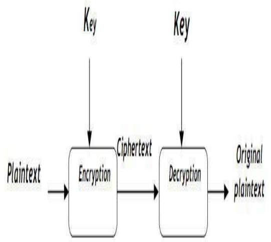

Fig. 1: Simplified Model of Conventional Encryption [2]

Data hiding methods hides the secret data into multimedia data such as sounds, images or videos. Three different aspects contend with each other characterize the techniques as shown in Figure 2: capacity, robustness, and security. Capacity is the amount of data bits that can be hidden in the cover medium relative to the size of the cover. This is measured in bits per pixel (bpp), robustness is the ability of the stego medium to remain intact and resist the modification before an eavesdropper can modify or destroy the hidden data, and security concerned about

* Corresponding author e-mail: marghny@aun.edu.eg

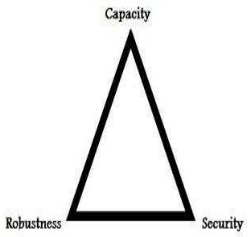

Fig. 2: features of information-hiding system [2]

the ability of an adversary to detect the hidden data easily [3]. Digital images are good secret communication method due to their insensitivity to human graphic system. Steganography is one main branch of the branches of the data hiding technology.

The art of covered or hidden writing is called steganography which hides the existence of the message. The Greek words steganos and graphia are the radix of the word Steganography and it means ”hiding writing” [5]. The main goal of steganography is how to hide a message from a third party by covert communication. The cryptography differs from this, which does not embed the presence of the secret communication but make a message unreadable by unauthorized users. Although steganography and cryptography are distinct and separate from each other, but there are some similarities between them, and some researchers define steganography as a type of cryptography since hidden communication is a type of secret writing [6]. Steganography uses audio, text, images, and video media for hiding data. The digital steganography technique has three basic components: 1) secret data, the data to be embedded, 2) the cover file (cover-carrier), which used to hold secret data inside, and 3) the resulting stego-file (stego-carrier).

Image steganography is used widely, compared with the other ways of steganography, this popularity because the amount of redundant data existing in the images that can be altered easily to hide secret messages in them, and because it has a limited power of the human visual system (HVS) [7]. The original image is called cover image and the embedded image is called the stego image. The secret message can be embedded in a cover image that has no sense, and then the sender transfers the stego image to the other side through a public channel. Whenever the cover image and the stego image are more similarities, it will be harder for an unauthorized person to obtain the stego image which the secret message embedded inside it. This way, the secret message can be transmited from the sender to the receiver safely and soundly.

Many steganographic methods for data hiding have been presented to hide secret data in digital images. One of the most common and well-known method is the LSB (least significant bit) techniques, which replaces some least significant bits of pixels in the original image with the secret message. The powerful of the LSB method are simplicity of computation and a large amount of data can be hidden in the original image with high visually.

Wang et al. [8] proposed an embedded technique in the moderately significant bit of the host image. A genetic algorithm is established to find optimal substitution matrix for embedding the secret messages. They also enhanced the stego-image quality by using local pixel adjustment process (LPAP).

Wang et al. [9] presented also a new method to hide data inside the cover-image. The basic concept of the method is carried out by the simple version of LSB substitution data hiding. They also solved the problem when k is large.

C.-K. Chan ans L.M. Cheng [11] proposed a data hiding method by the simple version of LSB substitution method. Low extra computational complexity based on an optimal pixel adjustment process is applied to the stego-image obtained by the simple LSB substitution scheme to improve the quality of the stego-image.

Wu and Hwang [12] presented some well-accepted schemes and classified them into two major types: high hiding capacities schemes and high stego-image degradation imperceptibility schemes. One of his methods called optimal LSBs method is a good choice for a large amount of data is to be hidden. On the other hand, two other methods called PVD and MBNS schemes which are superior to LSB-based schemes in terms of stego-image quality.

Marghny et al. [10] proposed a dynamic LSB substitution techniques by dividing the cover image into edge and smooth areas. This method can embed large amount of data as well as imperceptibility of stego image based on the pixel-value differencing for secret communication. Experimental results show that the proposed method can obtain a stego image with satisfactory quality. Moreover, it can resist steganalysis systems which are carried out by statistical analysis.

Marghny et al. [6] proposed a method for optimal key selection based on permutation method using genetic algorithms. The method is tested with varying data size as well as key space with different standard images. The experimental results show the improving of system security and decreasing of in computation time when the number of keys is increased.

Liao et al. [1] presented a novel method of steganographic to improve the multi-pixel differencing of LSB substitution to offer better stego-image quality and large amount of embedded message. Where, A four pixel blocks are considered with three difference values.

Marghny et al. [14] proposed a technique to embed secret message into the original image by a dynamic LSB substitution scheme. This scheme is carried out by utilizing the similarity in the smooth area not the edge area as in the simple techniques, and using the LSB substitution methods as a fundamental stage. This method increase the data capacity with preserving the quality of stego image.

Marghny et al. [4] propose an efficient steganographic method to embed message over gray scale images. This scheme is based on the nature of the human eye, which is more perceptive to the change in the smooth area than the edge area using pixel value difference, as well using the LSB substitution method as a fundamental stage. This method increased the capacity of embedding message, achieving the visual quality and more security.

In this paper, a method is proposed to increase the amount of capacity of embedding message and the quality of the stego-image based on LSB substitution scheme which embeds data by replacing k LSBs of a pixel in the cover image with k secret bits directly. A fixed number of LSB's is used. The cover image is divided into two parts and changing process is applied to the value of some bits that have the secret bits in the stego-image that are obtained by the simple form of LSB substitution technique. The experimental results on various standard images that evaluate the efficiency of the proposed method show that our method can embed a large amount of data than other methods and the quality of the stego image is enhanced as well.

The objective of this paper is handling the disadvantages of the previous LSB and enhancement scheme for steganography based on LSB substitution considering high capacity and high robustness, as well as system security. Therefore, we presented a method that improves data hiding method based on simple LSB substitution method.

The organization of the rest of this paper is going as follows. Briefly description about the simple LSB substitution method is introduced in Section 2.Section 3. demonstrates the optimal LSB method. Our scheme is presented in Section 4. Experimental results are given in Section 5. The conclusion of main results is presented in section 6.

2 DATA HIDING BY SIMPLE LSB SUBSTITUTION

LSB method is one of the most common and easiest steganographic techniques. The idea is to replace directly a number of bits of the least significant bits (LSB) of each pixel of the cover image with the embedded message. However, this method suffers from some problems as many steganograpic schemes. Noticeable distortion in the stego image will be produced by simple LSB substitution. This means that the stego image quality may be not acceptable and probably attracts unauthorized attention. To understand the LSB substitution method, suppose we have the following pixels in the image: P_1 = [10011011], P_2 = [01101010], P_3= [11001100], and the secret bits are $M = [011]$, and the resulted pixels after embedding the secret bits are P_1 = [10011010], P_2 = [01101011], P_3= [11001101]. So the LSB method has the following conditions [4]:

- –Since LSB becomes vulnerable to security attacks due to its simplicity.
- –Increasing the amount of secret data in each pixel implies to more visual degradation in the quality of the image.
- –Due to the uniform distribution of the secret message, the image histogram becomes noticeable.

3 The Optimal LSBs Technique

The simple of LSBs method has been improved by many authors. One of the improved methods called the optimal LSBs method. It improves the image quality of the stego-image by applying an optimal pixel adjustment process. Three candidates are selected from the pixels and matched to obtain the closest one to the original pixel value with the secret data [12]. The optimal pixel is the best candidate and is used to hide the secret data. The following steps describe the embedding algorithm:

- –Suppose P_i is the corresponding pixel values of the $i-th$ pixel in the cover-image C, and k bit(s) of embedded message.
- –Use the LSBs method to embed k bit(s) into P_i. Then the stego-image P_i' can then be obtained.
- –By adjusting the $(k+1)$ th bit of P_i' another two pixel values P_+' and P_-' will be generated as follows:

$$(P_+', P_-') = \begin{cases} p_+^{'} = p_i^{'} + 2^k \\ p_-^{'} = p_i - 2^k. \end{cases} \quad (1)$$

The last k bits of P_+' and P_-' are the same, so the hidden data in P_+' and P_-' are identical to P_i'.
- –The best candidate (closest on) to the original pixel value $P"_i$ can be found by the following formula:

$$p_i^{"} = \begin{cases} p_i^{'} & \textbf{if} \quad | p_i - p_i' | \leq | p_i - p_|' - \leq | p_i - p_+' | \\ p_+^{'} & \textbf{if} \quad | p_i - p_+' | \leq | p_i - p_i' | \leq | p_i - p_-' | \\ p_-^{'} & \textbf{if} \quad | p_i - p_-' | \leq | p_i - p_-' | \leq | p_i - p_+' | \end{cases} \quad (2)$$

The embedding algorithm comes to its end by replacing the optimal candidates $P_i^{"}$ by the original pixel values$P_i^{"}$. To explain that the distortion in the simple form of LSBs technique can be decreased by the optimal LSBs method, we present the following example: Suppose $P_i = 9$, $k = 3$, and the three bits of embedded message are 110. Then, by using the simple 3-LSBs method, the stego-image $P_i' = 14$ is obtained. After adjusting the 4-th bit of P_i', another two pixel values $P_+' = 22$ and $P_-' = 6$ can be obtained. The pixel values of last three bits $P_i' = 14$, $P_+' = 22$ and $P_-' = 6$ are the same. However, the optimal candidate is $P_-' = 6$ because it is the most closest one to the original pixel value $P_i = 9$. This example observes that the quality of the stego-image can be significantly improved by using the optimal LSBs method.

4 THE PROPOSED METHOD

In this section, the presented method will be introduced in detail. These methods as mentioned before based on the LSB substitution with inverting the value of some bits have the secret bits. The image is divided into two parts, one for embedding the secret message and applies change to the value of some bits that have the secret bits obtained by the simple form of LSB substitution technique. The other part is used to indicate which change is applied to each pixel exist in the first part. The advantages of the presented method are increasing the amount of secret message in each pixel in the cover image and improving the quality of the stego image. It consists of two phases, the embedding one and the extracting phase.

Let $I = p_1, p_2, \cdots, p_N$ be the original 8-bit grayscale cover-image which consists of set of pixels:

$$| p_i | = 8bits, p_i = (b_1, b_2, \cdots, b_8), b_j \in 0, 1 \tag{3}$$

The size of the image is computed as:

$$N = H \times W \tag{4}$$

Where H, W is the image height and width respectively. Assume M be the secret data bits, with length n,

$$M = m_1, m_2, \cdots, m_n \quad where \quad m_i \in 0, 1 \tag{5}$$

The maximum hiding capacity h in the image I in terms of bits is:

$$1 \leqslant h \leqslant (N \times 8) \tag{6}$$

4.1 The Embedding Procedure:

We assume that the pixels in the cover image consists of 256 gray values. The cover image is divided into two parts according to the size of the embedded data as shown in table 1. The first part is used to embed the secret message and make changes on it. The second part is used to refer to the change that has occurred.

- At start, the number of bits of the secret message will be embedded to each pixel P_i with gray value y_i in the cover image I is fixed to all the pixels.
- Divide the secret message into blocks of size k.
- In the first part, replace directly each block into the k LSB of y_i, and this produced y_i'
- In this step, one of two changes will be applied to the value of some bits of y_i'
  - Invert the value of the $(k-1)-th$ bit of the k LSB of y_i'.
  - Invert the values of the $(k-1, k)-th$ bits of the k LSB of y_i'.
- Apply the optimal LSBs method to each $y"_i$ obtained in step 3.
- Now, we have two pixel values.
- Choose the value closest to the original value y_i and replace them together. Then return 0 or 1 as indicator to show which change is selected.
- in the second part, we start from end. Note that, each bit of o LSB of each pixel in this part represents the change which applied to one pixel in the first part. Embedding the indicator in the o LSB of pixels. Then apply the optimal LSBs method to each pixel.
- Repeat the previous steps until embedding the entire secret message.
- After embedding all, the stego image I' is produced, then extract the secret data and send it to the other side.

4.2 The extracting algorithm

To recover the original secret data, the original image I must be known to determine which change is applied. The main sequences must be followed at the receiving end:

- Starting from the end of the stego image I', comparing o LSB of every pixel of it with o LSB of the corresponding pixel in original image I.
- If there is Similarity between bits, then the (k-1)-th bit is inverted. If no, then the (k-1, k) th bits are inverted.
- After determining which changing is occurred, invert the value of this bits in the first part to obtain the secret bits.
- obtain the k-bit secret message from the k-bit LSB of the stego-image.
- then, the algorithm of retrieving is finishing and the secret data is retrieved completely.

5 EXPERIMENTAL RESULTS

To evaluate our proposed scheme, Six experiments are performed. The standard grayscale images of Lena, Baboon, ”Pepper ”, ”Barbara” , ”Elaine” and ”Cameraman ” with size 512 x 512 and 128 x 128 of each are used in the experiments as cover images as shown in Figure. 3. The secret bit streams as series of pseudo random binary numbers are embedded into the cover images.

Figure 3. Six cover images with size 512 x 512: (a) Lena (b) Baboon (c) Peppers (d) Barbara (e) Elaine (f) Cameraman.

The performance is measured from two points of view, the data size and the quality of visual of the stego image.

The evaluation of the quality of stego image is evaluated by using the peak signal-to-noise ratio (PSNR), the most popular measurements of steganography performance. PSNR is expressed in terms of a logarithmic decibel scale. The PSNR value is defined as follows:

$$PSNR = 10 \cdot \log_{10} \frac{255^2}{MSE} (dB) \tag{7}$$

Fig3. a. Lena

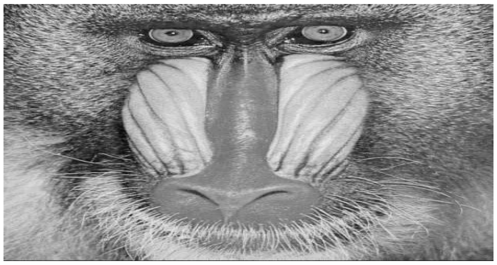

Fig3. b. Baboon

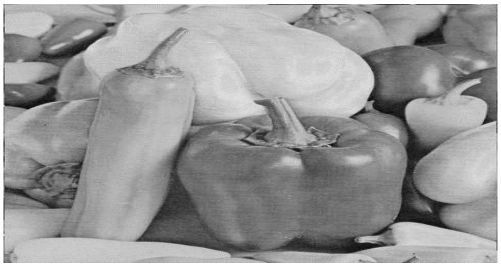

Fig3. c. Peppers

Fig3. d. Barbara

Fig3. e. Elaine

Fig3. f. Cameraman

Fig. 3: Six cover images with size 512 x 512

MSE is the mean square error between the cover and stego images. For a cover image with height H and width W, MSE is defined as:

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (I_{ij} - I'_{ij})^2 \qquad (8)$$

Where I_{ij} and $I_{ij'}$ are the pixel values of the cover and stego images, respectively.

Note that, the stego image is most similar to the original image, when the *PSNR* value is large and vice versa. Generally, if the PSNR value is larger than 30 dB, then this will be difficult to detect the distortion on the stego image by human eyes [4]. The experimental results show that the presented method can embed a large amount of data with an acceptable visual quality.

Another performance measurement is the data payload (capacity). Data payload is the amount of data can be hidden within the cover media, which can expressed as number of bits, which shows the max message size can inserted into an image [13].

$$Capacity = \frac{\textbf{Total number of bits embedded into image}}{\textbf{Total number of pixels}} \textbf{(bits/pixels)} \qquad (9)$$

Usually, the MSE will increase, when the payload increases, and PSNR will be affected inversely. So, a trade-off should be done between capacity requirements and PSNR [13]. Thus, our method presented to improve the capacity and the image quality.

Table 1 shows the results of the presented method in terms of embedding capacity (in bits) and PSNR value. We used images of size 512×512. In this table k, o refers to the number of LSB in the cover image pixels in the first and two parts respectively and C is the capacity of secrete data, $C_1 = 349524$, $C_2 = 524286$, $C_3 = 589824$, $C_4 = 699048$, $C_5 = 786432$, $C_6 = 838860$, $C_7 = 873810$, $C_8 = 983040$, $C_9 = 1048575$, $C_1 0 = 1092265$.

Table 3 shows the comparisons between X. Liao et al. [1] which used the optima LSBs method in his embedding algorithm and our results in terms of embedding capacity and PSNR value. The statistics show that the presented steganographic method is better than X. Liao et al.s approach.

Table 1: Experimental Results

CIs	P	P	P	P	P	P	P	P	P	P
	K=2	K=3	K=3	K=4	K=4	K=4	K=5	K=5	K=5	K=5
	o=2	o=2	o=3	o=2	o=3	o=4	o=2	o=3	o=4	o=5
	$C=C_1$	$C=C_2$	$C=C_3$	$C=C_4$	$C=C_5$	$C=C_6$	$C=C_7$	$C=C_8$	$C=C_9$	$C=C_{10}$
Lena	49.88	46.57	44.43	41.97	40.78	38.84	36.42	35.71	34.84	33.10
Baboon	49.90	46.55	44.40	41.96	40.78	38.85	36.42	35.72	34.83	33.11
peppers	49.91	46.54	44.40	41.95	40.77	38.83	36.42	35.70	34.83	33.11
Barbara	49.90	46.55	44.42	41.96	40.77	38.84	36.40	35.69	34.82	33.07
Elaine	49.89	46.55	44.42	41.96	40.78	38.84	36.43	35.72	34.86	33.11
Cameraman	49.90	46.57	44.43	41.97	40.79	38.87	36.45	35.74	34.88	33.14

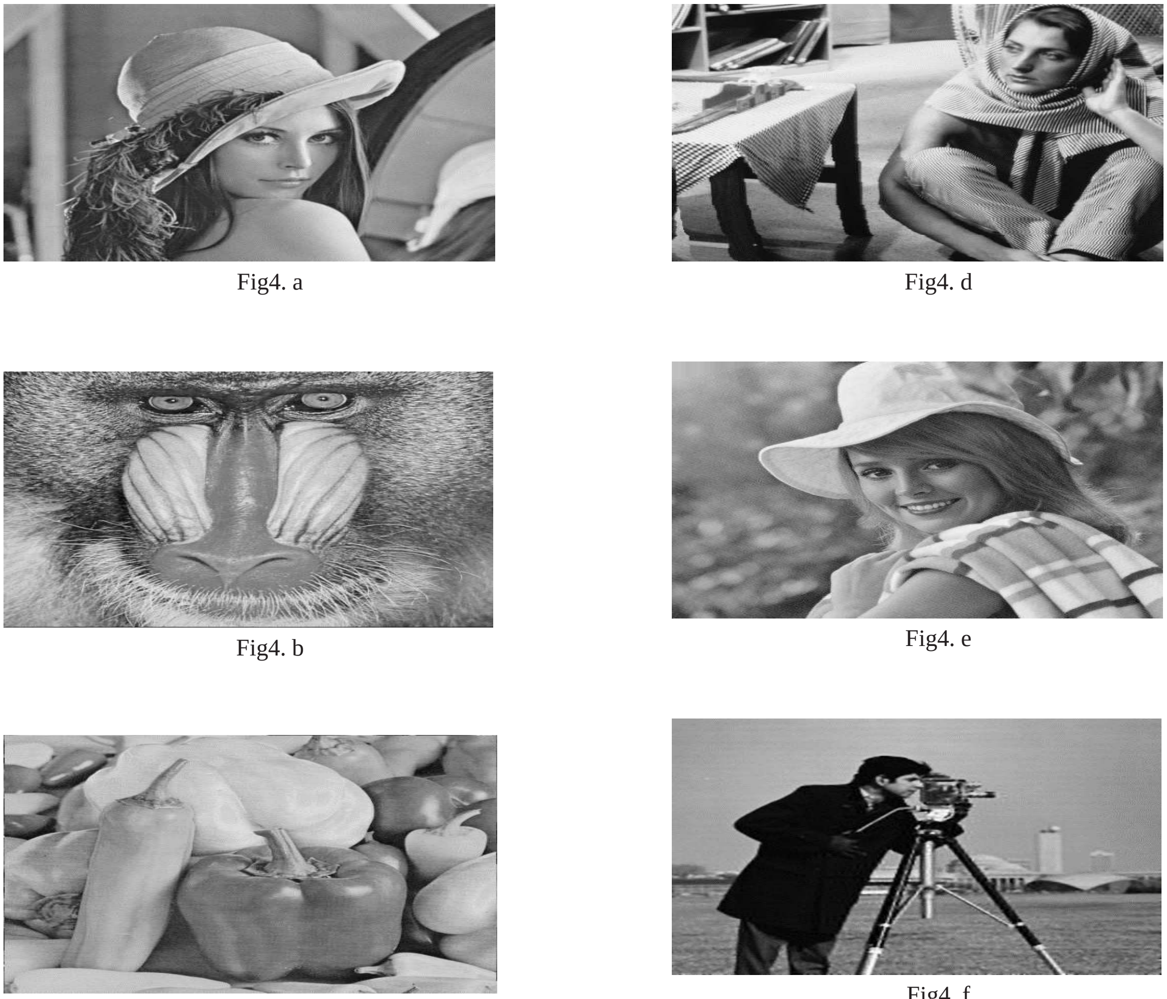

Fig4. a

Fig4. d

Fig4. b

Fig4. e

Fig4. c

Fig4. f

Fig. 4: Six stego images

Figs 4a to 4f show six stego images (4a) Lena (k =2, o=2, embedded 349524 bits PSNR = 49.88dB) (4b) Baboon(k =3, o=2, embedded 524286 bits, PSNR = 46.55dB) (4c) Peppers(k =3, o=3, embedded 589824 bits, PSNR = 44.40dB) (4d) Barbara (k =4, o=2, embedded 699048 bits, PSNR = 41.96dB) (4e) Elaine (k =4, o=3, embedded 786432 bits, PSNR = 40.78dB) and (4f) Cameraman(k =4, o=4, embedded 838860 bits, PSNR = 38.87dB).

The performance of a steganographic technique is favored if it can provide higher PSNR values when concealing with the same size of embedding data. Thus, Table2 shows the comparisons of our results with the result in [12], in terms of PSNR and the same embedding payload. It is clear that the proposed scheme provides better image quality and can embed large size of data.

Table 2: The same embedding capacity with better stego-image quality.

CIs	**C(OL)**	**P(OL)**	**C(OM)**	**P(OM)**
Lena	349524	48.13	349524	49.88
Baboon	786432	40.72	786432	40.78
Peppers	838860	35.79	838860	38.83
Barbara	873810	35.62	873810	36.4
Elaine	1048575	34.82	1048575	34.86
Cameraman	1092265	29.73	1092265	33.14

Table 3: Comparisons of the results between X. Liao et al.'s [12] and the proposed method

CIs	**C(XT**	**P(XT)**	**C(OM)**	**P(OM)**
Lena	579204	39.12	589824	44.43
Baboon	825172	32.57	838860	38.85
Peppers	568828	39.84	589824	44.40
Elaine	585144	38.51	589824	44.42
Barbara	741468	33.93	786432	40.77

Table 4: Comparison of the our method with Marghny et al. [10] method

CIs	**AC(M)**	**AP(MT)**	**AC(OM)**	**AP(OM)**
Baboon	1.56	41.74	2	46.54
Lena	1.47	41.10	2	46.59
Pepper	1.45	41.40	2	46.59
Cameraman	1.54	39.00	2	46.55

Images with size 128 × 128 are used to compare the proposed method with Marghny et al. [10] in terms of embedding capacity and PSNR value. The results are listed in Table 4.

Where *CIs* means Cover Images, *OL* means Optimal LSBs [12], *OM* means Our Method, *X* means X. Liao's Techniques. [1], *MT* means Marghny's Techniques [**?**], *C* means capacity, *P* means PSNR, *AC* means Average Capacity and *AP* means Average PSNR in the tables above.

6 Conclusion

Steganography, a branch of data hiding technology, aims to protect important data in transmission. Capacity and stego-image quality are important for a good steganographic approach. There is a trade-off between the amount of secret data that can be embedded, the image distortion, and the security of the stego-image. In this paper, an improvement data hiding method by simple LSB substitution with an optimal LSBs method is proposed. The experimental results show that the proposed method provides larger embedding capacity and better image quality.

The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

[1] X. Liao, Q. Wen and J. Zhang, ”A steganographic method for digital images with four-pixel differencing and modified LSB substitution”, Journal of Visual Communication and Image Representation, vol 22, no 1, pp. 18, 2011.

[2] M. H. Marghny, S. E. El-Gendi, F. Al-Afari and M. El-Melegy, ”Steganography for Secure Data Communication”, Msc Thesis, Faculty of Science, Assiut University, pp. 120, 2009.

[3] E. Lin and E. Delp, ”A Review of Data Hiding in Digital Images”, in Conference on Image Processing, Image Quality, and Image Capture Systems, PICS, pp. 274-278, 1999.

[4] M. H. Marghny, N. M. AL-Aidroos and M. A. Bamatraf, ”Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference”, International Journal in Foundations of Computer Science & Technology, vol. 2, no. 6, pp. 1-13, 2012.

[5] S. Katzenbeisser and F.A.P. Petitcolas, ”Information Hiding Techniques for Steganography and Digital Watermarking”, Artech house, Inc, 2000.

[6] M. H. Marghny, F. Al-Afari and M. A. Bamatraf, ”Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation”, International Arab Journal of e-Technology, Vol.2, No.1, 2011.

[7] M. Al-Husainy, ”A New Image Steganography Based on Decimal-Digits Representation, Computer and Information Science”, vol. 4, no. 6, pp. 38-47, 2011.

[8] R.-Z. Wang, C.-F. Lin and J.-C. Lin, ”Hiding data in images by optimal moderately significant-bit replacement”, IEE Electron. Lett , vol.36, no. 25, pp. 2069070, 2000.

[9] R.-Z. Wang, C.-F. Lin and J.-C. Lin, ”Image hiding by optimal LSB substitution and genetic algorithm”, Pattern Recognition, vol. 34, no. 3, pp. 671683, 2001.

[10] N. M. AL- Aidroos, M. H. Marghny, and M. A. Bamatraf, ”Data Hiding Technique Based on Dynamic LSB”, Naif Arab University for Security Sciences.

[11] C. -K. Chan and L.M. Cheng, ”Hiding data in images by simple LSB substitution”, Pattern Recognition, vol. 37, no. 3, pp. 469474, 2004.

[12] N. Wu and M. Hwang, ”Data Hiding: Current Status and Key Issues” International Journal of Network Security, vol. 4, no.1, pp.1-9, 2007.

[13] A. Al-Ataby and F. Al-Naima A Modified High Capacity Image Steganography Technique Based on Wavelet Transform, The International Arab Journal of Information Technology, vol. 7, no. 4, pp. 358-364, 2010.

[14] M. H. Marghny, N. M. AL-Aidroos, and M. A. Bamatraf ”A Combined Image Steganography Technique Based on Edge Concept & Dynamic LSB.” International Journal of Engineering Research and Technology, Vol.1, No. 8, ESRSA Publications, 2012.

Marghny H. Mohamed received his Ph.D. degree in computer science from the University of Kyushu, Japan, in 2001, his M.Sc. and B.Sc. from Asyut university, Asyut, Egypt, in 1993 and 1988, respectively. He is currently a Professor in the Department of Computer Science, and for Vice Dean for Student affairs of Faculty of Computers and Information Systems, University of Asyut, Egypt. His research interests include data mining, text mining, information retrieval, web mining, machine learning, pattern recognition, neural networks, evolutionary computation, fuzzy systems, and information security. Dr. Marghny is a member of the Egyptian mathematical society and egyptian syndicate of scientific professions.

Loay M. Mohamed received her Bachelor Science degree in computer science in 2006 at Assiut University, Faculty of Science, Dept. of Mathematics, Egypt and she is preparing the finale phase of her Master’s degree in Steganography, Her research activities are currently focused on the information security.