ICIT 2015 The 7th International Conference on Information Technology
doi:10.15849/icit.2015.0048

Hide Image in Image Based on LSB Replacement and Arnold Transform

Dr. Sadik Ali Al-Taweel
Information Systems Department
University science and Technology
Sana'a, Yemen
Dr.sadiq@ust.edu

Mohammed. Al-Hada, Ahmed. M. A. Naser, and Mohammed Al-Thamary
Information Technology Deparment
University science and Technology
Sana'a, Yemen
alhada.eng@gmail.com

***Abstract*— For quite a long time, computer security was a rather narrow field of study that was populated mainly by theoretical computer scientists, electrical engineers, and applied mathematicians. Data hiding techniques have taken important role with the rapid growth of intensive transfer of multimedia content and secret communications. There are many techniques used for data hiding and the well-known technique is the Steganography. Steganography is the art of hiding information in ways that prevent detection. For hiding secret information in images, there exists a large variety of Steganography techniques, some are more complex than others and all of them have respective strong and weak points. In this paper deals with encrypt and hide image in another gray image file using Least Significant Bit (LSB) based Steganography and Arnold's transformation algorithm based Cryptography. Experimental results show that the algorithm has good security and imperceptibility in grayscale images.**

***Keywords*— Image processing, Steganography, information hiding, Arnold Transform**

I. INTRODUCTION

Based on [1] stated that "Security through obscurity says that if you hide the inner workings of your system you will be secure. This philosophy does not work when it comes to security, and it does not work when it comes to cryptography". Most of the requirements of secret communication, sometimes in combination with other techniques, such as cryptography, as cryptography and Steganography complement each other. It is recommended to use these two techniques together for a higher level of security.

Information security is the protection of information and the systems and hardware that use, store, and transmit that information. Information security can be defined as measures adopted to prevent the unauthorized use or modification of use of data or capabilities [2].

Image scrambling refers to some kind of transform, which makes the spatial location of the pixel becomes chaos and lost their original features and meaning. But the total number of pixels and histogram has not unchanged so as to achieve the purpose of encryption. As well as the scrambling must be one kind reversible transform, otherwise it will not have any significance in the practical application. If you do not know the rules and keys of the transform, it is impossible to recover the original image. And in the process of scrambling, the loss of the hidden information is dispersed into the whole hidden data. Thereby it minimizes the loss of meaningful information in order to reach purpose of improving robustness. Therefore image scrambling technology has been widely applied in the image Steganography field [3].

Arnold transform is a type of image scrambling methods. The transformation shifts pixel position from (x, y) to (x', y') without changing its gray value. It is cyclic the secret image repeats itself after certain number of iteration.

II. RELATED WORK

M. Mahdavi, et.al [4] proposed a new accurate steganalysis method for the LSB replacement Steganography. The suggested method is based on the changes that occur in the histogram of an image after the embedding of data. Every pair of neighboring bins of a histogram are either inter-related or unrelated depending on whether embedding of a bit of data in the image could affect both bins or not.

Chang, C.C et al [5] proposed an image Steganography technique which offer high embedding capacity and bring less distortion to the stego image. The embedding process embed bits of secret bit stream on the stego image pixels. Instead of replacing the LSB of every pixel, this method replaces the pixel

doi:10.15849/icit.2015.0048

intensity with similar value. The range of modifiable pixel value is higher in edge areas than smooth areas to maintain good perceptual excellence. This method is falling of boundary problem which means the pixel which is located for embedding will become unused; since it exceeds the maximum intensity level which is greater than 255 (maximum gray scale intensity).

Wu. H.C et al [6] suggested to improve the capacity of the hidden secret data and to provide an imperceptible Stego-image quality. This method based on least significant bit (LSB) replacement and pixel-value differencing (PVD) method is presented in this paper. The limitation of this method is Low-hiding capacity owes to mainly hiding in smooth areas. For example if pixel value difference is 3 if the corresponding range width is 8, only 3 bits can be embedded in a pair of pixels.

Y. K. Jain et al [7] proposed an adaptive least significant bit spatial domain embedding method. The proposed method divides the image pixels ranges (0-255) and generates a stego-key. This private stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of this method is its integrity of secret hidden information in stego-image and high hidden capacity. This method could be weak for the hide extra bits of signature with hidden message for its integrity purpose. This study also proposed a method for color image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

According to Yang et al., in [8], an adaptive LSB substitution based data hiding method for image is proposed, to achieve better visual quality of stego-image. It takes care of noise sensitive area for embedding. Proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the edges, brightness and texture masking of the cover image to calculate the number of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over sensitive image area (k) value remain small to balance overall visual quality of image. The LSB's (k) for embedding is computed by the high-order bits of the image. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. The overall result shows a good high hidden capacity, but dataset for experimental results are limited, there is not a single image which has many edges with noise region like 'Baboon.tif'.

C.-H. Yang et al [9] proposed a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be estimated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. This method generally provides a good imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. The proposed method hides large and adaptive k-LSB substitution at edge area of image and PVD for smooth region of image. So in this way the technique provide both larger capacity and high visual quality according to experimental results. However, their algorithm is complex due to adaptive (k) generation for substitution of LSB.

K.-H. Jung er al [10] proposed a method of Multi-Pixel Differencing (MPD) which used more than two pixels to estimate smoothness of each pixel for data embedding and it calculate sum of difference value of four pixels block. For small difference value it uses the LSB otherwise for high difference value it uses MPD method for data embedding. In this method the experimental dataset is too limited.

In [11] authors proposed another pixel value differencing method, it used the three pixels for data embedding near the target pixel. Also it uses simple k-bit LSB method for secret data embedding where number of k-bit is estimated by near three pixels with high difference value. To retain better visual quality and high capacity it simply uses optimal pixel adjustment method on target pixels. In this method the histogram of stego-image and cover-image is almost same, but dataset for experiments are too small.

W. J. Chen et al[12] introduced a high capacity of hidden data utilizing the LSB and hybrid edge detection scheme. For edge computation two types of canny and fuzzy edges detection method applied and simple LSB substitution is used to embed the hidden data. This scheme is successful to embed data with higher peak signal to noise ratio (PSNR) with normal LSB based embedding. This method is tested on limited images dataset.

Madhu et al., in [13] proposed an image steganography method, based on LSB substitution and selection of random pixel of required image area. Also it is target to improve the security where password is added by LSB of pixels. It generates the random numbers and selects the region of interest where secret message has to be hidden. The limitation of this method it is not considers any type of perceptual transparency.

III. PROPOSED ALGORITHM

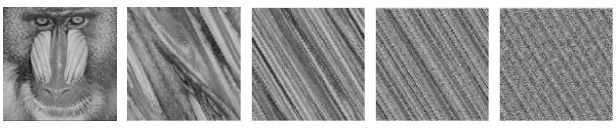
In this section the methodology of proposed method is given as following:

a. Arnold Transform and LSB Algorithms

Before embedding, the secret message is implemented for block transformation using the Arnold image transformation. The Arnold image transformation is defined as the point (x, y) in the unit square transforms into the other point (x', y') [14]:

$$\begin{bmatrix} \acute{x} \\ \acute{y} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\ \ N) \qquad (1)$$

Where, (x' , y') {0,1,2,3...N-1} are pixel coordinates of the secret image, (x,y) is the transformed position of (x', y') and N is the order number of image matrix. Suppose the secret image has iterated for K iterations we got the "chaotic" secret image, so K can be saved as a key1. Figure1 show an example of Arnold transform with four iterations.



doi:10.15849/icit.2015.0048

Fig.1. Example of Arnold Transform. The first image is the secret image, which has been encrypted with four iterations separately as shown.

After the encryption step the secret will hide in cover image by using Least Significant Bit (LSB) Replacement. This is the simplest of the steganography methods based in the use of LSB, and therefore the most vulnerable. The embedding process consists of the sequential replacement of each Least Significant Bit (LSB-1-2) of the image pixel for the bit-stream of secret image by bit-or function. The extracting process also consists of sequential extracting for bit-stream of secret image by concatenation method. For its simplicity, this method can camouflage a great volume of information. Figure 2 show the diagram of the proposed method and the following algorithm steps illustrate how the proposed method works.

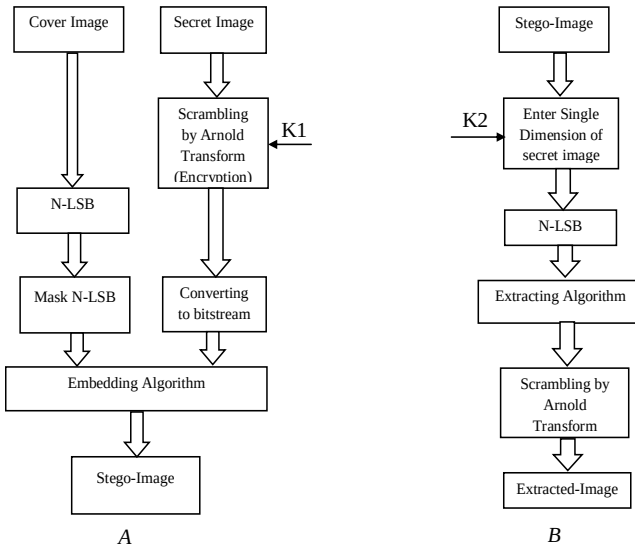


Fig.2. Block Diagram of Proposed Method: (A) Embedding Algorithm, (B) Extracting Algorithm.

In this figure, we have two keys K1 is a key of Arnold transform algorithm which will be the number of iterations. Moreover, K2 is a key of proposed LSB algorithm, when you want to extract the secret image you must enter single dimension of the secret image. By this number of dimension you can extract the right secret image. So, it will be another key and saved as K2.

b. Encryption and Embedding Algorithm

1. Read Cover image and Secret image.
2. Enter the number of iterations for encrypt the secret image (K1).
3. Apply Image scrambling Algorithm using Arnold Transform Method.
4. Enter the N bit plane that will be hide in.
5. Mask N-LSB of image pixel in cover.
6. Convert Secret image to bit stream.
7. If size of bits of secret image bigger than total size of bit space insert-able show error message and read another secret image else continue.
8. Hide first N bit of bit stream in Masked Last N of covered image.
9. Repeat step 6 until all the bits of bit stream embedded.
10. Then create stego image.

c. Decryption and Extracting Algorithm

1. Read Stego image.
2. Enter the single dimension of the secret image (K2).
3. Enter the N-LSB which is hidden in.
4. Find the Length of embedded bitstream.
5. Create a new bit stream.
6. Convert Stego image from decimal to binary.
7. Concatenate the new bit stream and Last N bit of binary Stego image.
8. Convert the new bitstream to array.
9. Then retrieval scrambled image.
10. Enter the number of iterations for decrypt the secret image (K1).
11. Apply Image scrambling Algorithm using Arnold Transform Method.
12. Finally, recuperation the secret image.

IV. RESULT AND DISCUSSION

In Steganography, technique Peak Signal-to-Noise Ratio (PSNR), Normalized Correlation (NC) are standard measures used in order to test the quality of the stego images. PSNR used to evaluate the imperceptibility of the Stego-image, the maximum value is (100) and the minimum value is (0), whenever the bigger the better. It can be found in equation (2). MSE is the Mean Square Error. For imperceptible hiding, the stego-image should look as similar as the cover-image, whenever was the youngest, the better. It can be found in equation (3). In this section, some experiments are performed to demonstrate the efficiency of the proposed method without and with attack. Before the embedding process, the secret image was firstly encrypted using Arnold transform algorithm. Three of 8-bit grayscale images of size 512*512 used as cover and shown in Figure 3.

$$MSE = \frac{1}{MxN} \sum_{i=0}^{M} \sum_{j=0}^{N} (I_B(i,j) - I_H(i,j))^2 \quad (2)$$

$$PSNR = 10\, x\, log_{10}(\frac{255^2}{MSE})\ (db) \quad (3)$$

(A) (B) (C)
Fig. 3. Cover Images: (A) Baboon (B) Lena (C) Airplane

a. Results without Attack

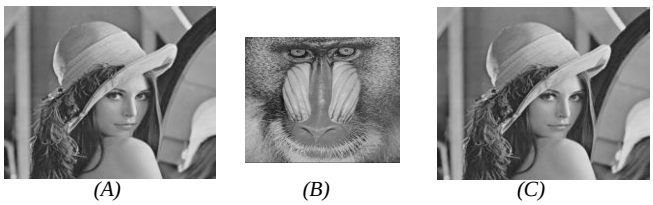
In this section, the proposed method has been tested in three experiments without attack by taking three standard

doi:10.15849/icit.2015.0048

512*512 gray scale images (Baboon, Lena and Airplane) as cover and three secret images with different lengths. Figure 4 used "Baboon.bmp" as a Cover image and "Flower.bmp" as Secret image with size (128*128). And Figure 5 used "Lena.bmp" as Cover and "Baboon.bmp" as Secret image with size (192*192). Also Figure 6 used "Airplane.bmp" as cover image and "Lena.bmp" as Secret image with size (256*256).

(A) (B) (C)

Fig.4. First Embedding Experiment: (A) Cover image, (B) Secret Image, (C) Stego-Image



(A) (B) (C)

Fig 5. Second Embedding Experiment: (A) Cover image, (B) Secret Image, (C) Stego-Image.

(A) (B) (C)

Fig.6. Third Embedding Experiment: (A) Cover image, (B) Secret Image, (C) Stego-Image.

b. -PSNR

The results that are obtained from these experiments are recorded and compared them with another method in [44]. It can be summarized in the following table:

TABLE1. COMPARATIVE PERFORMANCE OF MSE, PSNR WITHOUT ATTACK.

Methods	***Cover Image (512*512)***	***Number of Hidden Bits***	***PSNR***
LSB SM	Lena	164538	38.56
	Baboon	298413	48.18
Proposed Method	Lena	294912	43.60
	Baboon	131072	51.13
	Airplane	524288	44.29

As shown in the table the proposed method has been compared with another method, which labeled (LSB SM) with different capacity for the embedding. Proposed Method has three experiments, while another method has two experiments. Here PSNR used for indicate the preference. The following histogram will shows the different rate of the two methods.

- *Histogram of PSNR*

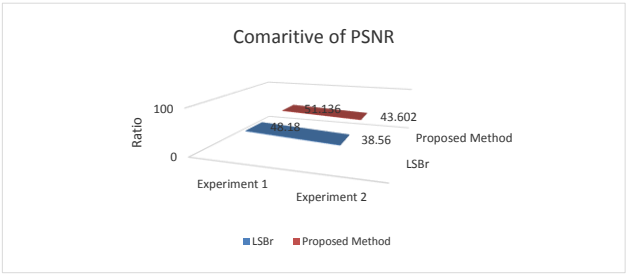
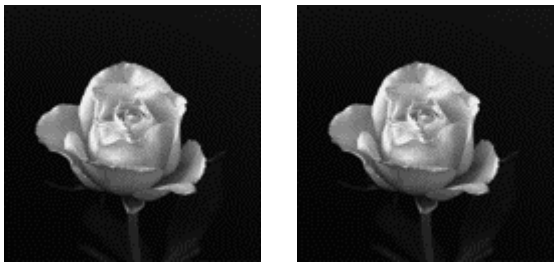


Fig .7. Comparative of PSNR

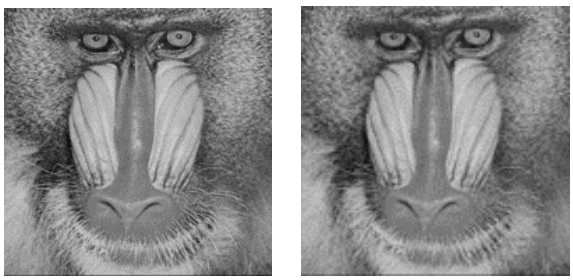
c. NC

The results of NC that obtained from secret images shown in Figures 8, 9 and10 below and recorded in the next table:



(A) (B)

*Fig .8. First NC without Attack: (A) Secret Image (128*128), (B) Extracted Image (128*128).*



(A) (B)

*Figure (9): Second NC without Attack: (A) Secret Image (192*192), (B) Extracted Image (192*192).*

(A) (B)

*Fig.10. Third NC without Attack: (A) Secret Image (256*256), (B) Extracted Image (256*256).*

doi:10.15849/icit.2015.0048

TABLE2.RESULT OF NC WITHOUT ATTACK

Secret Image	Extracted Image	NC
Flower (128*128)	Flower (128*128)	1
Baboon (192*192)	Baboon (192*192)	1
Lena (256*256)	Lena (256*256)	1

The table shows the results that are similar NC values which obtained from the different experiments cover-images in Figures 8, 9 and 10, which graphed in the following histogram.

- *Histogram of NC*

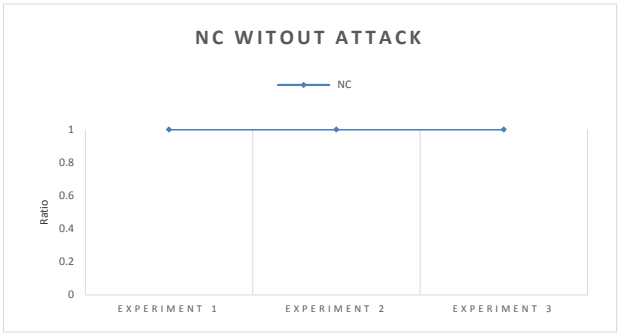


Fig.11. Histogram of NC without Attack.

V. CONCLUSION

The proposed method described in this paper helps to successfully hide the secret image into the cover image, with minimum distortion made to the cover image. First the secret image has been scrambled using Arnold algorithm and embedded to the cover image by using LSB algorithm. This method is essential for construction of accurate targeted and blind Steganalysis methods for BMP images. With using Arnold transform the proposed method will be more secure. The main features of the proposed method are imperceptibility and security. The limitations of the proposed method is slow with extracting algorithm when using large size image Higher than 160*160. Also can not used images which have different dimensions, only can use square array of image which have the same dimensions.

REFERENCES

[1] Cole, E. “Hiding in Plain Sight: Steganography and the Art of Covert Communication”, Indiana, John Wiley & Sons Inc, (2003)

[2] Whitman, M.E. & Mattord, H.J., "Principles of information security". Thomson course technology, 2007.

[3] Yinglan Fang, Lin Tian "An Improved Blind Watermarking Algorithm for Image Based on DWT Domain", Journal of Theoretical and Applied Information Technology, 15th November 2012. Vol. 45 No.1.

[4] M. Mahdavi*, Sh. Samavi*, N. Zaker** and M. Modarres-Hashemi*, "Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram", Iranian Journal of Electrical & Electronic Engineering, Vol. 4, No. 3, July 2008.

[5] Chang, C.C., Tseng, H.W.: "A Steganographic method for digital images using side match", Pattern Recognition Letters 25, 1431–1437 (2004).

[6] Wu. H.C, Wu, N.I., Tsai, C.S., Hwang, M.S. "An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods", IEEE Proceedings of visual image signal Process, November 7, 2004.

[7] Y. K. Jain and R. R. Ahirwal, “A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys”, International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

[8] H. Yang, X. Sun and G. Sun, “A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution”, Journal: Radioengineering, vol. 18, no. 4, (2009), pp. 509-516.

[9] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, “Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems”, IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[10] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, “Image data hiding method based on multi-pixel differencing and LSB substitution methods”, Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), (2008) August 28-30, pp. 355-358.

[11] H. Zhang, G. Geng and C. Xiong, “Image Steganography Using Pixel-Value Differencing”, Electronic Commerce and Security, ISECS '09. Second International Symposium on (2009) May.

[12] W. J. Chen, C. C. Chang and T. H. N. Le, “High Payload Steganography Mechanism Using Hybrid Edge Detector”, Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, (2010) April 4.

[13] V. Madhu Viswanatham and J. Manikonda, “A Novel Technique for Embedding Data in Spatial Domain”, International Journal on Computer Science and Engineering, IJCSE, vol. 2, (2010).

[14] Compressed image file formats: JPEG, PNG, GIF, XBM, BMP / by John Miano, First printing, July (1999), Copyright© 1999 by the ACM Press.