Yossra H. Ali
University of Technology Department of Computer Sciences Baghdad, Iraq
yossra_1@yahoo.com

Hussein J. Mankhi
University of Technology Department of Computer Sciences Baghdad, Iraq
hussin_jaeiz@yahoo.com

Received on: 18/4/2016
Accepted on: 8/6/2017

Text File Hiding Randomly Using Secret Sharing Scheme

Abstract- *Exchange of information through the channels of communication can be unsafe. Communication media are not safe to send sensitive information so it is necessary to provide the protection of information from disclosure to unauthorized persons. This research presented the method to information security is done through information hiding into the cover image using a least significant bit (LSB) technique, where a text file is encrypted using a secret sharing scheme. Then, generating positions to hiding information in a random manner of cover image, which is difficult to predict hiding in the image-by-image analysis or statistical analyzes. Where it provides two levels of information security through encryption of a text file using the secret sharing and the generating random positions of hiding. This method has been in hiding a text file and recovered without loss of information, as well as not noticing any deformation of the image. Where it was hiding a text file size of 20 KB in image cover (250x250) pixels, the result of MSE is 0.696 and PSNR is 49.211.*

Keywords- *Information Hiding, LSB, PSNR, Secret Sharing.*

How to cite this article: Y.H. Ali and H. J. Mankhi "Text File Hiding Randomly Using Secret Sharing Scheme," *Engineering and Technology Journal*, Vol. 36, Part B, No. 1, pp. 1-6, 2018.

1. Introduction

In recent year, steganography is consider as a promising way of safe electronic communication. Steganography is the science of hiding information such its presence cannot be detect and a communication is happening. The word steganography comes from the Greek words Steganos (covered) and graphic (writing) and literally means covered writing. Using steganography, information is embedding in a medium such as image, audio, video or text file called *carrier* in a way that it is not detectable by others [1]. A number of ways exist to hide information in digital images divided into two types: Spatial Domain and Frequency Domain. Spatial domain techniques embed messages in the intensity of the pixels directly. Least Significant Bit (LSB) is the first most widely used spatial domain steganography technique. In frequency domain, images are first transform and then the message is embedding in the image. The most common frequency domain method usually used in image processing is the 2D discrete cosine transforms [2].

This paper has proposed method using secret sharing scheme and random algorithm to choose positions hiding, where there 6 bits embedding in pixel of color image 2 bits embedded for each level. Method succeeded in hiding and retrieval of information without noticing any distortion in quality the image.

2. Related Work

In this section, we explain most studies about information hiding in spatial domain of image using least significant bit (LSB) technique.

Abdul Karim et al. [3] have proposed approach that the characters of the text embedded in pixels image a non-sequential, but will have a distance is not constant for hiding. It will be difficult to quest the place of bits of character in the pixels by image analysis or statistical analysis methods.

Ibrahim et al. [4] have proposed method to hide a text file in an image but before the hide compresses file. Different sizes of the data concealed in the cover image, distortion is not observe of stego image.

Brahma Teja et al. [5] have proposed method to hide data in the edge of the image by expansion LSB, where it was identified edges of the image using the canny edge detection method. This approach hide's data in the edge pixels applicable for all types of images.

Akhter [1] presented approach to hiding information in a digital image using Lucas number system. This approach increases of capacity embedding without a distortion in image quality and high PSNR value of stego image.

Lokhande et al. [6] proposed approach to combine between cryptography and steganography to provide the best security solution. First, the secret message encrypted using AES-128, then the encrypted message

https://doi.org/10.30684/etj.36.1B.1
2412-0758/University of Technology-Iraq, Baghdad, Iraq

embedding in an image using pseudo random numbers.

Preethi et al. [7] presented method a secret message encrypted by RSA algorithm and encrypted data embedding in random pixels of cover image. This method provides two levels of data protection against attacker**.**

3. Secret Sharing Scheme

In 1979, Shamir suggested that the principle of secret sharing scheme, where the secret $\boldsymbol{D}$ is divide into a number of pieces $\boldsymbol{n}$ each piece called *share* or *shadow* and then distributed to a number of participants. In the case of retrieval of the secret $\boldsymbol{D}$ requires just $\boldsymbol{t}$ or more participants to retrieve the secret image, where $\boldsymbol{t} \leq \boldsymbol{n}$. The scheme based on polynomial interpolation [8, 9]; the detail of this scheme defined as the following:

1- The secret $\boldsymbol{d}$ is an integer number, $\boldsymbol{n}$ is the number of participants (the number of shares), the threshold $\boldsymbol{k}$, where $\boldsymbol{k} \leq \boldsymbol{n}$.

2- Choosing a prime number $\boldsymbol{p}$, where $\boldsymbol{p} >$ max$(\boldsymbol{d}, \boldsymbol{n})$. All further calculations are in the range $\{0, \cdots, \boldsymbol{p}-\boldsymbol{1}\}$ denoted by $\boldsymbol{Z_p}$.

3- Defining$\boldsymbol{a_0} = \boldsymbol{d}$, and choosing$(\boldsymbol{t}-\boldsymbol{1})$ random number of the coefficients $\boldsymbol{a_1}, \cdots, \boldsymbol{a_{k-1}}$,$where\ \boldsymbol{0} \leq \boldsymbol{a_j} \leq \boldsymbol{p}-\boldsymbol{1}$.

4- Using $(\boldsymbol{t}-\boldsymbol{1})$ degree polynomial to compute the values of functionfrom the following equations:

$$f(\boldsymbol{x_i}), where\ \boldsymbol{i} = 1\ to\ \boldsymbol{n}, \boldsymbol{x} \in \boldsymbol{Z_p}$$

$$\boldsymbol{f(x_i)} = \sum_{\boldsymbol{j=0}}^{\boldsymbol{t-1}} \boldsymbol{a_j}\, \boldsymbol{x^j} \qquad (1)$$

Then computing $\boldsymbol{s_i} = f(\boldsymbol{x_i})\ mod\ p$,

where $\boldsymbol{i} = 1\ to\ \boldsymbol{n}$ (2)

5- Delivering $(\boldsymbol{x_i}, \boldsymbol{s_i})$ as a share to $\boldsymbol{n}$participants.

There are two methods to apply the secret-sharing scheme [10].

Lossy secret-sharing method: Allow the amputation of values to suit the conditions required in the secret sharing scheme (as is the case in the image gray values ranging from (0 to 255) while the nearest prime number to 255 is 251). This method can be used in the image without noticing any change or deformation of the image and cannot be used in the text

Lossless secret-sharing method: Do not allow the amputation of values to suit the conditions required in the secret sharing scheme. This method can be used in the text or image.

4. Cramer's Rule

Cramer's rule is a method for solving linear system. It makes use of determinants and so knowledge of these is necessary before proceeding [11].

Let the system of linear question as

$a_{11}\, x + a_{12}\, y = a_{13}$ (3)

$a_{21}\, x + a_{22}\, y = a_{23}$ (4)

The Equations (3) and (4) can put in the form:

$$\begin{pmatrix} a11 & a12 \\ a21 & a22 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a13 \\ a23 \end{pmatrix}$$

If D= $\begin{vmatrix} a11 & a12 \\ a21 & a22 \end{vmatrix} \neq 0$

Where D is Determinant, then the system has a unique solution, and Cramer's rule state that it may found from the formulas:

$$X = \frac{\begin{vmatrix} a13 & a12 \\ a23 & a22 \end{vmatrix}}{D}, \quad y = \frac{\begin{vmatrix} a11 & a13 \\ a21 & a23 \end{vmatrix}}{D}$$

5. Proposed Text File Hiding Method

The proposed method includes hiding the secret message (text file) in the cover image using a least significant bit (LSB) technique, Figure 1 shows block diagram that describes text file hiding method. There are several steps to implement the proposed method of hiding:

Step One: The proposed encryption of secret message uses secret sharing scheme by Lossless secret-sharing method, applies secret sharing scheme out of (2, 2) threshold in order not to expand a size of a message secret and reduce embedding cover image. It converts text to the hexadecimal system, then taking every value hex to apply lossless method before secret sharing scheme. Secret message encrypted using this method does not have a length equal to the length of the original secret message. This step determines the number of pixels required to hide secret message, algorithm (1) explains application of the lossless secret sharing method to secret message.

Figure 1: Block diagram for text file hiding method

Algorithm(1): Lossless Secret Sharing

***Input*:** Secret Message (Text file)

***Output*:** Encrypted text file, No. of pixels required for hiding

Start
Step1: Convert text to hexadecimal system
// Sequentially read values hex then store in T array
Step2: For each value hex Hi // Apply Lossless method
2.1. If Hi <12 then Store Hi to T
2.2. If Hi >=12 then Split Hi into two values (12, Hi -12) store to T
End for
// Apply secret sharing scheme out of (2,2) threshold using T array
and store the result in stega array
Step3: For i=1 to Length T array
Stega i = (Ti + Ti+1) mod 13 // nearest prime number to 15 is 13
Stega i+1 = (Ti + 2 * Ti+1) mod 13
i=i+2
End for
End

Step Two: The proposed algorithm of generating random positions of cover image pixels for hiding secret message encrypted uses LSB technique, where the number of required pixels is determined from the previous step. Random hiding in an image pixel gives more security and efficient of sequential hiding. Positions are generating to hide secret message in a random manner of cover image pixels, which is difficult to predict places for hiding in the image-by-image analysis or statistical analysis. Algorithm (2) describes method of generating random positions of cover image pixels.

Step Three: Finally, apply least significant bit (LSB) technique to cover image through taking bits lower in cover image pixel and substituting it with a secret encrypted message generated from the previous step, where 6 bits per pixel (Each red, green and blue color hides 2 bit) are hidden. Algorithm (3) describes work of LSB technique.

Algorithm (2) Generating random positions of cover image pixels

Input: Cover image, No. of pixels required , First position, Axis of x() array, Axis of y() array, X is Width of cover image; Y is Height of cover image, h=X, Flag = 0

Output: Array Random Points of Axis of y () and Axis of x ()

Start
Step1: Generate initialize point (R, C) by user
Step2: For i=1 to No. of pixels the required – 1
Flag = 0
R = Axis of y (i-1),
C = Axis of x (i-1)
2.1. R_{New}= (C * h) – (Axis of Y (i-1)) Mod X
C_{New}= (R* i) – (Axis of X (i-1)) Mod Y
2.2. If R_{New}, C_{New} is smaller than zero, then
$R_{New} = R_{New} + X$
$C_{New} = C_{New} + Y$
2.3. If R_{New} is not found in Axis of x or C_{New} is not found in Axis of y, then
Axis of x (i) = R_{New},
Axis of y (i) = C_{New}
Else
R=1
h=h-1
flag=flag+1
If flag>=2 then R = (X*Y) - Flag
Go to **2.1**
End If
End for
End

Algorithm (3): Least Significant Bit (LSB)
Input: Cover Image, Encrypted Secret Message, Array random points of cover image
Output: Stego Image
Start: ***Step1:*** Convert encrypted secret message to binary ***Step2:*** Read array random points of cover image ***Step3:*** For each pixel (selected positions) in cover image choose LSB ***Step4:*** Replace (LSB) of cover image with bits of encrypted secretmessage **End**

6. Extracting Algorithm

Information retrieval is reversing the process of the hiding. Data retrieval from stego image is by taking 6 bits of each pixel (2 bits of R, G, and B) until the end of the secret message. After that, convert binary value to hex value and reconstruct secret using Cramer's rule, Figure 2 represents the diagram to extract secret message **.**

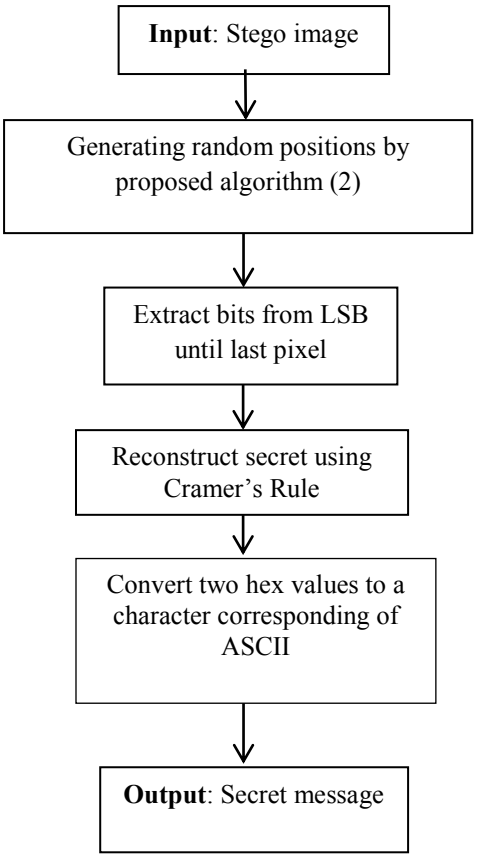

Figure2: Block diagram for extracting text file of proposed method

Algorithm (4): Reconstruct Secret Message
Input: Values Hex
Output: Secret Message (Text File)

Start
Step1: Compute determinant value
Step2: For each two values hex v1, v2 // Sequentially read values hex
H1= ((2 * v1) – v2) / D // Apply Cramer's Rule
H2= (v2 - v1) / D //D is Determinant
2.1. If H1, H2 < 0 then
H1=H1+13
H2=H2+13
2.2. If H1, H2 > 13 then
H1=H1 mod 13
H2=H2 mod 13
H1 and H2 store in R array // R array reconstruct secret message
End for
Step3: For each value in R array
3.1. If Ri < 12 then add Ri to L Array, //Apply Lossless method reverse
3.2. If Ri >=12 then add Ri + Ri+1 to L Array
End for
Step4: for each two hex values convert to a character corresponding ofASCII
Repeat step4 until secret message is completed
End

There are several steps for information retrieval are:

1- Determining positions of hide using Algorithm (2) by entering the stego image, first position and the number of pixels.

2- Extract 6 bits of each pixel (2 bits of red, green and blue color) until the last pixel, then converting the binary to the hexadecimal system.

3- Reconstruct the secret out of (2, 2) threshold using Cramer's rule (used to reconstruct the secret message after converting values to hex through applying algorithm (4))and convert each two values hex to decimal and thus extracting the secret message using ACSII.

7. Experimental Results

Experimental results depend on the quality of the image for measure differences and similarities between the cover image and stego image. There are several measures for evaluating image quality of which Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). Figure 3 explains random distribution of textual information

inside the cover image. Figure 4 explains the histogram of cover image and stego image after hiding file size 20 KB.

Mean Square Error (**MSE**) is the average squared difference between a reference image and a distorted image. The large value of MSE means that image is poor quality.

$$MSE=\frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{jk}-x'_{jk})^2 \quad (5)$$

Where*M*represents the number of pixels in a row direction, *N*represents the number of pixels in a column direction, *x*represents the pixel of original image, ′ represents the pixel of modified image

PSNR is define as the ratio between the maximum possible power of a signal and the power of corrupting noise. PSNR is used as a measure of quality of reconstruction image, the signal in this case is the original image (cover image) and the noise is the error introduced (stego image). PSNR is measured in decibel (db), the high value of PSNR indicates the high quality of the image [8].

$$PSNR=10\ log_{10}\left(\frac{Max^2}{MSE}\right) \quad (6)$$

Where *max* is maximum pixel value of image.

Figure 3: Random distribution of textual information inside image

Cover image		Size file	MSE	PSNR
Name	R*C			
pepper	250*250	20 KB	0.696	49.211
Baboon	192*192	15 KB	0.780	48.722
Lena	160*160	9 KB	0.766	48.797

Table 1: PSNR and MSE Values of Tested Images

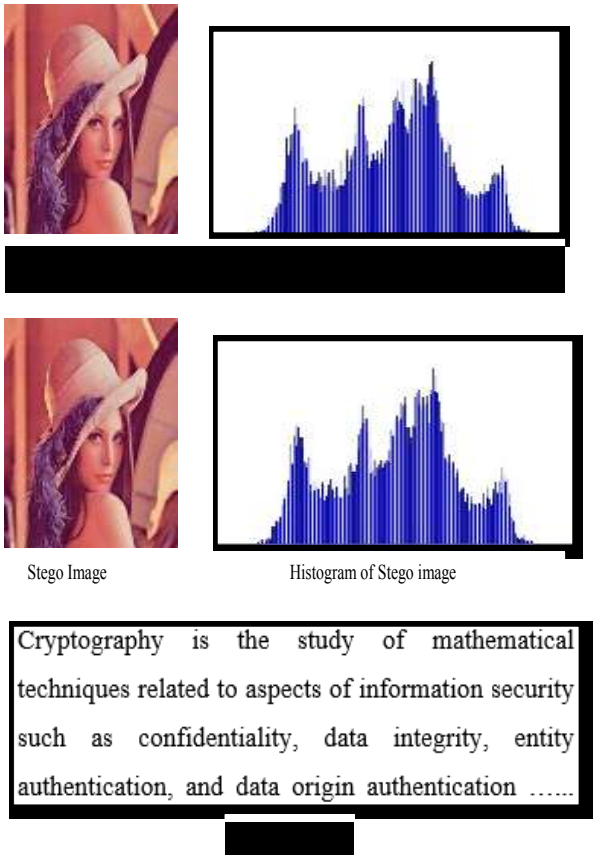

Figure 4: Explains the histogram of cover and stego image after hiding file size 20 k byte

8. Conclusion

In the method used has been hidden and information retrieval without any loss of information or reduction of image quality with good capacity. The using of random hiding in image pixels is more efficient and powerful than the sequential hiding against attacks, because it is difficult to predict of hiding positions in the stego image through image analysis or statistical analyzes. In addition to the use of secret sharing scheme of data before the hide increases the security and strength of the hide against attacker.

References

[1] F. Akhter, "A Novel Approach for Image Steganography in Spatial Domain," Global Journal of Computer Science and Technology Graphics & Vision, Global Journals Inc. (USA) [Online], Vol. 13, Issue 7 Version 1.0, 2013. Available: https://arxiv.org/ftp/arxiv/papers/1506/1506.03681.pdf

[2] D. Singla and R. Syal, "Data Security Using LSB & DCT Steganography in Images," International Journal of Computational Engineering Research, IJCER, Vol. 2, No.2, pp. 359-364, Mar-Apr 2012.

[3] M.A. Al baku'a and A.T. Suhail, "New Method for using Digital Images to Hide Secret Text Files," Foundation of Technical Education AL-TAQNI, Vol. 23, Issue 6, pp. 44-55, 2010, [Arabic].

[4] R. Ibrahim and T.S. Kuan, "Steganography Algorithm to Hide Secret Message Inside an Image," Computer Technology and Application 2, pp.102-108, 2011.

[5] K.N. Teja, G.L. Madhumati and K.R. Rao, "Data Hiding Using EDGE Based Steganography," International Journal of Emerging Technology and Advanced Engineering, Vol. 2, Issue 11, pp. 285-290, November, 2012.

Available: http://www.ijetae.com/files/Volume2Issue11/IJETAE_1112_44.pdf

[6] U. Lokhande and A.K. Gulve, "Steganography using Cryptography and Pseudo Random Numbers," International Journal of Computer Applications, Vol. 96, No.19, pp.40-45, 2014.

[7] P. Preethi and Y. Dasar, "A Secure Image Steganography Based on RSA Algorithm and Random Pixel Selection Technique," International Journal of Research in Engineering Technology and Management, Vol. 3, Issue 3, May 2015.

Available: http://www.ijretm.com.

[8] M. Ghazi and H.M. Salman, "Secret Sharing Scheme Based Technique for Authentication of Documents Images," Eng. &Tech Journal, Vol. 32, Part (B), No.6, pp. 1093-1105, 2014.

[9] A. Shamir, "How to Share a Secret," Communication of the ACM, Vol. 22, No 11, pp. 612–613, November 1979.

[10] C. Thien and J. Lin, "Secret Image Sharing," Computers & Graphics 26, pp. 765–770, 2002.

[11] A. Croft, "Engineering Maths First-Aid Kit," Pearson Education, Ltd, Prentice Hall, 1st ed., England, 2000.