Information Hiding in Image Based on Random Locations

Mohsin H. AL-Zohairi*

mh_alz@yahoo.com

Received on: 25/09/2011
Accepted on: 14/05/2012

Abstract: Network Security for data transmission is the most vital issue in modern communication systems. This paper discusses a new steganographic technique and the effectiveness of the proposed method is described through which the idea of enhanced security of data can be achieved. To hide data in a binary image, the proposed method focuses on the Least Significant Bit (LSB) technique in hiding messages in an image. The proposed method enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message easily.

Keywords: Steganography, Cryptography, Cover image, Random locations

***Engineer at Ministry of Higher Education and Scientific Research, Baghdad, Iraq**

1. Introduction

The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, for example, confidential transmission, video surveillance, military and medical applications. In steganography, the secret message is embedded into an image (or any media) called cover image, and then sent to the receiver who extracts the secret message from the cover message. After embedding the secret message, the cover image is called a stego-image. This image should not be distinguishable from the cover image, so that the attacker cannot discover any embedded message. The security of the transformation of hidden data can be obtained by two ways: cryptography and steganography. A combination of the two techniques can be used to increase the data security [1]. *Cryptography* is the study of Secret Writing. It is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form. As the field of cryptography has advanced; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of the transfer of information under difficult circumstances [2]. *Steganography* is the study of techniques for hiding the existence of a secondary message in the presence of a primary message. The primary message is referred to as the carrier signal or carrier message; the secondary message is referred to as the payload signal or payload message [3].

2. Previous works

Simply, LSB modification bits from data that has to be hidden are put at the LSB of the cover image. Digitized images are made of pixels in which each pixel can use three bytes i.e. 24 bits. Here, three bytes are the representative of red, green and blue colors respectively. In the LSB method the least significant bit of each byte is set to zero. Now according to the bits 0 or 1 in data, LSB is being changed. If data bit is 0 then LSB remains the same & if data bit is 1 then LSB is changed to 1.For doing this modification, the image becomes a little bit lighter than the original one. Nowadays, a more sophisticated approach has been taken for hiding data. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 0001000011001011

Now suppose we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the9 bytes above, we get the following (where bits in bold have been changed):

10010101 0000110**0** 11001001
10010111 0000111**0**11001011
10011111 00010000 11001011

Note that we have successfully hidden 9 bits but at a cost of only changing 4, or roughly50%, of the LSBs [1].

3. Image Processing

An image file is merely a binary file containing a binary representation of the color or light intensity of each picture element (pixel) comprising the image. Gray-scale images, too, are very useful for steganographic purposes [4]. We are using 24-bit color. The amount of change will be minimal and indiscernible to the human eye[1]. The matrix of pixels represents every image. According to the basic RGB color model, every pixel is represented by the three bytes namely red, green, and blue. Their significance is as follows:

Red: Gives the intensity of red color in that pixel.

Green: Gives the intensity of green color in that pixel.

Blue: Gives the intensity of blue color in that pixel [5].

4. Steganographic Algorithm Criteria

Steganographic algorithms can be characterized by a number of defining properties. Three of them, which are most important for image steganographic algorithms, are defined below.

- ***Transparency:*** Evaluates the image distortion due to signal modifications like message embedding or attacking. In most of the applications, the steganography algorithm has to insert additional data without affecting the perceptual quality of the image host signal. The fidelity of the steganography algorithm is usually defined as a perceptual similarity between the original and stego Image sequence.
- ***Capacity:*** The capacity of an information hiding scheme refers to the amount of information that a data hiding scheme can successfully embed without introducing perceptual distortion in the marked media. In other words, the bit rate of the message is the number of the embedded bits within a unit of time and is usually given in bits per second (bps).
- ***Robustness:*** measures the ability of embedded data to withstand intentional and unintentional attacks. Unintentional attacks generally include common data manipulations such as lousy compression, digital-to-analog conversion, re-sampling, re-quantization, etc. whereas intentional attacks cover a broad range of media degradations which include addition white and colored noise, rescaling, rotation , resizing, cropping, random chopping, and filtering attacks .Also, the robustness of the algorithm is defined as an ability of the data detector to extract the embedded message after common signal processing manipulations[3].

5. The Proposed System

This paper proposed a *Secure Information Hiding System* (SIHS) that is based on *Least Significant Bit* (LSB) technique in hiding messages in an image. The system enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message. We randomly select the pixels of the *cover-object* that is used to hide the secret message. The selection of pixels is based on the following formula that generates locations without any repeating.

$$x(i+1)=(a*x(i)+c) \bmod m \quad (1)$$

Where m, n, a, c and x are non-negative integers. We can generate locations without any repeating only with values in Table (1) below.

Table (1) Parameter values of generation formula

a	c	X(0)	m	X(i+1)
11	11	11	71	70 locations
11	11	11	101	100 locations
11	11	11	701	700 locations

Then we generate random numbers among (0 to 2) on chosen pixel to select one byte to hide one bit in it, in other words we hide one bit in one byte of chosen pixel.

For example, if chosen pixels are 60, 5 and 31.

10000101 10001110 00111001

01010111 00111001 11100011

11110000 11000111 10000011

Byte locations used to hide a message (110) in pixels are 1, 2 and 1.

10000101 1000111**1** 00111001

01010111 00111001 1110001**1**

11110000 1100011**0** 10000011

Note that there is no problem if the locations of bytes are repeated because we hide one bit in one pixel and this increases the security of hiding information and makes it difficult to attacker to detect it easily. Both the sender and receiver must share the *stego-key* during the communication. The key is then used for selecting the positions of the pixel and byte where the secret bits had been embedded.

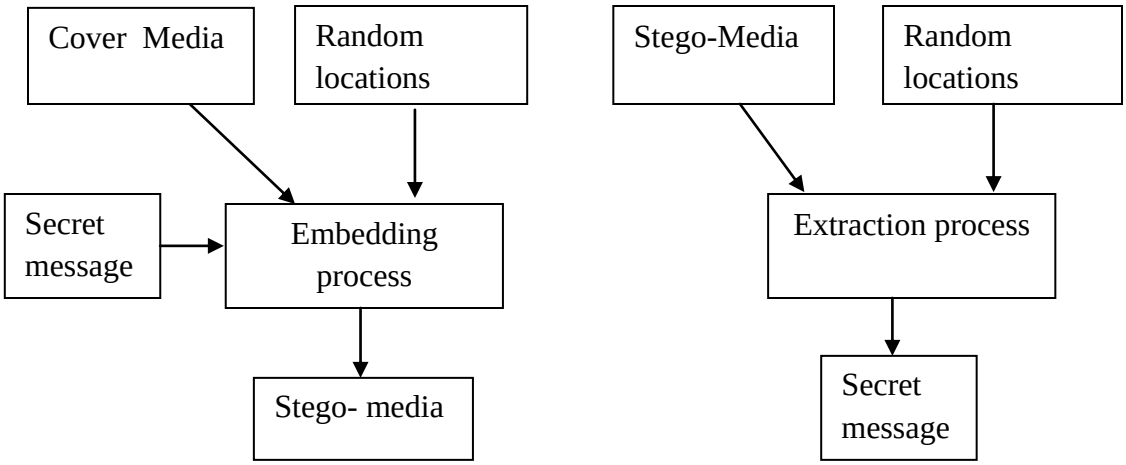

Figure (1) Steganography System

6. Experimental Results

The (weighted) mean squared error between the cover -image and the stego-image can be used as one of the measures to assess the relative perceptibility of the embedded message, see Table 2.

$$\mathbf{MSE}=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}||C(i,j)-S(i,j)||^2$$

Where m and n are the number of rows and number of columns of the cover image, respectively; C (i, j) is the pixel value from the cover- image; S (i, j) is the pixel value from the stego-image[6].

Table (2) Results of MSE

Secret message	MSE
10 bytes	1.6286×10^{-4}
20 bytes	3.3025×10^{-4}
30 bytes	5.2931×10^{-4}
40 bytes	6.7861×10^{-4}
50 bytes	8.7314×10^{-4}
60 bytes	1.0631×10^{-3}
70 bytes	1.2576×10^{-3}
80 bytes	1.4296×10^{-3}

Original image **Stego-image**

Figure 2 The original and stego-image using the proposed technique

7. Discussion

Random locations play an important role in the secure implementation of steganography. In this method there are two keys used to hide the secret message: the first to select the pixel and the other to select one byte of the pixel that is used to hide one bit of a message in it. The present work concentrates upon using Least Significant Bit but is not limited to it. In general, from the result tables above, the Mean Squared Error (MSE) increases when the embedded message size increases.

8. Conclusion& Suggestions for Future Work

After studying the whole system, one can conclude the following:

1-This method is applicable when the size of a message is small, also the error will appear because the present work is LSB.

2- Image file (24 bit color) is a good cover for hiding secret data because the amount of change will be minimal and indiscernible to the human eye, see Figure 2.

3- There is a tradeoff between the amounts of the information to be hidden and the robustness of the system, it is impossible to obtain both. If the information to be hidden has big size then this will reduce the robustness of the system.

Suggestions for Future Work are:

1- Developing a system that uses another hiding image file format, for example (JPEG or GIF).
2- Developing a system that offers a better performance in security field.

Acknowledgement
I would like to thank Miss Susan S. Ghazoul for her guidance and direction

References

[1] Debnath Bhattacharyya, Arpita Roy, Pranab Roy, and Tai-hoon Kim, ”Receiver Compatible Data Hiding in Color Image”, International Journal of Advanced Science and Technology Volume 6, May, 2009.

[2] Amoghmahapatra and Rajballav dash,” Data Encryption and Decryption by using Hill Cipher Technique and Self Repetitive Matrix”, Thesis, Department of Electronics & Instrumentation Engineering, National Institute of Technology
,Rourkela ,2007.

[3] Mazdak Zamani , Azizah A. Manaf , Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, "A Genetic-Algorithm-Based Approach for Audio Steganography", World Academy of Science, Engineering and Technology 54 2009.

[4] Sanjeev Manchanda, S. B. Singh and Mayank Dave," Customized and Secure Image Steganography through Random Numbers Logic”, Signal Processing: An International Journal, Volume1: Issue (1).

[5] http://www.4shared.com/ Steganography.

[6] Susan Sabah Ghazoul, "development of information Hiding System Based on AVI format”, M. Sc. Thesis, University of Technology - Baghdad, 2007.