Enhanced Least Significant Bit Technique for Hiding a Text Message in an Image Cover Object

Prof. Dr. Taleb A.S. Obaid,
Department of Computer Information Systems,
University of Basrah,
e-mail: tasobaid@gmail.come
tasobaid@uobasrah.edu.iq

ABSTRACT

Maintaining the security of information is the most significant factor of information technology and communication since the growth of the internet technology implementation. Fast transferring of data from the source to destination should be entirely safe. Safekeeping the data from penetration by hackers and altering the content of the transferred data is essential objective in communication.

Steganography is away to reserve the existence of hidden secret data inside a cover object, while pictures and images are the most common cover objects for steganography.

This work introduces the concept of steganography using an improved approach to enhance least significant bits algorithm: "Enhanced LSB Algorithm". The used method is by implementing a colored image as a cover object to hide secret text messages. Taking in consideration that embedding secret information inside images requires sensitive and intensive computations, while the spatial domain techniques manipulate the cover-image pixel bit values to embed the confidential information.

Keywords— Steganography, Scattered style, Embedded, Data hiding, LSB method, Carrier file

1 INTRODUCTION

To keep communication transmission through the electronics channels secured and safe the cryptography techniques may be used. Many different methods have been developed to encrypt and decrypt data in order to keep the message transmission more opacity by Intrusive, in addition to its fundamental purpose to protecting the confidentiality of messages transferring. This paper aspires to conceal the messages mainly from the source to the second party, where Steganography is the technique used to satisfy this goal [1]-[3].

The term "Steganography" refers to covered writing text message by other media, is the art and science of transparent communication of messages. This is done by hiding any sending information in additional information as a cover object, i.e., hiding the existence of the communicated information, [4]-[7].

Furthermore, Steganography and Cryptography have significant differences in nature. Cryptography focuses on retaining the contents of a message, unreadable by using different encrypted techniques, on the other hand, Steganography focuses on keeping the existence of a message's secret hidden, [8]. Despite the variation in the two techniques, both Steganography and Cryptography are ways for protecting information from undesirable party, as there are also other technologies that are closely related to Steganography, such as watermarking and fingerprinting.

This paper described many different approaches to the Enhanced Least Significant Bits (ELSB) approach, and implemented them to illustrate the more security potential of Steganography data communication for business and personal use. The Steganography framework in this work is made up of three elements:

- ✓ The carrier digital file,
- ✓ The text message,
- ✓ Least significant bits location array.

The carrier digital file is the object; digital image, video, audio...; that wills "carry‶ the hidden message without affecting the nature of the original covered file. Moreover, text message is the plain text or encrypted text that we are interested to forward it to the specific destination and retrieve the message safely. Finally, location array contains the array indices, where that the message bits will to be hidden. Different scenarios could be imposed to conceal the text message, and secret bits of the message are saved directly in the cover image pixel bytes.

2 RELATED WORK

Hiding information is the process of embedding data into digital cover object as a carrier file without causing perceptual degradation [1]. The popular techniques which can be used to hide data are watermarking, Steganography and Cryptography. The authors propose an algorithm to hide data inside image using Steganography technique, where the proposed algorithm uses binary codes and pixels inside an image, [4]-[6]. The zipped file is used before it is converted to binary codes to maximize the storage of data inside the image, [1].

Steganography is hiding the existence message by hiding its information into various carriers. The primary intent is to prevent the detection of hidden information. since the Steganography message is invisibly integrated and covered inside other harmless sources, so it is very challenging to detect the message without knowing the existence and the appropriate encoding scheme [2].

Many researchers have carried out studies in hiding data inside image using Steganography technique, for example in [6-10]. El-Emam [9], on the other hand, proposed a steganography algorithm to hide a large amount of data with high security. His steganography algorithm is inside a color bitmap (bmp) image. Furthermore, Kavate et al. [10], gives a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hiding data into image which is implemented through Microsoft .NET framework.

3 PROBLEM DEFINITION

The aim of this work is to hide a text message over an image object using least significant bit algorithm and to send the stego file to the intended destination. The receiver of the embedded message can retrieve the secret message that has been forwarded, [2].

3.1 Least Significant Bit Technique

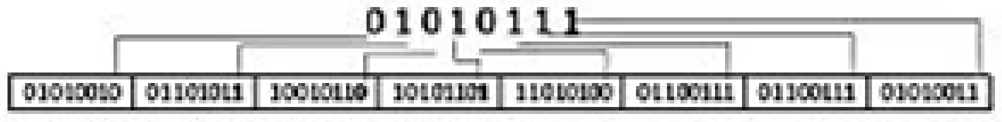
Least significant bit (LSB) insertion is very familiar, and relatively simple, approach to embed any digital based on hiding a large amount of data (image, audio, text) file data in a cover object, which is usually an image file. This technique required to convert the text message to ASCII code data and then to binary data (bits) to replace with an LSB bit. This technique works well for image Steganography. The human's eye dose not distinguishes the first carried image and stego image and will look like as an identical image.

In LSB Steganography, the eight's bit in gray scale of the cover media' is used to conceal the required hidden message. LSB technique tends to replace some of the last bit of each of the pixel values to reflect the message that needs to be hidden.

To clarify, consider an 8-bit gray scale bitmap image where each pixel is stored as a byte representing a gray scale color value. Then, suppose the first eight pixels of the original image has the following gray color value:

01010010	01101010	10010111	10101100	11010101	01100111	01100110	01010011

To hide the letter W whose ASCII code is 87 and binary value code is 01010111, we would replace the LSBs of these pixels to have the following, [2], [11]-[14].



Note that, the average half of the LSBs need to be changed. The difference between the cover image and the stego image will be hardly noticeable to the human eye. However, one of the significant limitations is the small size of data which can be embedded in such type of images using only LSB bits. This method is not completing safe and porous by intruders.

4 ENHANCED LSB (ELSB) ALGORITHM

LSB algorithm hides information in the least significant bit of each color sequentially of the carrier image. The main drawback of this algorithm is not challenging to detection. Thereafter, the preferred method that would introduce more efficiency and less distortion is **Enhanced Least Significant Bit**, as it improves the performance of LSB algorithm by hiding information not only in one of the LSB sequentially.

Steps of Enhanced Least Significant Bit (ELSB) Algorithm

1. Select a cover image of size M*N as an input.
2. Convert the color image to gray scale then to binary
3. The message to be hidden is embedded in least significant bits of the binary image randomly.
4. After that message is hidden using bit replacement method.
5. Send stego image to the receiver.

4.1 EMBEDDING PROCESS

After completion of image to matrix the next step is to embed a message into an image. The image obtained during this process is called a stego-embed image. The message is inserted into the intensity values of image obtained during image to matrix conversion. The intensity values of the embedded image are as shown in the figure 1.

I. First, distributing a text message bit between the least two significant bit, i.e. '8th and the '7th column in gray scale' sequentially as the following:

Suppose one byte of the text message as:

Message byte

7	6	5	4	3	2	1	0
0	1	1	1	0	1	1	1

And the eight bytes of the image as:

Image bytes

01010010	01101010	10010111	10101100	11010101	01100111	01100110	01010011

Embedded first procedure of the message bits in image bytes

Byte No.	Image Bytes	Stego image Bytes	Notes
0	01010011	01010011	No change in 8th bit
1	01100110	01100110	No change in 7th bit
2	01100111	01100110	Change in the 8th bit
3	11010101	11010101	No Change in the 7th bit
4	10101100	10101101	Change in the 8th bit
5	10010111	10010111	No change in 7th bit
6	01101010	01101011	Change in the 8th bit
7	01010010	01010000	Change in the 7th bit

The implementation of this result is shown in Figure 2.

II. Secondly, embedding text bits in the cover image byte sequentially in reverse order approach of LSB as the following:

Message bit of one byte

7	6	5	4	3	2	1	0
0	1	1	1	0	1	1	1

And the eight bytes of the image as:

Image bytes

01010010	01101010	10010111	10101100	11010101	01100111	01100110	01010011

Embedded the second procedure of the message bits in image bytes

Byte No.	Image Bytes	Stego image Bytes	Notes reverse order
0	01010011	01010010	Change in LSB
1	01100110	01100111	Change in LSB
2	01100111	01100111	No change in LSB
3	11010101	11010101	No change in LSB
4	10101100	10101100	No change in LSB
5	10010111	10010110	Change in LSB
6	01101010	01101011	Change in LSB
7	01010010	01010001	Change in LSB

The implementation of the second procedure is shown as in figure 3.

III. Thirdly, distributing the odd bit of text message in the first half of the image byte as:

Message bits of one byte

7	6	5	4	3	2	1	0
0	1	1	1	0	0	1	1

And the eight bytes of the image as:

Image bytes

01010010	01101010	10010111	10101100	11010101	01100111	01100110	01010011

Embedded the third procedure of the message odd bits (yellow shading) in image bytes:

Byte No.	Image Bytes	Stego image Bytes	Notes reverse order
0	01010011	01010011	No change in LSB
1	01100110	01100110	No change in LSB
2	01100111	01100111	No change in LSB
3	11010101	11010100	Change in LSB
4	10101100	10101101	Change in LSB
5	10010111	10010110	Change in LSB
6	01101010	01101011	Change in LSB
7	01010010	01010001	Change in LSB

The implementation of the second procedure is shown as in figure 4.

5 RESULTS AND DISCUSSION

To be able to compare the performance of the proposal improvement method on the LSB method with respect to the classical LSB method, the image in Figure 1, will be used as cover image. The text message to be embedded in the cover image is: "**In general, when you have many possible discrete, known values, switch statements are easier to read than if statements**."

Noting that, the distortion in the cover images of those three procedures cannot be recognized easily by human eyes with respect to original LSB method, as shown in figures 1, 2, 3, and 4, respectively. These excellent results were obtained since the common use of the least significant bits of the cover image but in different scattering styles. Moreover, breaking through the proposed approach is not easy to discover the embedded text message in the cover image compared to the classical LSB method.

The proposed style hardness came from the nature of the text message scattering style inside the cover image, as the scattering style plays a significant role to protect hiding the message in the cover image. Due to the randomly scattered text message bits in LSB, the retrieving procedure more sophisticated. There are many approaches on how to scatter the text message in the cover image.

6 CONCLUSION

This paper proposes three enhanced LSB technique, ELSB (Enhanced Least Significant Bit) that improves the performance of the LSB method of hiding information in only one of the three colors at each pixel of the cover image. Knowing that using the LSB approach does not cause a significant change in the original image.

One of its major limitations of this technique is only a small size of text message data can be embedded in an image using only the least significant bits, the last eight bits. For this reason, the method is not completely safe and porous by intruders. While the sequential scattering of the text message in a cover image is unsecured method. This paper implements different scattering styles to enhance the embedment message. In general, and as a recommendation, it might require a comprise to ensure the original image will not be tempered with too many changes and secured the text message.

REFERENCES

[1] Ibrahim R. and Suk Kuan T. "Steganography Algorithm to Hide Secret Message inside an Image," Computer Technology and Application 2 (2011) 102-108

[2] Champakamala B.S., Padmini K., and Radhika .D. K., "Least Significant Bit algorithm for image steganography," International Journal of Advanced Computer Technology (IJACT), Vol 3, No 4, 2013, ISSN:2319-7900.

[3] Gupta S., Gujral G., and Aggarwal N. "Enhanced Least Significant Bit algorithm For Image Steganography," International Journal of Computational Engineering & Management," Vol. 15 Issue 4, July 2012

[4] Al-Shatnawi A., “A New Method in Image steganography with improved image quality,” Applied mathematical science, Vol.6, no 79, 2012.

[5] Kadam K., Koshti A., Dunghav P., "Steganography Using Least Signicant Bit Algorithm," International Journal of Engineering Research and Applications (IJERA),

[6] Singh K, Singh J., Singh H. V., "Steganography in Images Using LSB Technique," International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 5 Issue 1 January 2015

[7] Kumar A. Pooja Km., "Steganography- A Data Hiding Technique," International Journal of Computer Applications (0975 – 8887), Volume 9– No.7, November 2010

[8] Kiswara Agung K., Fatmawati , Suprajitno H. " Image encryption

based on pixel bit modification," IOP Conf. Series: Journal of Physics: Conf. Series 1008 (2018) 012016 doi :10.1088/1742-6596/1008/1/012016

[9] El-Emam N. N., Hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.Purohit A., Sridhar P." Image Steganography: A Review", International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 4891-4896

[10] Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Signicant Bit Algorithm," International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

[11] Natarajan N., Jose T., Sasidhar Babu S. S., " Secret Data Hiding Using Image Segmentation and Least Significant BIT (LSB) Insertion Steganography," International Journal of Pure and Applied Mathematics Vol. 117 No. 15 2017, 527-534

[12] Obaid T, Khami M., Shehab L., "A classical approach for hiding encryption key in the same encrypted text document" J. of Kufa for Math and Computer, Vol.5, No.1, Mar. 2018, pp 25-38

[13] Darabkh K. A, Jafar I. F. , Al-Zubi R. T., Hawa M. " An improved image least significant bit replacement method," 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Publisher: IEEE, Conference Location: Opatija, Croatia

[14] Odat A. M and Otair M. A, "image Steganography using Modified Least Significant Bit," Indian Journal of Science and Technology, Vol 9(39), DOI: 10.17485/ijst/2016.

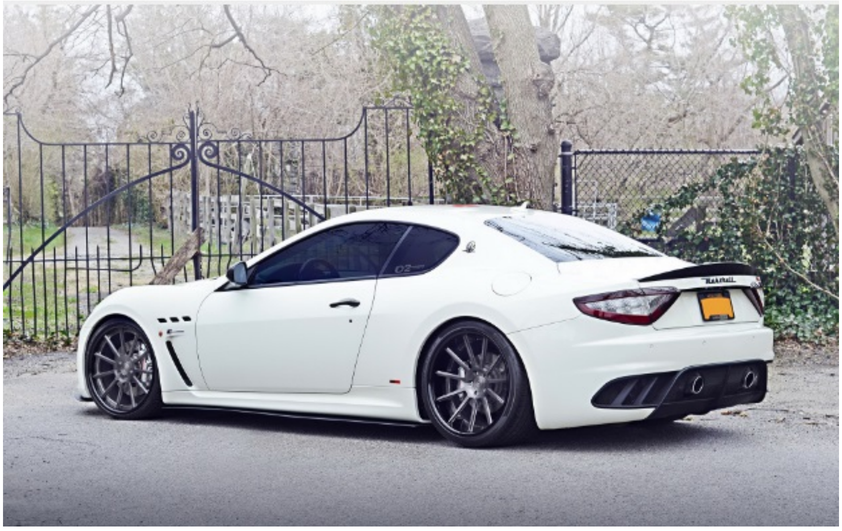


Figure 1: The cover image

Fig. 2 (a), over object

Fig. 2 (b), stego image

Fig. 3 (a), over object Fig. 3 (b), stego image

Fig. 4 (a), over object Fig. 4 (b), stego image