Indian Journal of Science and Technology, Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/86878, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Image Steganography using Modified Least Significant Bit

Ahmad M. Odat[1] and Mohammed A. Otair[2*]

[1]Faculty of Science and Information Technology, Irbid National University, Irbid-Jordan; Aodat@yahoo.com
[2]Faculty of Computer Sciences and Informatics, Amman Arab University, Amman-Jordan; Otair@aau.edu.jo

Abstract

Background/Objective: Manipulation of sensitive images is a very important issue in modern transmission and storage. The objective of this study is to achieve the protection by applying a modified steganography method. **Findings:** The proposed method uses modified Least Significant Bit (LSB) algorithm which depends on segmentations of the secret image bits and distributing it through the odd bytes of the cover image, which in turn must be 16 time the size of the secret image in order to increase the level of protection. **Improvements:** Experimental results show that the levels of hiding capability using the proposed algorithm are improved.

Keywords: Image Processing, Least Significant Bit, Segmentation, Steganography

1. Introduction

Image processing is a wide field and mainly includes key steps that can be mathematically sophisticated; however, the core idea of the image processing is very simple. Using the image data is the main goal of image processing in order to enable the computer perception by recognizing, interpreting and understanding the image patterns. In other words, it is dynamic and expanding field that touch a huge number of applications in different and wide rage disciplines. They include various processes such as object detection and image enhancement[3].

Several mathematical processes and techniques are implemented on the data to digitize an image. In general, digital images have to be improved and more helpful in order to satisfy to a human spectator, or to achieve various of image processing steps such recognition and interpretation that mainly achieved by human. Different fields of engineering and science could use the enhanced images. With some lightning situations, goodness of the images could be influenced by weather disturbance and external noise like inconsistencies of temperature. Enhancement techniques of contrast restricted image through histogram stretching over a logical domain and dynamic multiscale histogram equalization have been proposed[3,6,9].

An image is defined as a two dimensional array, each element (picture element of pixel) of this array represents the intensity value. They could be decreased to a finite set of numbers that can be processed by the direct or neighboring processing. The main steps in image processing can be grouped into[7]: (1) Image acquisition (2) Image compression and coding (3) Image restoration and enhancement (4) Image segmentation (5) Image representation and description (6) Image detection and recognition.

2. Image Security

With the growing uses of computer networks, internet image information must be conveniently and rapidly transformed and distributed. The sharing of secret images has been a main technology to save the exclusiveness in the domain of information protection and security. Unlike, there is a significant trouble that such mechanisms should handle with intentional/accidental images' deterioration when an individual tries to access to the image information. The attacker can modify, destroy,

*Author for correspondence

or even stole the secret images if they are protected by individual user[1,2].

In recent years, how to protect the security of image has become an important issue, and techniques for data hiding have become increasingly more sophisticated and widespread. Image security involves important techniques such as: Digital Image Sharing, Digital Watermarking, and Steganography or Image Hiding. Data hiding is a technique to embed the original secret image in another cover image by some encryption/encoding techniques[1,2].

Recently and due to the possible implementation in information and multimedia security, many researches on techniques of information hiding and information embedding have been considered. Data hiding techniques have been designed to make it harder for users to find data by hiding it in the forms of various materials, such as image, text, audio, and video[1,2].

The main architecture of Steganography consists of three constructs as follow: the Carrier image, the Message, and the Key. The carrier could be an image, which carries the secret message. The purpose of the key is to decrypt or extract the secret message.

A steganographic algorithm is considered as good if it has a significant feature when it is preserving an embedding percentage as much as possible where the original carrier media must be identical as in the stego media[4].

Empirical studies have been undertaken to embed metadata such as image, video, audio or text files in other media, as shown in figure (1). The methods include discrete cosine transform (DCT) encoding, least significant bit (LSB) embedding, MP3Stego, spread spectrum, echo data hiding, etc.

3. Image Steganography with Least Significant Bit

In steganography, a mostly used cover objects are images. Using an embedding algorithm, an image is embedded (as cover image) into another image based on the secret key. The receiver will receive the stego image which is a result of embedding process. The stego image is processed by extracting algorithm at the other side. Unauthenticated persons could access the image transmission but cannot access the stego image, or even discover or extract the hidden message[4].

The Least Significant Bit embedding (LSB) is considered as one of the mostly used digital steganography and embedding techniques. In steganography using LSB, the encryption of the secret messages are achieved by hiding them in the LSBs of the digital signal samples. When the digital sensor is designed, the quantizer puts the LSB in binary coding system or even below the sensor noise of energy level to prevent losing the precision[5], as shown in figure (2).

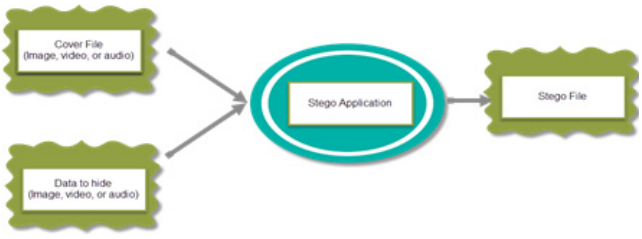


Figure 1. Embedding Data in Steganography.

4. The Proposed Algorithm

There are several types of segmentation images, one of this type is segment image based on the bytes. In this paper, segmentation through the LSB algorithm is applied, and it is expected that the groups of bytes in the cover image submit mixture distributions.

After obtaining the mixture distribution of bytes group for each original and secret image, the next step is to embed the secret image bytes into the original image bytes. The following steps describe how the proposed model works:

1. It used one of the popular methods of steganography (LSB algorithm) which is the simplest technique to

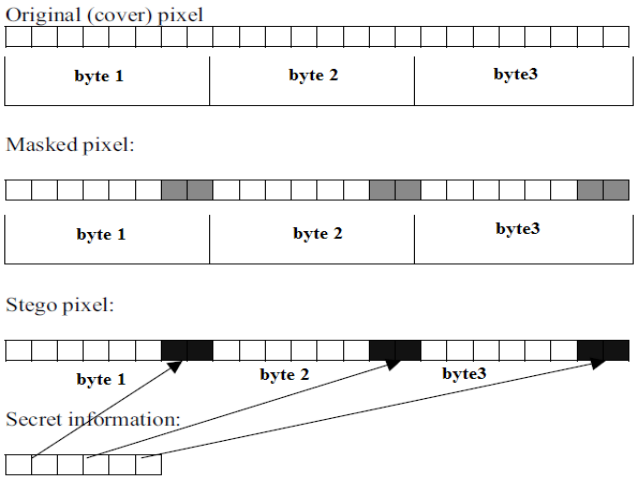


Figure 2. Process of Least Significant Bit.

embed the secret image data into the cover image by exchanging the least significant bit in odd bytes of the cover image to hide bits from the secret image.

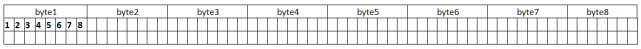
2. LSB algorithm is hidden more than one bit from secret image per one byte from cover image, so the cover size should larger than secret data size. In this paper, the size of cover image should be 16 times in compare with the secret image size, because one bit which is located in the right-most bit is used, and handling the bytes based on the odd and even position.

Cover or Original image

Original Image in Binary Representation

Secret image

Secret image in Binary Representation



Stego Image

Stego Image in Binary Representation

3. This model includes the following two procedures:-

Sender procedure: the sender will hide the secret image in cover image through handling the cover image by using Least Significant Bit; the result for this step will produce stego image, then sent it to receiver party see figure (3) .

Receiver procedure: The receiver will receive stego image from sender, and will decrypt the stego image by Least Significant Bit. The result for this step will retrieve secret image as in figure (4).

5. Experiments

In order to test the stego images based their statistical features, the proposed modified LSB and the classical algorithm were compared from the image distortion levels perspective. To achieve this goal, two of the well-known objective measures for the image quality were used as follow[8]:

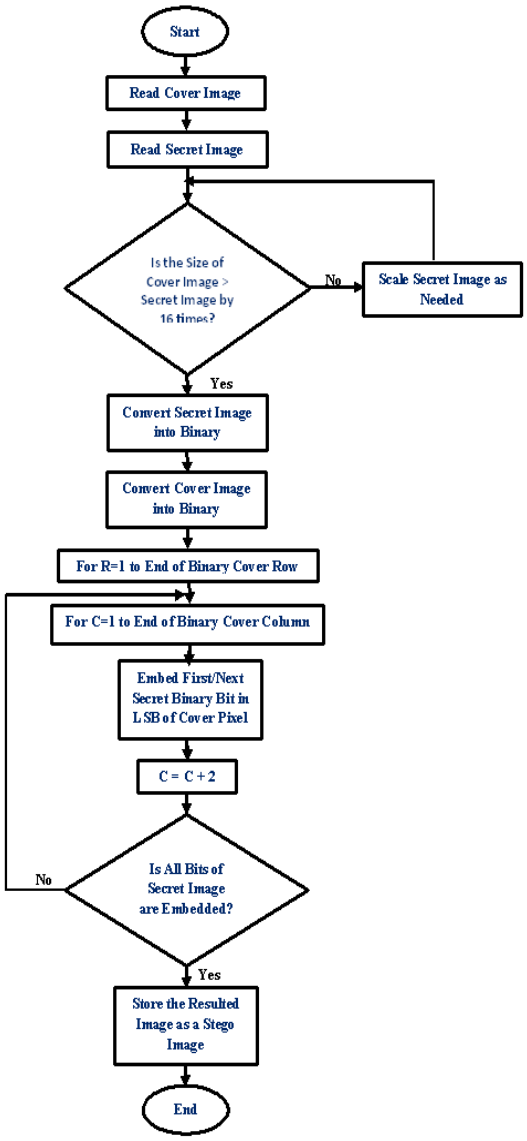


Figure 3. Encrypting Process.

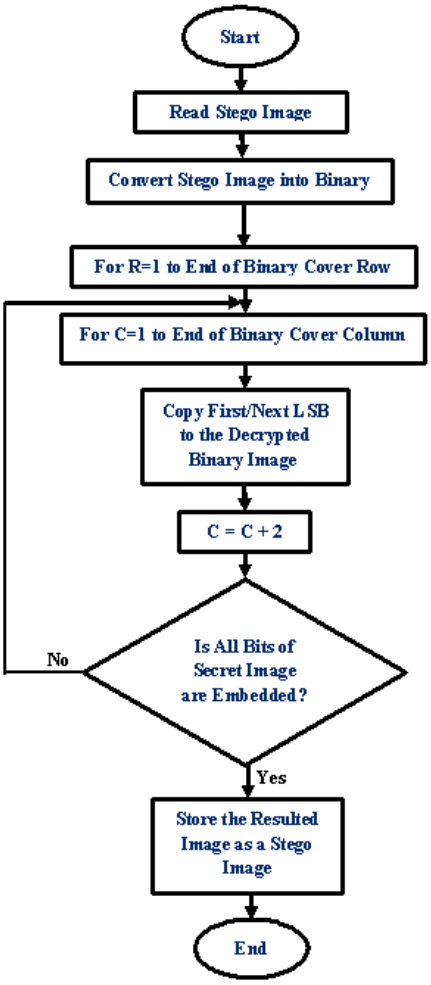


Figure 4. Decrypting Process.

Table 1. Test Images

Image Name	Original Image Size/Bytes
Cameraman.png	38267
Lena.png	38936
House.png	34985
Peppers.png	40181
Bird.jpg	32629

5.1 Peak Signal to Noise Ratio (PSNR)

In steganography, when the secret data is embedded. PSNR measures the ratio noise between the stego image and the original one. Based on the PSNR value, the image quality will be better when its value is higher.

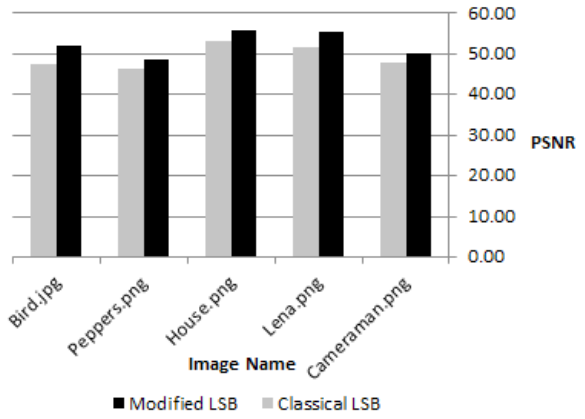


Figure 5. Comparison between Modified and Classical LSB Methods (PSNR base).

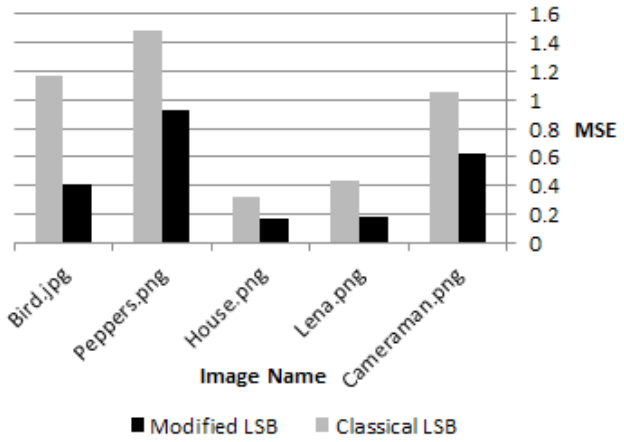


Figure 6. Comparison between Modified and Classical LSB Methods (MSE base).

5.2 Mean Square Error (MSE)

MSE measures the accumulative squared error between the stego image and the original one. According to MSE, the quality of the image in steganography is considered to be better when the value of MSE is lower.

Five 8-bits gray scale images were tested as cover images. Table 1 mentions these images that mainly used in most of the image processing researches.

The values of PSNR and MSE with each cover image were computed and compared using the Modified LSB and Classical one. Figure 5 compares the resulted values of PSNR for all test images using the modified and classical methods. It is noticeable that the modified has a lager values for PSNR with all images, which means the modified method is better

Figure 6 is comparing the resulted values of MSE for all test images using the modified and classical methods. The modified method has a lower values for MSE with all stego images, which means the modified method is better in term of image quality (i.e. it has lower rate of distortion), and then enhance an imperceptibility

6. Conclusion

We applied segmentation through the LSB algorithm, and modified the Least Significant Bit (LSB) algorithm for the secret image bits and distributing it through the odd bytes of the cover image, which in turn must be 16, time the size of the secret image.

7. References

1. Feyzi AKAR, Yalman Y, Varol HS. Data hiding in digital images using a partial optimization technique based on the classical LSB method. Turkish Journal of Electrical Engineering and Computer Science. 2013; 21(Sup. 1):2037–47.
2. Hu C, Liao X, Xiao D. Secret image sharing based on chaotic map and Chinese remainder theorem. International Journal of Wavelets, Multi resolution and Information Processing. 2012; 10(03).
3. Kuber MP, Dixit M. A Review on Modified Image Enhancement Applications. International Journal of Signal Processing, Image Processing and Pattern Recognition. 2014; 7(5).
4. Patel H, Dave P. Steganography Technique Based on DCT Coefficients. International Journal of Engineering Research and Applications. 2012; 2(1):713–7.
5. Revathi M, Bhattacharjee JB, Vijayalakshmi S. Framework of LSB, Adaptive Steganalysis with IQM and Stegnography of Digital Media. Computer Science and Telecommunications. 2010; 25(2).
6. Vijay Ananth S, Sudhakar P. Performance Analysis of a Combined Cryptographic and Steganographic Method over Thermal Images using Barcode Encoder. Indian Journal of Science and Technology. 2016 Feb; 9(7). Doi:10.17485/ijst/2016/v9i7/84152.
7. Shin SY, Jang DH, Park HK. General Image Processing Technique and Car License Plate Application. International Journal of Software Engineering and its Applications. 2013; 7(6):175–84.
8. Stoica A, Vertan C, Fernandez-Maloigne C. Objective and subjective color image quality evaluation for JPEG 2000 compressed images. International Symposium on Signals, Circuits and Systems, SCS. 2003; 1:137–40.
9. Kingslin S, Kavitha N. Evaluative Approach towards Text Steganographic Techniques. Indian Journal of Science and Technology. 2015 Nov; 8(29). Doi:10.17485/ijst/2015/v8i1/84415.