World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:3, 2016

High Secure Data Hiding Using Cropping Image and Least Significant Bit Steganography

Khalid A. Al-Afandy, El-Sayyed El-Rabaie, Osama Salah, Ahmed El-Mhalaway

***Abstract*—**This paper presents a high secure data hiding technique using image cropping and Least Significant Bit (LSB) steganography. The predefined certain secret coordinate crops will be extracted from the cover image. The secret text message will be divided into sections. These sections quantity is equal the image crops quantity. Each section from the secret text message will embed into an image crop with a secret sequence using LSB technique. The embedding is done using the cover image color channels. Stego image is given by reassembling the image and the stego crops. The results of the technique will be compared to the other state of art techniques. Evaluation is based on visualization to detect any degradation of stego image, the difficulty of extracting the embedded data by any unauthorized viewer, Peak Signal-to-Noise Ratio of stego image (PSNR), and the embedding algorithm CPU time. Experimental results ensure that the proposed technique is more secure compared with the other traditional techniques.

***Keywords*—**Steganography, stego, LSB, crop.

I. Introduction

IN the past years, the internet proved to be a suitable medium for transferring digital data and multimedia. Its main advantage is the availability to almost everyone, and the message can be received within a few seconds of sending it. The main disadvantage of using the Internet is the data security because data can be monitored by any unauthorized viewers. This is why steganography should be used. Steganography is a technology for embedding a secure data into a cover image. Any unauthorized user can view the stego image, but only authorized users can extract the secure data [1].

LSB [1] is a widely-used steganography algorithm. It is based on converting characters of the secret text message into binary bits' string. The original algorithm uses a grayscale cover image by embedding up to three bits from the secret text message into the least three significant bits of the cover image pixel [1]. The algorithm was adapted to work on the color images by using the three-color channels. The eight bits are divided into three bits in one color channel, three bits in another channel, and two bits in the last color channel with many variations of the sequence used [5]-[8]. Another adaptation of the LSB is to use it only on a crop from the cover image [2]. It is based on extracting a crop from the cover image and then embedding the secret text message into this crop using LSB technique. Stego image is given by reassembling the image and the stego crop [2]-[4]. The crop coordinates must be known to the receiver to be able to extract the message.

The aim of this paper is to present a more secure steganography technique. It is based on extracting a predefined quantity crops from the cover image with predefined certain secret coordinates (e.g. four crops). Divide the secret text message to sections (four sections). The secret text message sections are embedding into the crops that extracted from the cover image by a secret sequence using LSB technique. The embedding is done using image three color channels by a sequence of three bits into the red color channel, three bits into the green color channel, and two bits into the blue color channel. Extracting the secret text message is impossible without knowing the image stego crops quantity, the image stego crops coordinate that contains the secret text message parts, the secret sequence of embedding the secret text message parts into the cover image stego crops, and the color channels embedding sequence. So the unauthorized viewers cannot monitor the secret message. It means that this technique is high secured.

The rest of paper is organized as follows. The literature review is presented in section II. Section III shows the proposed technique. The simulation results explained in detail in section IV, and section V presents the conclusions followed by the relevant references.

II. Literature Review

A. Least Significant Bit (LSB)

LSB technique is the simplest and widely used steganography *technique*. It is based on embedding the secret text message bits into the least three significant bits of the cover image pixels [8]. LSBs of the cover image's digital data are used to hide the secret text message; it is the LSB steganography [5]. The LSB steganography technique can be classified into two main approaches, LSB replacement and LSB matching [8]. LSB replacement is the simplest. It is based on replacing the least three bit of cover image pixels with each up to three bits of the message data values that needs to be hidden [5]. LSB Basic technique is given by:

$$C = \{ X_{ij} \mid 0 \le i < M_c, 0 \le j < N_c \} \quad (1)$$

$$X_{ij} \in \{ 0,1,2,3,\ldots,255\} \quad (2)$$

$$M = \{m_i \mid 0 \le I < N, m_i \in \{0,1\}\} \quad (3)$$

Khalid A. Al-Afandy, El-Sayyed El-Rabaie, Osama Salah Ahmed El-Mhalaway are with the Faculty of Electronic Engineering, Menoufia University, Egypt (e-mail: khalid_yuosif@yahoo.com, Srabie1@yahoo.com, osam_sal@yahoo.com, Ahmed.elmahalawy@el-eng.menofia.edu.eg).

where C is the 8-bit grayscale cover image with size $M_c \times N_c$, M is the n-bit secret message.

Embed n-bits secret message M into k-LSBs of cover image C, rearrange secret message M to form a conceptually k-bits virtual image M^* represented as:

$$M^* = \{ m^*_i \mid 0 \le i < n^*, m^*_i \in \{0,1,2,\ldots,2^{k-1}\} \quad (4)$$

where $n^* < M_c \times N_c$. Mapping between secret message $M=\{m_i\}$ and embedded message $M^*=\{m^*_i\}$ is defined as:

$$m^*_i = \sum_{j=0}^{k-1} m_{ixk+j} x 2^{k-1-j} \quad (5)$$

A subset of n^* pixels $\{x_{11}, x_{12},\ldots,x_{1n}\}$ is chosen from the cover image C in a predefined sequence. Embedding is done by replacing LSBs of x_{1i} by m^*_i. mathematically, the pixel value x_{1i} of the chosen pixel for storing the message m^*_i was modified to form the stego pixel x^*_{1i} as:

$$x^*_{1i} = x_{1i} - x_{1i} \bmod 2^k + m^*_i \quad (6)$$

The embedding algorithm is changed slightly to be adapted to RGB color images. The mathematical models (1) to (6) are used for each color channel pixels. The 8-bits of secret text message are divided into 3 parts for embedding into color channels with the sequence, three bits in the red color channel, three bits in the green color channel, and two bits in the blue color channel. It must be noted that authorized receivers must have the same color channels 8-bits order used for embedding the secret text message into the color cover image to be able to extract the secret message [1], [5]-[8]. Fig. 1 shows LSB in RGB color cover image.

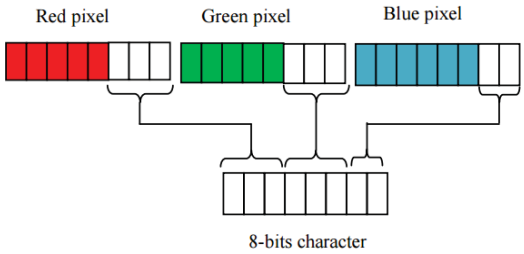


Fig. 1 LSB in RGB color cover image

B. LSB on Cover Image Crop

LSB on cover image crop is applied according to [4]. It is based on extracting a crop from the cover color image with predefined secret coordinates. The secret text message is embedded into this crop using LSB technique explained in A. Stego image is given by reassembled image and the stego crop. It must be noted that authorized receiver must have the cover image crop coordinates and the bits order into color channels to extract the secret message [2]-[4]. Fig. 2 shows the cover image (a) and the cover image crop (b) that the secret message is embedded into.

(a) (b)

Fig. 2 (a) Cover image, (b) cover image crop

III. The Proposed Technique (LSB in Predefined Crops Color Image)

The goal of the proposed technique is to ensure that no one except the authorized viewer can monitor or extract the secret text message. This technique is based on cropping the cover image into a predefined number of crops with certain secret coordinates (e.g., four crops). Divide the secret text message into parts with the same cover image crops quantity (four parts). Embed each secret text message part into an image crop by secret sequence using the LSB technique. Embedding is done in color channels by the sequence, three bits in the red color channel, three bits in the green color channel, and two bits in the blue color channel. Finally assembles back the stego crops and the cover image given the stego image. It must be noted that the secret message can't be extracted without knowing the cover image stego crops coordinates, the quantity of the stego crops, embedding sequence of the secret text message parts into the image crops, and the bit's sequence into color channels. Fig. 3 shows the cover image (a) and the four crops (b) that the secret message is embedded into it.

(a)

(b)

Fig. 3 (a) Cover image, (b) cover image 4 crops

LSB multi crops color image Embedding Algorithm:

Step1. Read the cover RGB color image.
Step2. Read the secret text message.
Step3. Divide the secret message into four parts.
Step4. Extract four crops from the cover image with certain coordinates.
Step5. Convert each part from the secret text message into binary.
Step6. Embed each part from the secret message into a crop using known sequence by the order that three bits in the red color channel, three bits in the green color channel, and two bits in the blue color channel.
Step7. Assemble the four stego crops and the cover image and given the stego image

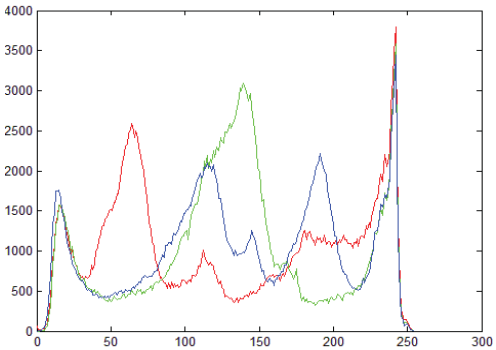
LSB multi crops color image Extracting Algorithm:

Step1. Read the stego RGB color image.
Step2. Extract four crops from the stego image with the same crops coordinates in the embedding algorithm.
Step3. Read LSB from the four stego crops with the same color channels bits order in embedding algorithm.
Step4. Convert binary to text.
Step5. Connect the four parts of a secret text message with the same sequence in embedding algorithm given the secret text message.

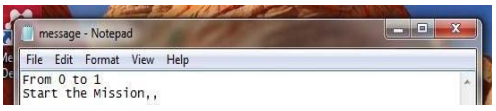
IV. Simulation Results

All tests were performed using an Intel® core™i5 CPU M 450 @ 2.4 GHz with 6 GB Memory, running Windows 7 64-bit operating system and using MATLAB 8.

(a)



(b)



(c)

Fig. 4 (a) original image (image.jpg), (b) original image histogram, (c) secret message (message.txt)

The image used are RGB color JPEG images with size 512 × 512, resolution 96 × 96 dpi and bit depth 24 cover image Rokayya and text secret message message.txt as shown in Fig. 4 where (a) original image Rokayya, (b) original image histogram and (c) secret message message.txt. There are four main tests to determine the performance of any steganography technique. Visually test to determine any degradation in quality or colors compared to the original image, the Peak Signal-to-Noise Ratio (PSNR) of the stego image, Embedding algorithm CPU time and the secret text message extracting complexity (the secure of the steganography technique). PSNR can be calculated by:

$$\mathrm{MSE} = \frac{1}{\mathrm{N}^2} \sum_{x=0,y=0}^{N-1} (\mathrm{A_s}(x,y) - \mathrm{A}(x,y))^2 \tag{7}$$

$$\mathrm{PSNR\ (DB)} = 10 \log_{10} \frac{255^2}{\mathrm{MSE}} \tag{8}$$

where A is the original image, A_s is the stego image and M, N are the sizes of the original and the stego image. It must note that higher PSNR is the best result. Visualization test results for the proposed technique compared with the other state of art techniques shown in Fig. 5. The PSNR and algorithm CPU time are shown in Table I and Fig. 6.

TABLE I
Comparison for Related Works and Proposed Work Based on PSNR and Algorithm CPU Time for Stego Image

	Related works		Proposed work
	LSB	LSB on crop	LSB on 4 crops
PSNR	62.5699	63.3480	62.5332
Algorithm CPU Time	0.6552	0.39	0.4524

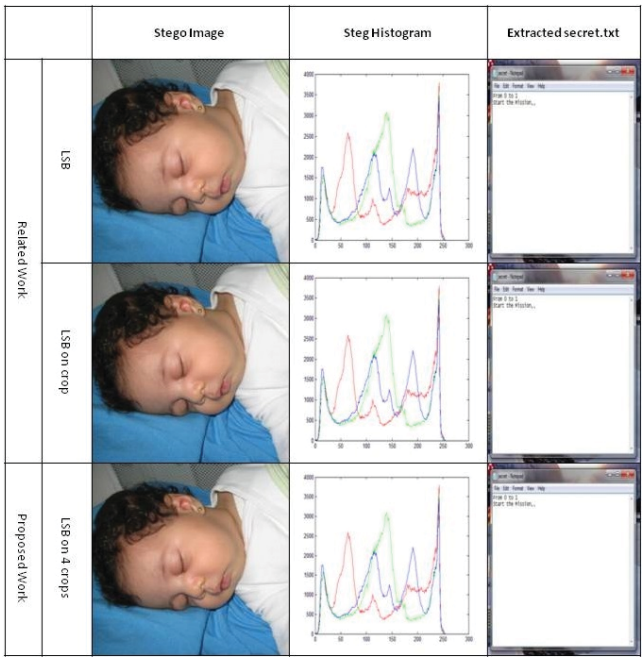
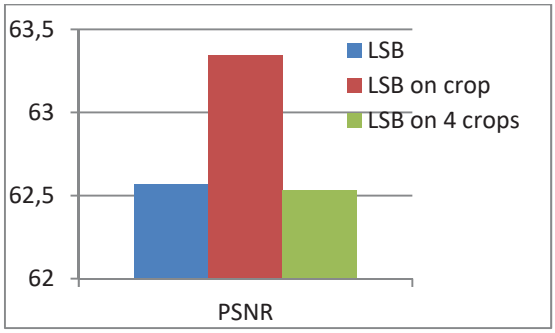
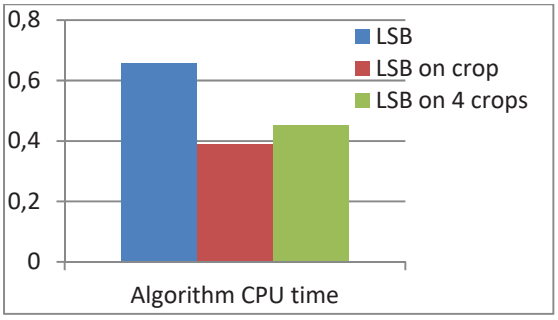


Fig. 5 show visualization test results for proposed technique compared with other techniques



(a)



(b)

Fig. 6 (a) show PSNR for stego images, (b) show Algorithms CPU Time

As shown from the visualization test, the stego images for the proposed technique and the other compared techniques in this paper are have not any degradation in quality. The evaluation figures results (Figs. 2-6) illustrate that the PSNR of the stego image for the proposed technique is in the range of the other state of art techniques and algorithm CPU time for the proposed technique is in the range of the other state of art techniques, the difference is a fraction of a second. Extracting the secret text message in the proposed technique is more complex, secure, and could not be monitored by unauthorized users.

V. Conclusions

This paper proposes a high secure data hiding technique using cropping image and LSB steganography. It is based on dividing the secret text message into four parts and extracting four crops from the cover color image with certain secret coordinates. Embed each message part into image crop using predefined secret sequence. Reassemble the crops with the cover image given the stego image. This proves to be a more secure method for data hiding and at the same time more complex in secret data extraction. The experimental results demonstrated that the proposed technique PSNR and CPU time is within the same range of other similar techniques yet it proves to be more secure.

References

[1] Jassim, Firas A., "A novel steganography algorithm for hiding text in image using five modulus method", arXiv preprint arXiv, Vol. 72, No. 17, PP. 39-44, 2013.

[2] Bandyopadhyay, Debiprasad, et al., "A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 3, No. 1, PP. 11-22, 2014.

[3] Jain, Nitin, Sachin Meshram, and Shikha Dubey., "Image Steganography Using LSB and Edge–Detection Technique", International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, No. 3, PP. 217-222, 2012.

[4] Rakhi1 & Vijay Prakash Singh., " Data Hiding In Skin Tone Of Images Using SteganographY", International Journal of Electronics and Communication Engineering (IJECE), Vol. 2, No. 4, PP. 105-112, 2014.

[5] Goel, Stuti, Arun Rana, and Manpreet Kaur., "Comparison of image steganography techniques", International Journal of Computers and Distributed Systems, Vol. 3, No. 1, PP. 20-30, 2013.

[6] Lwin, Thandar, and SUWAI PHYO., "Information Hiding System Using Text and Image Steganography", International Journal of Scientific Engineering and Technology Research, Vol. 3, No. 4, PP. 1972-1977, 2014.

[7] Krati Vyas, B.L.Pal, "A Proposed Method In Image Steganography To Improve Image Quality With Lsb Technique", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, No. 1, PP. 5246-5251, 2014.

[8] Rawat, Deepesh, and Vijaya Bhandari., "Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method", International Journal of Computer Applications, Vol. 67, No. 1, PP. 22-25, 2013.

Khalid A. Al-Afandy. Born in Egypt, 1st Aug 1975, B.Sc degree 1997 in Electronic Engineering, Computer department, Menoufia University, Egypt.
Work in Town Gas company, May 2006 to Jan 2012 Senior Engineer in GIS department, Jan 2012 to May 2013 GIS Head Department, May 2013 to Jan 2014. Finally, he is the Head of Department in Marketing, then, from Jan 2014 till now, he is the Major Customers Administration Director.