Journal of Engineering and Applied Sciences 13 (Special Issue 1): 2282-2287, 2018
ISSN: 1816-949X

Image Steganography Based on Variable Sized Segments

Samraa Adnan Al-Asadi
College of Information Technology, University of Babylon, Hillah, Iraq

Abstract: Steganography is the method of concealing a secret message within a cover object such as text, image, audio and video. The main goal of the steganography is the imperceptibility which means making the prediction of the existence of the secret message difficult. This study develops an imsage steganography method deals with hiding a text message within a JPEG cover image. The proposed method has the goal of increasing the security by applying the encryption to the secret message before concealing it. The encryption is based on using an audio file as a key. The proposed method is achieved by modifying the Least Significant Bit (LSB) insertion method. Each step in the proposed system will generate four segments, segment's size is variable throughout the processing. The proposed system used different number of bits with the LSB for each selected pixel, so, the 1st selected pixel will be leaved without concealing any secret bit, LSB (1-1-0) will be applied to the 2nd selected pixel while the LSB (0-1-2) will be applied to the 3rd selected pixel. Finally, LSB (2-0-1) will be applied to the 4th selected pixel. The proposed method is considered secure against the attack since, it uses the encryption, also, it has a good PSNR, AD and COR statistical values making it convenient.

Key words: Information hiding, image steganography, PSNR, COR, AD, modifying

INTRODUCTION

Steganography is one of the methods used for hiding information within a cover object, steganography deals with hiding the existence of the secret message. In this way, if successfully achieved, the message does not attract attention from eavesdroppers and attackers. With steganography, there are many types of cover medium which known as carrier, like images, video files, audio files and text files (Hamid *et al*., 2012).

Steganography is an old technology whereas the ancient Greeks used to pass the secret messages from one area to another. They used the heads of the slaves to wrote the secrete message and they wrote the secret message on a wax wood tablet after removing the wax, then recovering this tablet with the wax and then sent it to the destination (Bansod and Bhure, 2014). Invisibility (imperceptibility) which is keeping the secret message invisible without affecting the carrier and ensure that no one can notice that a change had occurred is the main objective of steganography. This feature makes steganography differ from cryptography which is ensuring only the confidentiality of the message content (Al-Asadi and Bhaya, 2016). Another two main objectives of steganography are:

- Capacity: that deals with information amount that can be hidden within the cover object
- Security: that deals with the inability of the attacker to retrieve the secret hidden information

Files that have high redundancy are more suitable to use for steganography because any substitution to the redundant bits of that object cannot be noticed easily. For that reason, images and audio files are the most suitable file formats that can be used with steganography, since, they have a lot of redundant bits.

The embedding part within each steganography method has the inputs (the cover object and the secret message) whereas the key is the implemented method to conceal the secret message within the cover object. The key is important to ensure that no one can easily extract the secret message without knowing the applied steganography method. The output is the Stego object which looks like the cover object but the invisible secret message concealed within it (Al-Asadi and Bhaya, 2016).

Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR) are the most popular distortion measurements, deal with coding and compression of the image and audio files, they are measured in decibels (dB). For checking the quality of the image steganography method, Mean Square Error (MSE), the PSNR measurements will be used (Al-Asadi and Bhaya, 2016). The Average Difference (AD) is also used to check the quality of the steganography method (Al-Shatanawi and Emam, 2015). For comparing the similarity between the cover and the stego images, cross Correlation Coefficient (COR) is used (Tayel and Shawky, 2014).

Literature review: Following are some of the related published works in image steganography (Al-Shatanawi and El-Emam, 2015) present a steganography method and in order to make a secret image unreadable, they used Advanced Encryption Standard (AES) and they modify the traditional LSB method to conceal more than one bit in every byte and finally they segment the image to non-uniform segments in order to make the concealing process non-sequential (Al-Shatanawi and El-Emam, 2015).

Khan *et al*. (2016) proposed a new steganography algorithm, this algorithm has the property of contrast modification. They used histogram modification to maintain the image quality and they used second order mathematical differential equation to protect the image during transmission (Khan *et al*., 2016).

Kaul and Chandra (2015) proposed a new algorithm to increase the data payload to be hidden. Their proposed algorithm works on the bit level and it deals with text in image steganography. The proposed algorithm generates a key after searching text in image. The key will determine where the text will be hidden (Kaul and Chandra, 2015).

Bawaneh and Obeidat (2016) propose a method that converting many types of images to gray scale 24 bitmaps, then find the possible segments within the image.

Debiprasad propose a method that first encrypts the secret message bits based on chaos theory, then concealing this encrypted stream of bits within the cover image using LSB (3-3-2) image steganography method (Bandyopadhyay *et al*., 2014).

Adil (2015) proposed a method deals with both encrypting text message and plain digital image. The encrypted method named as assignment significant bit. His proposed method transforms each word to 26 digits grey level numbers. Then, the message will be represented as a border of the cover image (Ali *et al*., 2015). Abdelmgeid *et al*. (2016) proposed a method of hiding the secret message within the cover image using the Zero Order Hold (ZOH) (Abdelmged *et al*., 2016).

Ali *et al*. (2015) improved a technique to hide the secret message within RGB image by using the LSB algorithm and by first encrypting the secret message using the secret key transformation function. The key is randomly selected in the GF (2n) with the condition of having the inverse value to be used in the retrieving of the encrypted message. Only, two least significant bits are used in each pixel (only, the blue byte) to hide the secret message because the effect of the blue color on human eyes is weak (Ali *et al*., 2015).

MATERIALS AND METHODS

The alphabet A-Z, a-Z and all other symbols can be concealed using the proposed method, each one of the symbols and the alphabet will be first encoded using Ascii codes. The first bit of the secret message will be concealed within the first pixel of the cover image (RGB 24 bit JPEG image), so, there is no need to denote the beginning of the secret message bit stream in contrast to the end of the secret message bits must be recognized, the Ascii code "1111111" for the symbol "Del" will be added to the end of the secret message bit stream for this purpose.

Within the proposed method, the second step after encoding the secret text message using the Ascii code is the encryption of the secret message based on the X-OR between the encoded bit stream and the bits of the audio file (.wav). The audio file will be converted to binary bits, this audio file bits is considered as a key to encrypt the coded stream of the secret message, the length of this key is as the length of the text secret message bits. This step has the benefit of making the secret message not understandable to everyone who can get the secret message except the one (the recipient) who already has a knowledge about that audio file. The audio file is considered the first key used in the proposed method.

The second key is random variable sized segments used for distributing the secret message bits randomly throughout the cover image. The image will be divided into four parts, each two diagonal parts will be used at the same time (simultaneously) as shown in Fig. 1. Each part is a quarter of the cover image if the cover image size is n*m, so, each part size is n/2*m/2.

For each two diagonal parts, variable sized segments will be selected with a simple processing depending on two counter variables and the height and width of each part for the concealing of the secret bits. Four segments will be selected each time, two segments within each part

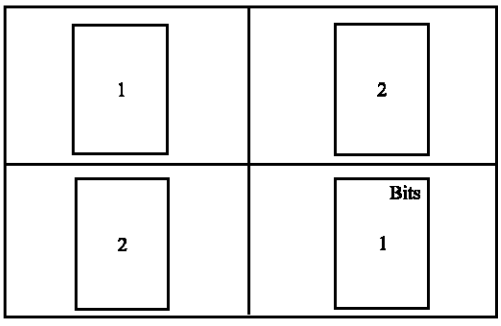

Fig. 1: The main parts of the cover image

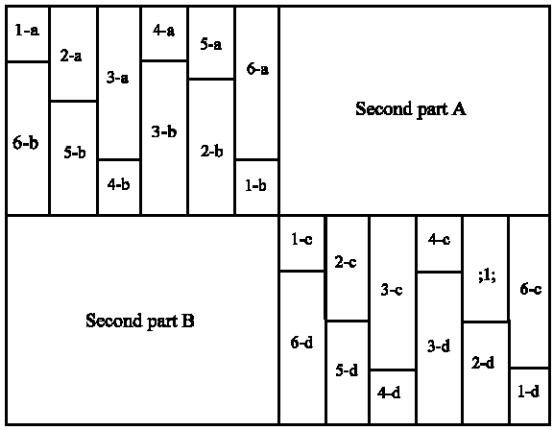

Fig. 2: Sample of the generated sized segments used in the proposed method

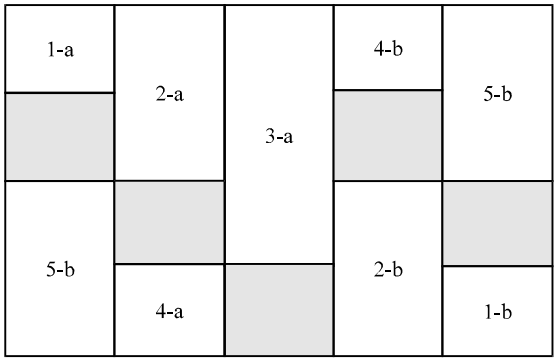

Fig. 3: Generated variable size segments used in the proposed method

as Fig. 2 shows where this figure demonstrate the generation of segments within a small piece of cover image proposed to be 10*12 pixels. At each time, segments labeled 1a-1d will be processed successively and so on. The segments' size is increased and decreased throughout the processing, this make the secret message undetectable unless the manner of generating the segments is known.

Depending on the cover image size, there may be some pixels that are not used as shown in Fig. 3 where each colored unlabeled block is unused. The third key used in the proposed method is the variable number of bits used with LSB insertion method for embedding the secret message bits. The manner of embedding the secret message bit is different from pixel to pixel.

The embedding and extracting processes are selecting four pixels within each step, so there are four cases for using LSB insertion method. 1st pixel_ LSB will not be used (the pixel will be passed without any processing):

- 2nd pixel→LSB (1-1-0) will be used
- 3rd pixel→LSB (0-1-2) will be used
- 4th pixel→LSB (2-0-1) will be used

The LSB (1-1-0) that applied to the 2nd selected pixel is done through concealing two secret bits, each one of these two bits will be concealed in the 8th bit of the red and green color bytes consecutively, while the LSB (0-1-2) that applied to the 3rd selected pixel is done by concealing three secret bits, two of these three embedded bits will be concealed in the 8th and 7th bits of blue color byte and the third bit will be concealed in the 8th bit of the green color byte. Finally, LSB (2-0-1) that applied to the 4th selected pixel is done by concealing three secret bits, two of these three embedded bits will be concealed in the 8th and 7th bits of red color byte and the third bit will be concealed in the 8th bit of the blue color byte. The proposed method will conceall byte from the secret message within 4 pixels of the cover image. The proposed method has two parts: embedding and extracting parts.

Embedding part: As Fig. 4 shows, this part has the following steps:

Step 1: Decide which cover image and audio file will be used.

Step 2: Coded the secret text message depending on the Ascii codes, adding the code "1111111" to the end of the stream of bits.

Step 3: X-OR this stream of secret message bits with the audio file bits.

Step 4: If the image size is n*m, so for each two parts (a two quarters of the image) and during the loop, find four pixels within the four segments as shown in Fig. 2 and applying the appropriate LSB insertion method:

$$j \rightarrow 1 \text{ to } m/4$$
$$i \rightarrow 1 \text{ to } j$$

- Pixel position within the 1st segment is: I (i, j) → this pixel will be passed without any processing
- Pixel position within the 2nd segment is: I (n/2-i+1, m/2-j+1). → apply LSB (1-1-0) to this pixel
- Pixel position within the 3rd segment is: I(n/2+i, m/2+j). → apply LSB (0-1-2) to this pixel
- Pixel position within the 4th segment is: I (n-i+1, m→j+1). → apply LSB (2-0-1) to this pixel

This loop will get all pixels within the four segments.

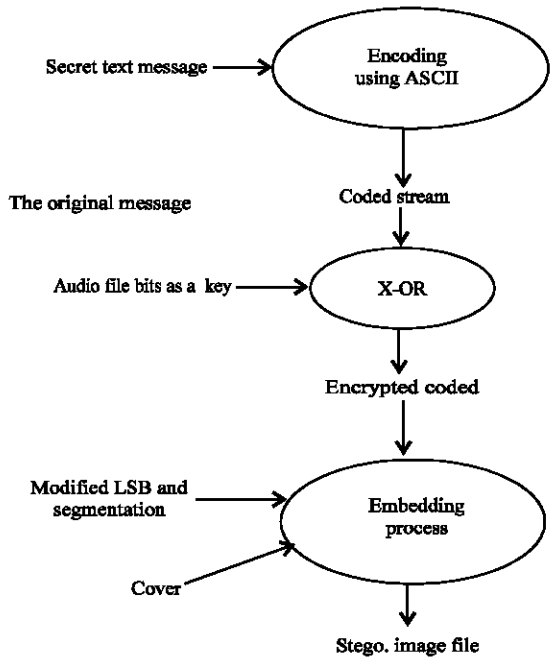

Fig. 4: The proposed steganography method: embedding part

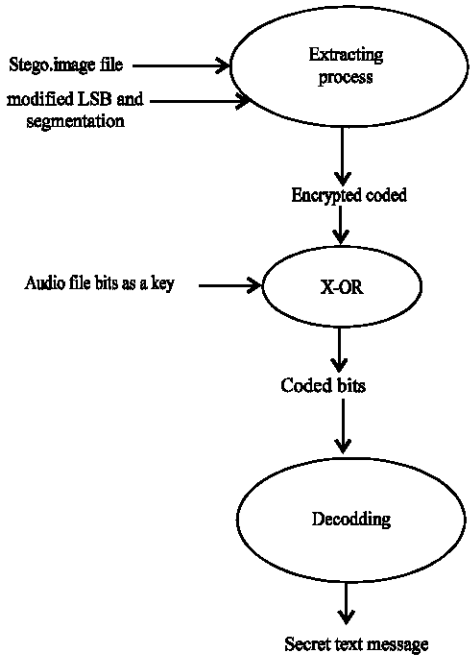

Fig. 5: The proposed steganography method: extracting part

Step 5: Repeat step 4 until the end of the secret encrypted message bit stream.

Extracting part: This part has the following steps as shown in Fig. 5:

Step 1: Get the stego image and the audio file.

Step 2: According to the loop discussed in the embedding part, pick each pixel within each segment and then apply the corresponding LSB to get the secret coded encrypted bits within each pixel.

Step 3: Repeat step 2 until the special ending code "1111111" is found.

Step 4: X-OR the retrieved coded encrypted secret message bits with the audio file bits to get the coded stream bits.

Step 5: Kccording to Ascii codes, get the original message.

RESULTS AND DISCUSSION

Since, the proposed method can conceal 8 secret bits within four pixels, the secret message size which can be concealed throughout the cover image is: (Image Height *Image width/4) this gives the number of concealed bytes of the secret text message and for getting the secret message size in Kelo Byte, it will be: (Image height* image width/4*1024).

When the proposed method (the variable sized segments and the modified LSB) is applied, the results are compared with the LSB (3-3-2) method by applying the same variable sized segments. The results showed that the proposed method has a less amount of embedded secret message bits, since, it conceals one byte within four pixels while the LSB (3-3-2) can hide one byte of secret message within each pixel.

As Eq. 1, PSNR used to check the similarity between the cover and the stego images. As the value of PSNR getting high, the quality of the steganography method is increased:

$$PSNR = 10\log_{10}\frac{(MAX)^2}{MSE} \quad (1)$$

where, MAX is the maximum value could be found for example for the double-precision image, MAX is 1 while MAX is 255 when the gray scale image is used, etc. MSE is the Mean Square Error and is computed as shown in Eq. 2:

$$MSE = \frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j)-K(i,j)\right]^2 \quad (2)$$

As Eq. 3 shows, AD is also, used to check the quality of the proposed method. When the value of the AD is small, the quality of the steganography method will be better:

Table 1: The comparison depends on the PSNR

	PSNR	
Cover image	LSB (3-3-2) insertionmethod	The proposed steganography method
Lena	37.67	59.88
Balloon	38.49	60.14

Table 2: The comparison depends on the AD

	AD	
Cover image	LSB (3-3-2) insertion method	The proposed steganography method
Lena	0.25	0.017
Balloon	0.14	0.021

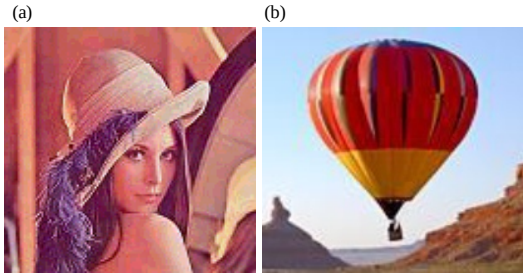

Fig. 6: a, b) Two cover image samples

$$AD = \sum_{i=1}^{m} \sum_{j=1}^{n} |I(i,j) - K(i,j)| \quad (3)$$

COR is a measurement used to ompare the similarity between the stego and the cover images as shown in Eq. 4:

$$COR = \frac{\sum (I(i,j)-v1)(K(i,j)-v2)}{\sqrt{\sum (I(i,j)-v1)^2}\ \sqrt{\sum (K(i,j)-v2)^2}} \quad (4)$$

where, m and n are the image's height and width, respectively. I(I, j) is the value of the original pixel within the cover image, K(i, j) is the value of the pixel after the insertion process within the stego image. v1 and v2 are the mean pixel value of the cover and stego image, respectively.

The proposed method had a better (higher) PSNR value than the LSB (3-3-2) since, it uses fewer bits within the LSB insertion method and using three pixels only and leave one without processing at each step. Table 1 depicts those results. Also, the proposed method has a better (smaller) AD value than the LSB (3-3-2) for the same reasons. Table 2 shows the results based on the value of the AD. COR will be better whenever it approximate to the value 1, Table 3 shows a comparison between the proposed method and the LSB (3-3-2). Figure 6 shows samples of the cover images while Fig. 7 shows the stego images depending on the proposed steganography method and Fig. 8 shows the stego images depending on the LSB (3-3-2) with the same proposed segmentation.

Table 3: The comparison depends on the COR

	COR	
Cover image	LSB (3-3-2) insertionmethod	The proposed steganography method
Lena	0.793	0.945
Balloon	0.817	0.971

Fig. 7: a) The stego images based on the proposed segmentation and b) The proposed LSB insertion method

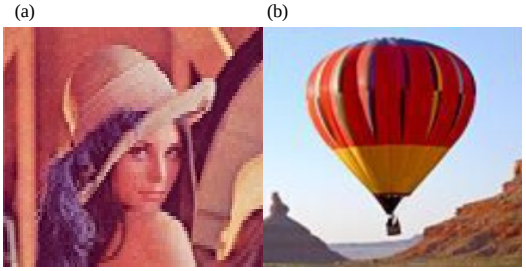

Fig. 8: a) The stego images based on the proposed segmentation and b) The LSB (3-3-2) insertion method

CONCLUSION

This study develops a steganography, method that conceals a text message within a cover image. Since, the secret message is first encrypted using the X-OR with an audio file where only the sender and the recipient know it, the proposed steganography method is considered robust against the attacker. This increases the security feature whereas if the message is extracted, it will have no mean, since, it is encrypted.

Throughout using the proposed method, it is difficult to predict the position of the secret message, since, it is concealed in randomly distributed different sized segments, this also, make the proposed steganography method robust against the attackers. Different number of bits is used within the LSB insertion method, this also, make it difficult to retrieve the secret embedded message. Where LSB (1-1-0), LSB (0-1-2) and LSB (2-0-1) are used within three random pixels and the fourth pixel is passed without any processing.

Simplicity that depends only on the image's size and two counter variables is the feature that makes the

proposed steganography method differs from many other methods that generate segments, so, the proposed method take less time to embed and extract the secret text messagebut in the same time is considered robust, since, it distributes the secret message throughout the image randomly and since, it encrypts the secret message before the embedding process, it considered more secure.

Because the proposed method imbeds only one byte within each four random selected pixels, the impact on the original image is considered small, so, the stego image has a good PSNR, COR, AD values.

REFERENCES

Abdelmged, A.A., S.S. Al-Hussien and N. Hussien, 2016. A technique of image steganography using parity checker and LSBraille. Intl. J. Comput. Appl., 144: 37-41.

Abdelmgeid, A.A., A.A. Tarek, S.S. Al-Hussien and M.H. Shaimaa, 2016. New image steganography method using zero order hold zooming. Intl. J. Comput. Appl., 133: 27-31.

Adil, A.R., 2015. Text steganography to border image using novel method. Appl. Math. Sci., 9: 3087-3096.

Al-Asadi, S.A. and W. Bhaya, 2016. Text steganography in excel documents using color and type of fonts. Res. J. Appl. Sci., 11: 1054-1059.

Al-Shatanawi, O.M. and N.N. El-Emam, 2015. A new image steganography algorithm based on Mlsb method with random pixels selection. Intl. J. Network Secur. Appl., 7: 37-53.

Ali, N.H.M., A.M.S. Rahma and A.S. Jamil, 2015. Text hiding in color images using the secret key transformation function in GF (2 n). Iraqi J. Sci., 56: 3240-3245.

Bandyopadhyay, D., K. Dasgupta, J.K. Mandal and P. Dutta, 2014. A novel secure image steganography method based on Chaos theory in spatial domain. Intl. J. Secur. Privacy Trust Manage., 3: 11-22.

Bansod, S. and G. Bhure, 2014. Data encryption by image steganography. Intl. J. Inf. Comput. Technol., 4: 453-458.

Bawaneh, M.J. and A.A. Obeidat, 2016. A secure robust gray scale image steganography using image segmentation. J. Inf. Secur., 7: 152-164.

Hamid, N., A. Yahya, R.B. Ahmad and O.M. Al-Qershi, 2012. Image steganography techniques: An overview. Intl. J. Comput. Sci. Secur., 6: 168-187.

Kaul, N. and M. Chandra, 2015. A proposed algorithm for text in image steganography based on character pairing and positioning. Intl. J. Comput. Appl., 126: 19-22.

Khan, I., S. Gupta and S. Singh, 2016. A new data hiding approach in images for secret data communication with Steganography. Intl. J. Comput. Appl., 135: 9-14.

Tayel, M. and H. Shawky, 2014. A proposed assessment metrics for image steganography. Intl. J. Cryptography Inf. Secur., 4: 1-11.