AENSI Journals

Advances in Environmental Biology

ISSN-1995-0756 EISSN-1998-1066

Journal home page: http://www.aensiweb.com/aeb.html

The Use of Image Edges and Chaotic Logistic Map in Steganography

[1]Mitra Daneshmand and [2]Ali Broumandnia

[1]Software engineering department, South Tehran branch, Islamic Azad University, Tehran, Iran.
[2]Faculty member in department of software engineering, South Tehran branch, Islamic Azad University, Tehran, Iran.

ARTICLE INFO

Article history:
Received 11 June 2014
Received in revised form 25 July 2014
Accepted 20 August 2014
Available online 20 September 2014

Keywords:
Image Steganography; Cryptography; Chaotic Logistic Map; LSB Replacement; EA-LSBMR

ABSTRACT

Steganography as a data hiding science into varied media is implemented in different ways. Also, there are loads of algorithms for carrying out image steganography. Their common goal is protecting hidden information against attackers. Moreover, achieving to it requires performing the process according to a manner in which both image quality is kept as possible and resistance against information detection invades is prepared. This paper proposes a method based on chaotic maps in steganography. Furthermore, to ensure the confidentiality, steganography and cryptography are combined together. Steganography is performed in the pixels locating in the edges of the carrier image. Thus, in addition to those significant aims said, this method executes data embedding very quickly.

To Cite This Article: Mitra Daneshmand, Ali Broumandnia, The Use of Image Edges and Chaotic Logistic Map in Steganography. ***Adv. Environ. Biol., 8(11),*** *189-194, 2014*

INTRODUCTION

Nowadays, information security field is considered the most. So, as a main focus of research's subjects, different algorithms have been investigated in this area.

Steganography is a frequent mechanism for hiding information into a digital cover media such as text, image, voice, and video. There is a very close relationship between steganography and cryptography. Albeit, there is a vital difference. Cryptography's aim is modifying a message in a form which is ambiguous for others and it is not important to discover existence the message. Put it another way, with encrypting the message, everyone can understand that two sides have an arcane communication together. In spite of the fact that steganography intends to conceal the secret message pursuant to a way in which nobody can be aware of its existence. In other words, steganography hides the existence of a secret message. Actually, this technique is based on the weakness being in the human sense such as the human visual system (HVS).

However, both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques. [1]

This paper has been prepared to hide text messages inside image files. To achieve this aim, there are several methods. The easiest and the most popular present one is steganography using Least Significant Bits (LSB) replacement mechanism. In this approach, the bits of the message are embedded directly into least significant bit plane of the cover image in a deterministic sequence. These modifications applied to image have not seen apparently by the human eyes. To hide a message inside an image file, a proper cover image is required. Because this technique uses the bits of pixels in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

When the character A which binary value equals 01000001, is inserted, the following grid results:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001001 00100110 11101001)

Corresponding Author: Mitra Daneshmand, Software engineering department, Islamic Azad University, South Tehran branch, Tehran, Iran.
E-mail: daneshmand_mitra@yahoo.com

The changes made to the least significant bits are too small to be recognized by the human visual system, so the message is effectively hidden.

In this paper, image steganography has been done by LSB replacement method in the pixels locating in its edges. With utilizing the chaotic logistic mapping in two phases including the encryption the binary data stream of the secret information and indicating the target pixels for embedding, security has been increased apparently. Also, this selection way has provided better quality for the carrier image.

Related Works:

Article [2], in steganography based on EA-LSBMR (Edge Adaptive-LSB Matching Revisited), selecting the embedding regions has been implemented according to the size of secret message and the difference between two consecutive pixels in the cover image. The difference between [3] and previous theory is in selection region determined for embedding message. In this paper those areas are some blocks. In this approach the visual quality is kept better than EA-LSBMR in higher embedding rates. [4] by using the chaotic logistic map in BPCS (Bit-Plane Complexity Segmentation Steganography) model and changing threshold employed in this model, not only provides good visual imperceptibility also increases data embedding capacity. Such as the last paper, for encrypting the secret message, article [5] uses the chaotic map and asymmetric encryption algorithm RSA, too. Then encrypted text is hidden into the carrier image. As a consequence, both provides good visual imperceptibility and increases data embedding capacity. In [6] first of all, by using the chaotic logistic map, the secret text has been encrypted. After compressing the image color range using Fuzzy logic compressor, the encrypted text has been embedded into the image.

In most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security. LSB matching (LSBM) is a bit different from LSB replacement method. LSBM employs a minor modification to LSB replacement. If the secret bit does not match the LSB of the cover image, then +1 or -1 is randomly added to the corresponding pixel value. Statistically, the probability of increasing or decreasing for each modified pixel value is the same and so the obvious asymmetry artifacts introduced by LSB replacement can be easily avoided. Therefore, the common approaches used to detect LSB replacement are totally ineffective at detecting the LSBM. Up to now, several steganalytic algorithms have been proposed to analyze the LSBM scheme. Unlike LSB replacement and LSBM, which deal with the pixel values independently, LSB matching revisited (LSBMR) uses a pair of pixels as an embedding unit in which the LSB of the first pixel carries one bit of secret message, and the relationship (odd–even combination) of the two pixel values carries another bit of secret message. In such a way, the fewer modification rate of pixels can be applied to the cover image at the same payload compared to LSB replacement and LSBM. It is also shown that such a new scheme can avoid the LSB replacement style asymmetry, and thus it should make the detection slightly more difficult than the LSBM approach based on our experiments. [2, 7]

EA-LSBMR is a technique providing a higher level of security in comparison to the others mentioned above. The superiority of EA-LSBMR is reflected in selecting embedding regions adaptively by considering the image content and the secret message length. In other words, in the lower embedding rate, the sharper regions are released adaptively, while the smooth regions remain unchanged. Thus good image quality and relatively high security are achieved by this steganographic method. However, based on our analysis and experiments, with the increasing of embedding rate, the visual quality descends inevitably, and some evidences appear in the Discrete Fourier Transform (DFT) spectrum of the pixel-pairs differences histogram. [3]

The Conversion of Text Information:

The meaningful text messages need to be translated into encrypted binary data stream. The data stream is used for the embedding of carrier image. The conversion is shown as Fig. 1.

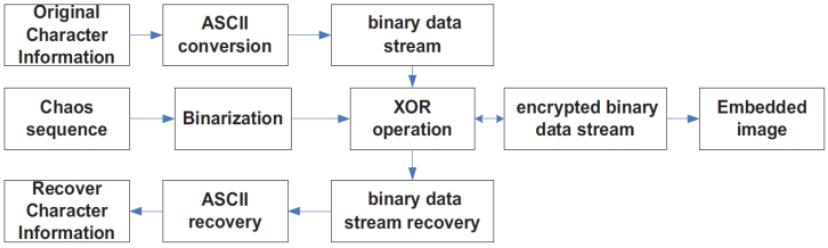


Fig. 1: The conversion of text data information [4, 5, 8]

Advances in Environmental Biology, 8(11) Special 2014, Pages: 189-194

Chaos Theory:

Chaos is a kind of behavior about nonlinear dynamics law control. This paper adopts Logistic mapping method to generate chaotic sequence:

$$X_{n+1} = r.X_n(1 - X_n) \quad (1)$$

This function with initial value $X_0 \epsilon (0, 1)$ and $r=3.877$ (as a control parameter or a bifurcation parameter) creates a data stream that has random-like behaviors. As a major characteristic of this function, its deterministic performance can be pointed. However, as this signal has a random noise behavior, by knowing the chaotic map type and its initial value, the data set liking random noise stream always can be regenerated again. [4, 5, 8] This feature is much more fruitful in steganography process to provide the higher level of security and carry out the reverse of that to retrieve the hidden message.

The new binary sequence generated by the chaotic logistic map has two main functions in this paper:

1. It is used to encrypt text data information, which can enhance the security of the steganography.
2. It is used to select the target pixels for hiding the secret information.

Proposed Method:

The generated binary sequence from the secret information, will be concealed into pixels existing in the edges of the cover image. In order to that, with Canny function we attempt to identify those pixels. Because this algorithm is not susceptible to noise interference, it is able to detect true weak edges, too. [9]

In this step, the target pixels will be specified to embed the bits of the message into their LSB. Hence, we use the chaotic logistic map. To achieve more security, a key of 80 bits long is utilized for generating the initial value of the function. This key can be defined in ASCII code as below:

$k=k_0, k_1, \ldots, k_9$ *(ASCII)* (2)

Where k_i determines a block of 8 bits long of the key. We convert the key into binary format:

$$k = \begin{pmatrix} k_{01}, & k_{02}, & k_{03}, & k_{04}, & k_{05}, & k_{06}, & k_{07} \\ ,k_{08}, & \ldots\ldots & , & k_{91}, & k_{92}, & k_{93} & \\ ,k_{94}, & k_{95}, & k_{96}, & k_{97}, & k_{98} & (Binary) & \end{pmatrix} \quad (3)$$

The initial value derived from (4):

$$X_0 = \begin{pmatrix} k_{01} \times 2^{79} + k_{02} \times 2^{78} + \\ \ldots\ldots \\ k_{11} \times 2^{71} + k_{12} \times 2^{70} + \\ \ldots\ldots \\ k_{n7} \times 2^1 + k_{n8} \times 2^0 \end{pmatrix} \Big/ 2^{80} \quad (4)$$

In a proper method, the key space should be large enough to make the brute force attack infeasible. The proposed method has 2^{80} different combinations of the secret key. An image steganography with such a long key space is sufficient for resistance versus these such attacks. [11]

We divide the cover image into *32×32* bits blocks to dedicate the numbers derived from the logistic map function to their corresponding pixels. The function output has been extended into the blocks in homogeneous matrixes form and used as a pattern to find the embedding units. Finally, the intersection points from image edges and each block edges are determined as the target pixels on the original image.

As a consequence, the bits of the secret information are inserted into the LSB of color pixels and the carrier image containing the bits of the secret message is constructed.

Analyzing and Evaluating The Proposed Method:

In this method the image of Lena with a size of *512×512*, from standard image database in image processing field, has been used. As mentioned previously, to select the target pixels in the chaotic logistic map, parameter *r* has been set equal to *3.877*. This control parameter plays a significant role in affecting entropy amount of the attained numbers. So, this value gives the results with a high quantity of the entropy. Fig. 2 demonstrates two diagrams showing the noise like behavior of this signal in 1024 first iteration.

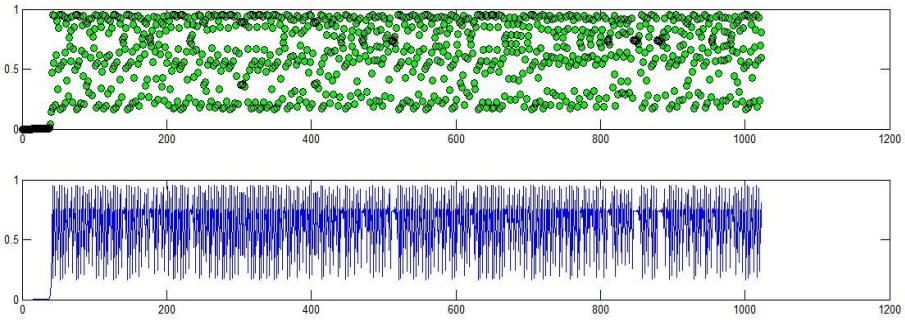


Fig. 1: The noise like behavior of the logistic map signal in 1024 first iteration

It would be clear that such an entropy amount makes impossible detecting the modified pixels without having the secret key and increases the security of the steganography process.

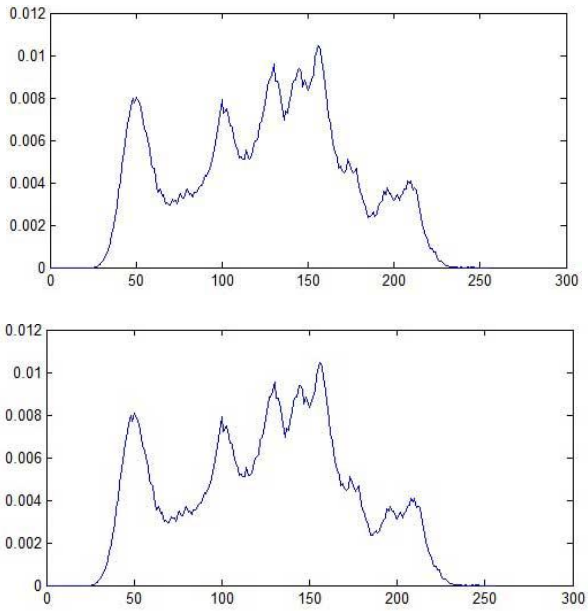
As a quantity assessment of the proposed method, three parameters have been presented including embedding time, Peak Signal to Noise Ratio (PSNR), and the DFT spectrum of pixel-pairs differences between histograms. PSNR is calculated using the Mean Square Error (MSE). The quantifiers are defined as follows:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) dB \quad (5)$$

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - y_{ij})^2 \quad (6)$$

Where M, N are the horizontal and vertical pixels of the cover image, x_{ij} and y_{ij} are the pixel values in the cover and the stego image respectively. In (6), constant value *255* signifies the maximum value that a color may hold in a pixel having a color depth of 8 bits. For 24-bit RGB images, each color component has a color depth of 8 bits. Higher PSNR value indicates better fidelity of the stego image in which enforced lower distortion.

Fig. 3 illustrates the image histograms before and after embedding the bits of the message into the LSB of the image pixels. By utilizing the proposed method in the image of Lena, 54112 bits of the message has been inserted in 0.67 seconds. Although, in EA-LSBMR method in case of the same image file, 60128 bits of the message has been inserted in 2.76 seconds. In the proposed method, DFT spectrum of pixel-pairs differences between histograms equals to 0.05. In terms of image quality, the result concluded before and after executing this program can be investigated in Fig. 4.



(a)

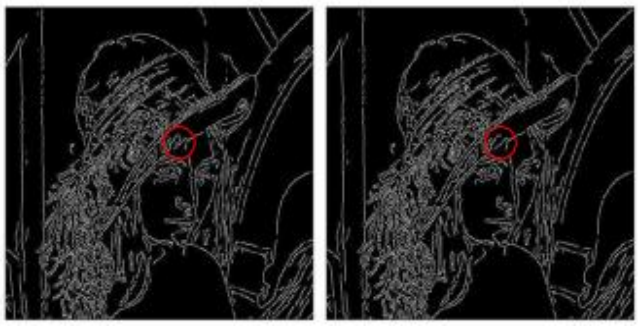
(b)

Fig. 2: The image histograms before (a) and after (b) implementing steganography

(a) (b)

Fig. 3: The original image (a) and the carrier image (b)

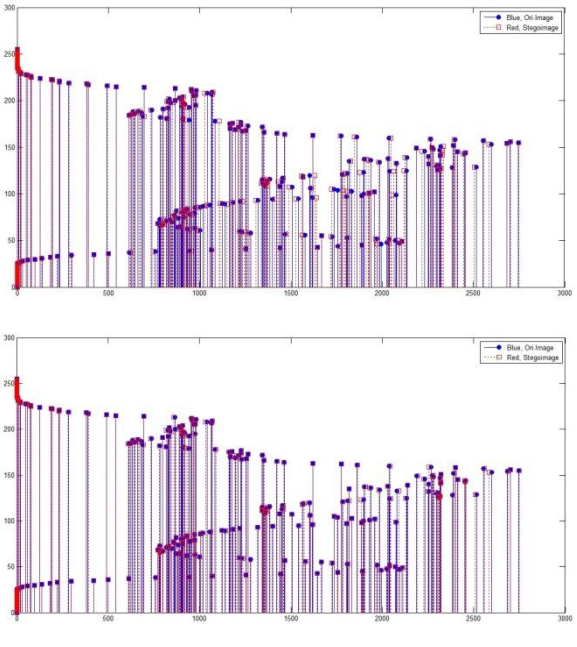
Detected edges from the original and carrier images has been shown in Fig. 5. Additionally, a sample of pixels locating in the original image and the corresponding pixels modified in the stego image has been indicated by two circles to have a better comparison between effects.



(a) (b)

Fig. 4: Detected edges from the original (a) and carrier images (b)

To demonstrate the differences between pixel-pairs values before and after embedding process, Fig. 6 shows both Stem diagrams regarding two methods. Obviously these values are more accordant in our method.



(a)

(b)

Fig. 5: The Stem diagrams regarding EA-LSBMR (a) and the proposed method (b)

Table 1 lists the results derived from two pointed ways applied to some standard images.

Table 1: the comparative parameters between two methods for varied images

Methods	Proposed Method					EA-LSBMR				
	PSNR	*DFT*	*Time*	*Edges*	*Capacity*	*PSNR*	*DFT*	*Time*	*Edges*	*Capacity*
Lena	68.75	0.05	0.67	15216	54112	62.31	0.26	2.76	22549	60128
Macaw	68.94	0.22	0.65	14478	51488	62.47	2.77	2.65	21402	57072
F16	69.02	0.04	0.63	14394	51168	62.56	0.19	2.62	21271	56720
Pepper	69.64	0.04	0.54	12391	44064	63.2	0.19	2.17	18254	48672

Conclusions:

In this paper, image steganography has been done by using the chaotic logistic map and the pixels locating in its edges. With utilizing this mapping in two phases including the encryption the binary data stream of the secret information and indicating the target pixels for embedding, security has been increased apparently. Also, this selection way has provided better quality for the carrier image.

The comparisons accomplished with EA-LSBMR algorithm indicates that our method hides the secret message in a faster and more secure manner with the same embedding rate.

It goes without saying that because of the selection way in which the target pixels are indicated, the embedding rate decreases. Future work will develop a considerable attention to extend the proposed method for higher order bits in the image planes to compensate for the capacity shortfall.

REFERENCES

[1] Nosrati, M., R. Karimi, M. Hariri, 2011. "An Introduction to steganography methods", World Applied Programming, I: 3
[2] Sivaranjani, S. Sara mani, 2011. "Edge Adaptive Image Steganography Based On LSB Matching Revisited", Journal of Computer Applications (JCA), Vol. IV, Issue 1.
[3] Huang, W., Y. Zhao, R.R. Ni, 2011. "Block-Based Adaptive Image Steganography Using LSB Matching Revisited", Journal of Electronic Science and Technology, IX,(4).
[4] Shi, P., Zh. Li, T. Zhang, 2010. "A Technique of Improved Steganography Text Based on Chaos and BPCS", Advanced Computer Control (ICACC), 2010 2nd International Conference, II.
[5] Rudramath, P.R., Prof. M.R. Madki, 2012. "High Capacity Data Embedding Technique Using Improved BPCS Steganography", International Journal of Scientific and Research Publications, II: 7.
[6] TayeJ, M., H. Shawky, A. EI-Din Sayed Hafez, 2013. "A Hybrid Chaos- Fuzzy -Threshold Steganography Algorithm for Hiding Secure Data", ICACT Transactions on Advanced Communications Technology (TACT), II: 1.
[7] Luo, W., J. Huang, 2010. "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transaction on Information Forensics and Security, V(2).
[8] Khairnar, P.P., Prof. V.S. Ubale, 2013. "Steganography Using BPCS Technology", International Journal of Engineering and Science, III: 2.
[9] Bin, L., M. Samiei Yeganeh, 2012. "Comparison for Image Edge Detection Algorithms", IOSR Journal of Computer Engineering, II(6).
[10] Jabbar Altaay, A.A., Sh. bin Sahib, M. Zamani, 2012. "An Introduction to Image Steganography Techniques", Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference.
[11] Pareek, N.K., V. Patidar, K.K. Sud, 2006. "Image encryption using chaotic logistic map", Image and Vision Computing, www.sciencedirect.com.