Image Hiding Using Logistic Map Chaotic Function

Mehdi Alirezanejad[1*]

Abstract–Steganography is the action of hiding a secret message within another cover message. The secret message and the cover image can be text, image, voice even signal. In this article an image is used as the secret message while the cover message is also a gray level image. This paper proposes a new method of steganography based on logistic chaotic maps. This function is used to determine the position of different bits of the secret image in the covering image. The main advantage of the proposed method is that the pixels of the secret image in the covering image is uniformly distributed, which increases the robustness of the proposed method to common attacks. The robustness and performance of the proposed method against common attacks in the area of steganography including corruption, clipping, and noise is tested. The high PSNR of the proposed method (about 45) expresses the high performance of the proposed method.

Keywords: Image Hiding, Secret Image, Cover Image, Chaotic Function

1. Introduction

Steganography, as a new type of covert communication technology, is mainly used to conceal a message by hiding its very existence[1]. Data security on the Internet is becoming increasingly important due to the digitalization of data and the networking of communications. Since the Internet is an open channel of communication, it can be tampered with, intercepted and altered. For this reason, steganography offers different approaches for transmitting secret messages. The most common and well-known method of steganography, called least significant bit (LSB) spoofing, allows to infiltrate secret data by directly replacing a k LSB pixel with k secret bits[2]. A number of optimized LSB methods have been proposed to improve this problem. In 2003, Wu and Tsai proposed a new reduced method which uses the value of the difference of two neighboring pixels to determine the number of secret bits to embed[3]. A wavelet-based method was also proposed, which sequentially places pixels of the secret image in the cover image. Its drawback is vulnerability to slice attacks[4]. In recent years, more and more attention has been paid to methods that allow pixels to be placed homogeneously[5-7].

In this paper, we propose a method to uniformly distribute the pixels of the secret image over the cover image based on a chaotic function. In particular, the chaotic property of the logistic function is used to determine the position of each pixel in the secret image. Experimental results show the robustness of our method to common attacks.

The rest of this paper is organized as follows. First, the logistic function and its features are discussed, and then the proposed method is described. Finally, experimental results and conclusions are presented.

1.1 Logistic map

The list of references is headed “References” and is not assigned a number. The list should be set in small print and placed at the end of your contribution, in front of the appendix, if one exists. Please do not insert a page break before the list of references if the page is not completely filled. An example is given at the end of this information sheet. For citations in the text please use square brackets and consecutive numbers: [1], [2], [3].

A logistic map is a nonlinear polynomial dynamic equation that can produce incredibly chaotic results[8-10]. Mathematically, the logistic mapping (function) is denoted

[1*] **Correspoding Author:** Department of Computer Engineering, Firoozkooh Branch, Islamic Azad University, Firoozkooh, Iran.Email:me.alirezanejad@gmail.com

Received: 2022.10.12; Accepted: 2022.12.03

by equation (1), where R is usually chosen to be [0,4] and in this study is taken to be 3.99. In addition, x_n is a random number in [0,1]. The dynamic behavior of the logistic mapping function over 500 iterations for R=3.99 and X_n=0.3 is shown in Figure 1[8, 11] .

$$x_{n+1} = Rx_n(1 - x_n) \qquad (1)$$

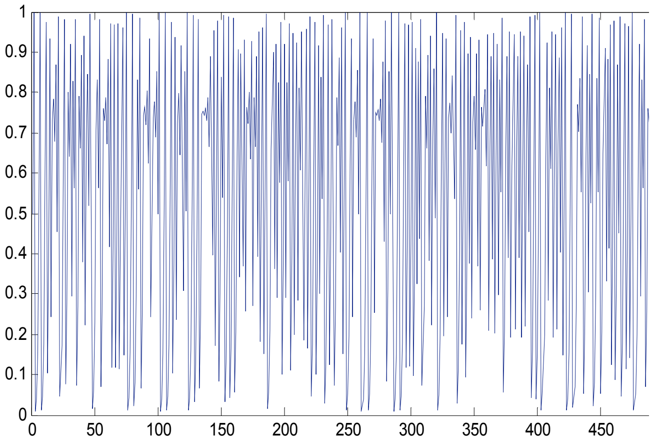


Fig. 1. Logistic map for $R = 3.99$ and $X_0 = 0.3$ regarding 500 iterations

2. Proposed methodology

2.1 General description:

The gray level of each pixel in the secret image is converted into binary mode. The position of each pixel in the covering image is then determined using a logistic map. The three least significant bits (LSBs) of the selected pixel are selected to hide the pixel in the secret image.

2.2 The detailed description:

An 80-bit key is used to determine the initial value of the Mackey-Glass series. This key is described in ASCII format as follows

represents an 8-bit block of the aforementioned key. The key is converted to binary numbers using equation (3).

K_(i=0,j=1,...,8),K_(i=1,j=1,...,8),...,K_(i=9,j=1,...,8) (3)

where - the j-th bit of the i-th key block.

The initial value is calculated as follows

X_0=(〖k_0,1〗 ^9+ 〖k_1,1〗 ^8+ 〖k_1〗 ^7+⋯+ 〖k_9,1〗 ^0) /2^10 (4)

where X_0∈[0,1].

Step 1: The series shown in Equation 5, obtained after binarizing one pixel of the secret image.

B= B_7,B_6,B_5,B_4,B_3,B_2,B_1,B_0 (binary) (5)

Convert all the pixels of the secret image to binary code and arrange them sequentially.

Step 2: Create a new value for the Mackie glass using equations (1) and X0.

Limitation: If the created value is not within the specified range, the new value is created anew.

Step 3: In this step, a pixel is selected from the hidden image to hide the bits of that pixel in the secret image using a logistic mapping. Equations (6,7) are used to determine the position of this pixel [12].

$$R_{\text{Cover\_Image}} = \text{round}(X_i \times R_L) + 1 \qquad (6)$$
$$C_{\text{Cover\_Image}} = \text{round}(X_i \times C_L) + 1 \qquad (7)$$

Where R_(Cover_Image) and C_(Cover_Image) are the positions of pixel rows and columns in the covering image, and R_L and C_L are the number of rows and columns in the covering image respectively.

Step 4. In this step, the 3 bits of the secret image are replaced with the younger 3 bits of the covering image in the corresponding positions of rows and columns R_(Cover_Image) and C_(Cover_Image) obtained in step 2.

Step 5. Carry out steps 2-4 for all pixels of the secret image, considering the following constraints.

Restrictions If a pixel is already selected in step 3, it should be ignored.

3. Experimental Results

In this section, the robustness of the proposed method to common attacks is evaluated using experiments.

3.1 Resistance to cover image corruption

In addition, common attacks on stego images using the proposed method are investigated. There are three common attacks on stego images: corrupted images, cropped images, and noisy images.

Fig. 3 shows the robustness of the proposed method with the secret image (64×64) and Cover image (800×600) shown by Lena and AliBorna in Fig. 2 and Fig. 3, respectively.

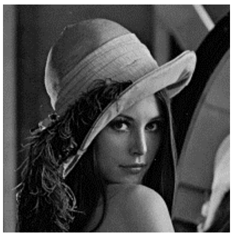
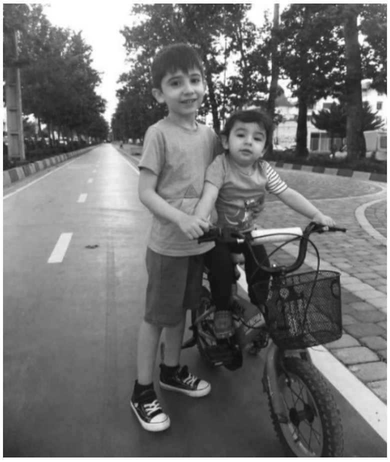


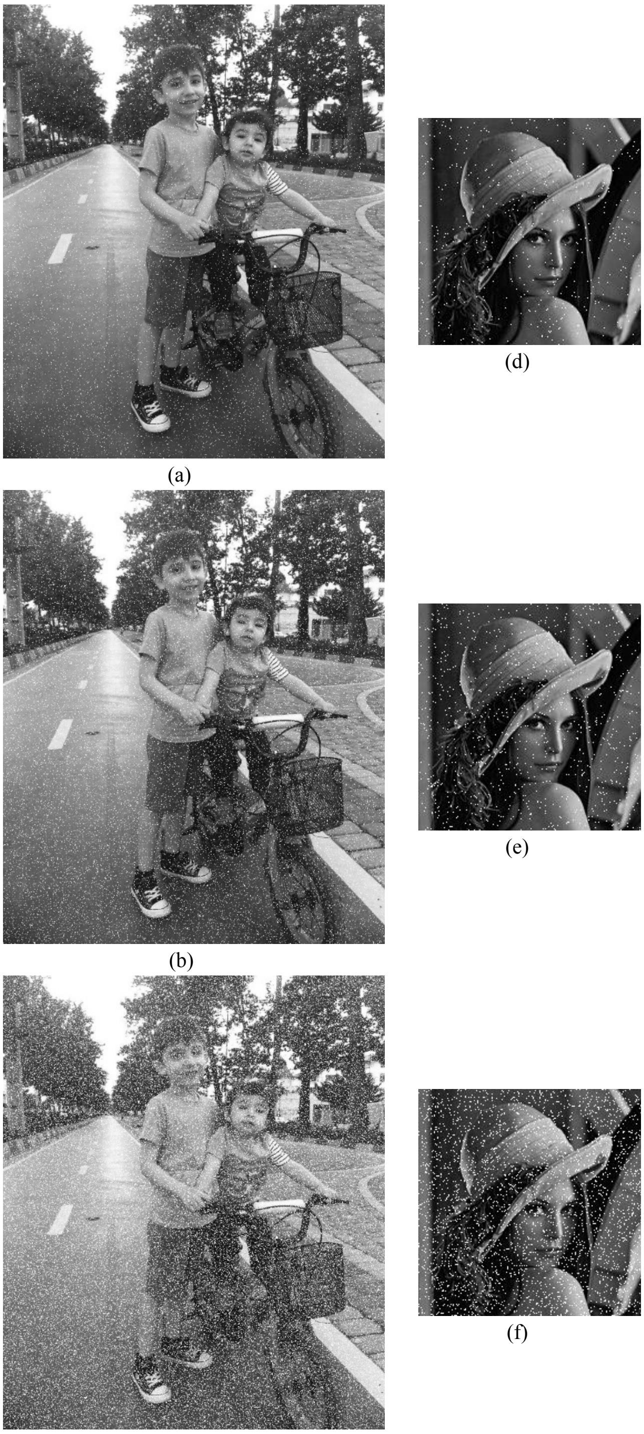
Fig. 2. Secret Image



(b)

Fig. 3. Cover Image

Figures 4, 5, and 6 (a.b.c) are the resulting images of Firura 3.a in Fig. 3b with hiding. The proposed method applies 5, 10, and 30% noise, 5, 10, and 30% clipping, and 5, 10, and 30% distortion, respectively. Figures 4d.e.f., 5d.e.f., and 6d.e.f. show the results of extracting the secret image from the cover image. Figures 5.d.e.f. and 6.d.e.f. show the resulting images of extracting the secret image from the cover image. It can be seen that even if the details of the original image are damaged during the secret image extraction, it does not affect the recognition of the secret image. The main reason for this stability is the uniform pixel distribution of the secret image in the cover image.



(a) (b) (c) (d) (e) (f)

Fig. 4. (a,b,c) Stego-Image after 5%,10%,30% noise (d,e,f) Secret Image after extracing from Stego-Image

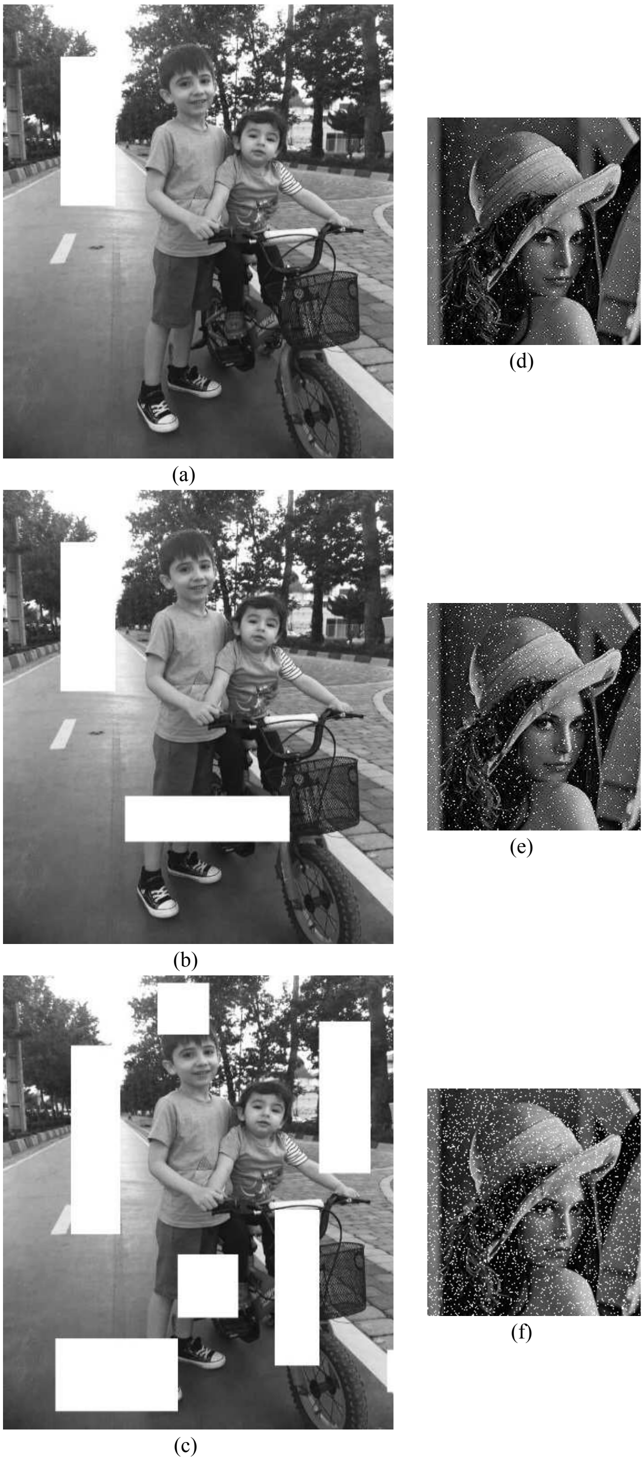


Fig. 5. (a,b,c) Stego-Image after 5%,10%,30% cutting
(d,e,f) Secret Image after extracting from Stego-Image

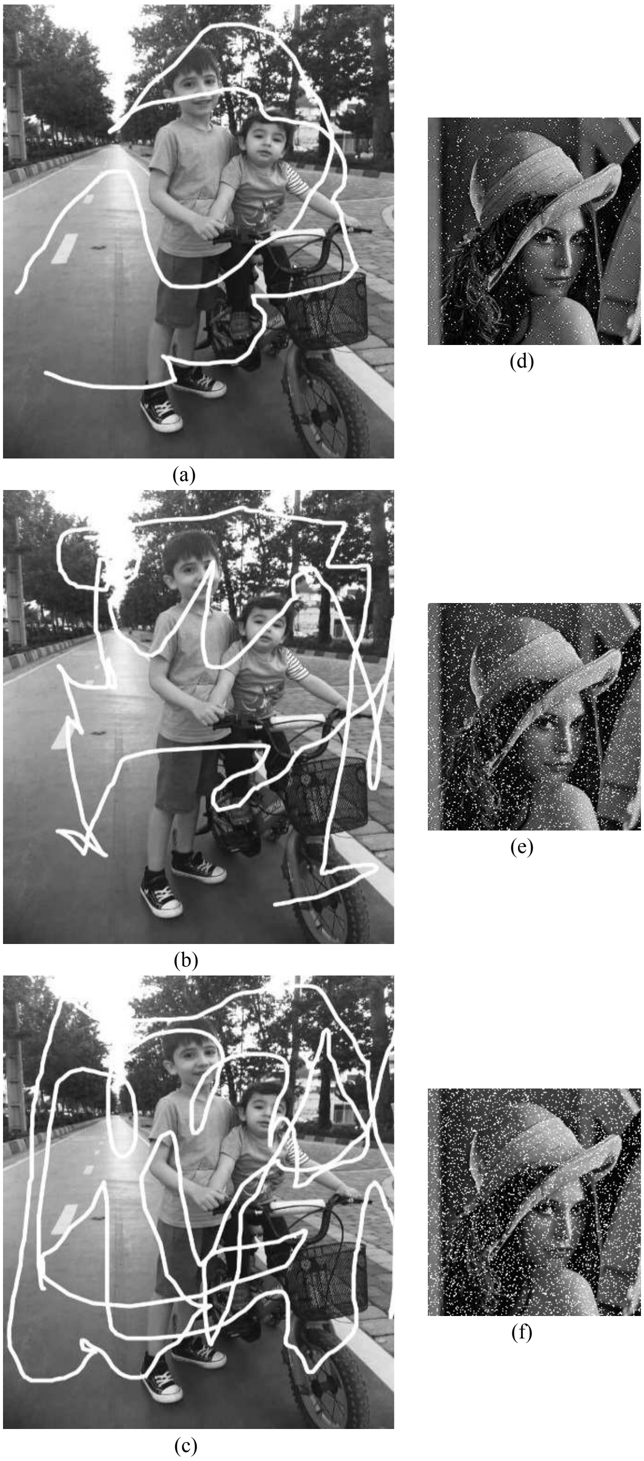


Fig. 6.(a,b,c) Stego-Image after 5%,10%,30% corrupted
(d,e,f) Secret Image after extracting from Stego-Image

3.2 Peak Signal to Noise Ratio

PSNR is used to scale the quality of Stego-image[13, 14]. PSNR can be explained as follows.

$$PSNR = 10 * \log_{10}\left(\frac{255^2}{\frac{1}{W*H}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(O_{ij} - D_{ij}\right)^2} \right) \quad (8)$$

In the above equations, H and W represent the gray level of pixels in the main and stego images, respectively; H and W are image height and width; H and W are image height and width.

To measure the PSNR of the proposed method, four images - Lena, Lena, AliBorna, Boat, and Tree - were used as 800*600 covering images, and these four 64*64 images were used as secret images. The results are shown in tabel 1.

Tabel 1. PSNR for the proposed method

	Lena	AliBorna	Boat	Tree
Lena	37.53	41.68	43.94	41.75
AliBorna	39.86	44.35	44.26	38.31
Boat	40.81	38.09	42.66	36.18
Tree	42.17	40.29	45.90	44.40

To compare the PSNR of the proposed method with other methods, four images of plane, house, green pepper and boat of size 800*600 are used as secret images. In addition, a 64*64 image of Lena was used as a cover image. As shown in Table 2, the proposed method compares well with the results of other methods and shows better results in most cases.

Table 2. Compare other methods with proposed method

Secret Image	Ref [15]	Ref [16]	Ref[17]	Proposed Method
Baboon	40.12	39.83	43.89	44.77
House	42.03	42.92	40.83	43.16
Painter	38.80	41.72	43.58	42.69
Girl	40.51	40.48	44.10	45.26

4. Conclusion

This paper proposes a new method of steganography. The main idea of the method is to determine the pixel position of the secret image using logistic mapping. The main advantage of the proposed method is that the distribution of pixels of the secret image in the covering image is uniform. The security of the method is also improved by embedding a key bit in each bit of the secret image before hiding the image.

As shown in the results section, the above features increase the robustness of the proposed results against common attacks. The high PSNR of about 45 also proves the effectiveness of the proposed method.

References

[1] R. Enayatifar, F. Mahmoudi, K. Mirzaei, Using the Chaotic Map in Image Steganography, 2009 International Conference on Information Management and Engineering, 2009, pp. 491-495.

[2] H.E. Rostam, H. Motameni, R. Enayatifar, Privacy-preserving in the Internet of Things based on steganography and chaotic functions, Optik, 258, (2022), 168864.

[3] H.S. Kwok, W.K.S. Tang, A fast image encryption system based on chaotic maps with finite precision representation, Chaos, Solitons & Fractals, 32(4), (2007) 1518-1529.

[4] A. Abdelwahab, L. Hassaan, A discrete wavelet transform based technique for image data hiding, 2008.

[5] H. Sajedi, Steganalysis based on steganography pattern discovery, Journal of Information Security and Applications,Vol. 30 ,(2016) ,3-14.

[6] P.C. Mandal, I. Mukherjee, G. Paul, B.N. Chatterji, Digital image steganography: A literature survey, Information Sciences ,609 ,(2022) 1451-1488.

[7] I.J. Kadhim, P. Premaratne, P.J. Vial, B. Halloran, Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research, Neurocomputing, 335, (2019) ,299-326.

[8] A.H. Abdullah, R. Enayatifar, M. Lee, A hybrid genetic algorithm and chaotic function model for image encryption, AEU - International Journal of Electronics and Communications, 66(10), (2012), 806-816.

[9] H. Ghanbari, R. Enayatifar, H. Motameni, Chaos-based image encryption using hybrid model of linear-feedback shift register system and deoxyribonucleic acid, Multimedia Tools and Applications (2022).

[10] R. Enayatifar, A.H. Abdullah, I.F. Isnin, Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, Optics and Lasers in Engineering, 56, (2014), 83-93.

[11] R. Enayatifar, A.H. Abdullah, I.F. Isnin, A. Altameem, M. Lee, Image encryption using a synchronous permutation-diffusion technique, Optics and Lasers in Engineering, 90, (2017), 146-154.

[12] M. Yadollahi, R. Enayatifar, H. Nematzadeh, M. Lee, J.-Y. Choi, A novel image security technique based on nucleic acid concepts, Journal of Information Security and Applications, 53, (2020), 102505.

[13] D. Shah, T. Shah, Y. Naseer, S.S. Jamal, S. Hussain, Cryptographically strong S-P boxes and their application in steganography, Journal of Information Security and Applications, 67 ,(2022), 103174.

[14] V. Sabeti, M. Sobhani, S.M.H. Hasheminejad, An adaptive image steganography method based on integer wavelet transform using genetic algorithm, Computers and Electrical Engineering ,99, (2022), 107809.

[15] Y.-H. Yu, C.-C. Chang, I.-C. Lin, A new steganographic method for color and grayscale image hiding, Computer Vision and Image Understanding ,107(3) ,(2007), 183-194.

[16] Y.-S. Wu, C.-C. Thien, J.-C. Lin, Sharing and hiding secret images with size constraint, Pattern Recognition ,37(7), (2004), 1377-1385.

[17] R.-Z. Wang, Y.-D. Tsai, An image-hiding method with high hiding capacity based on best-block matching and k-means clustering, Pattern Recognition ,40(2), (2007), 398-409.