DOI: 10.24996/ijs.2021.62.9.34

ISSN: 0067-2904

Chaos-based Color Image Steganography Method Using 3 D Cat Map

Sarab M. Hameed*[1], Zuhair Hussein Ali[2], Ghadah K. AL-Khafaji[1], Safa Ahmed[1]

[1]Department of Computer Science, College of Science, University of Baghdad, Iraq

[2]Department of Computer Science, College of Education Mustansiriyah University, Baghdad-Iraq

Received: 30/11/2020 Accepted: 19/1/2021

Abstract

Steganography is a technique to hide a secret message within a different multimedia carrier so that the secret message cannot be identified. The goals of steganography techniques include improvements in imperceptibility, information hiding, capacity, security, and robustness. In spite of numerous secure methodologies that have been introduced, there are ongoing attempts to develop these techniques to make them more secure and robust. This paper introduces a color image steganographic method based on a secret map, namely 3-D cat. The proposed method aims to embed data using a secure structure of chaotic steganography, ensuring better security. Rather than using the complete image for data hiding, the selection of the image band and pixel coordination is adopted, using the 3D map that produces irregular outputs for embedding a secret message randomly in the least significant bit (LSB) of the cover image. This increases the complexity encountered by the attackers. The performance of the proposed method was evaluated and the results reveal that the proposed method provides a high level of security through defeating various attacks, such as statistical attacks, with no detectable distortion in the stego-image. Comparison results ensure that the proposed method surpasses other existing steganographic methods regarding the Mean Square Error (MSE) and Peak Signal-to-Noise Ratio(PSNR).

Keywords: 3D cat map, data embedding, least significant bit (LSB), steganography

طريقة إخفاء الصور الملونة القائمة على الفوضى باستخدام خريطة القط ثلاثية الأبعاد

سراب مجيد حميد*[1]، زهير حسين علي [2] ، غادة كاظم الخفاجي[1] ، صفا احمد[1]

[1]قسم علوم الحاسوب ، كلية العلوم ، جامعة بغداد ، بغداد، العراق

[2]قسم علوم الحاسوب، كلية التربية ، جام عة المستصرية ، بغداد، العراق

الخلاصة

الكتابة المخفية هي تقنية لإخفاء رسالة سرية داخل ناقل وسائط متعددة مختلف بحيث لا يمكن التعرف على الرسالة السرية. أهداف تقنيات إخفاء المعلومات هي عدم الإدراك وإخفاء المعلومات والقدرة والأمن والمتانة. على الرغم من العديد من المنهجيات الآمنة التي تم تقديمها ، هناك محاولات مستمرة لتطوير هذه التقنيات لجعلها أكثر أمانًا وقوة. هذا البحث يقدم طريقة إخفاء الصور الملونة بناءً على خريطة سرية ، وهي القط ثلاثي الأبعاد. تهدف الطريقة المقترحة إلى تضمين البيانات باستخدام بنية آمنة من إخفاء الفوضى، مما يضمن أمانًا أفضل. بدلاً من استخدام الصورة الكاملة لإخفاء البيانات ، يتم اختيار نطاق الصورة وتنسيق

*Email: sarabmajeed71@gmail.com

البكسل ، باستخدام الخريطة ثلاثية الأبعاد التي تنتج مخرجات غير منتظمة لتضمين رسالة سرية بشكل عشوائي في أقل قيمة بت (**LSB**) من صورة الغلاف. هذا يزيد من التعقيد الذي يواجهه المهاجمون. تم تقييم أداء الطريقة المقترحة وكشفت نتائج تقييم الأداء أن الطريقة المقترحة توفر مستوى عاليًا من الأمان من خلال التخلص من الهجمات المختلفة مثل الإحصاء ولا يوجد تشويه يمكن اكتشافه في صورة **stego.** تضمن نتائج المقارنة أن الطريقة المقترحة تتفوق على طرق إخفاء المعلومات الموجودة فيما يتعلق بخطأ مربع الوسائل، ونسبة ذروة الإشارة إلى الضوضاء.

1. Introduction

Recently, the data security concern has attained significant attention, considering that millions of users are often sending and receiving data [1]. Improvements in computer security have demonstrated that steganography is a better technique for securing data than cryptography [2]. The output of cryptography is twisted, meaning it can draw the attention of a third party to encrypted messages. Whereas steganography deals with the ability of embedding data into a digital cover so that the secret message is unable to be recognized where the output is not visible [3]. The steganography aim is to transfer the secret message to another via concealing the secret message in a carrier object [4]. Typically, all kinds of files, like text, image, video, and audio can be used as carriers. The carrier that has a high rate of redundancy is the more suitable media for the steganography. Since text files do not include a large amount of redundant data, they are used rarely in steganography; also audio and video are complicated to apply. Therefore the image is the best cover for hiding information [5].

An efficient steganography method should provide invisibility or perceptual transparency, high hiding capacity, robustness (i.e. the capability of the method to keep the data embedded in the cover), tamper resistance (the ability to avoid change, removal, or hiding of a different message). Although some of these requirements are disproportionate to each other, one or two of them can be achieved by one method. It is difficult to satisfy all these requirements in one algorithm [6].

Steganography strategy consists of several components; plaintext is the secret message needing to be transferred to another party; cover is the media that is used as a container of the secret message; and finally, the stego is the resultant media after hiding the secret message in the cover [7]. On the other hand, steganalysis involves discovering the presence of steganography in addition to trying to retrieve hidden messages from the cover text [8]. In recent decades, the evolution of chaotic theory has led to its extensive use in secure communications. It produces some benefits, such as high security, speed and sound computational overheads. Furthermore, steganalysis of chaotic steganographic algorithms demonstrates extraordinary results compared to conventional algorithms [9].

The goals of steganography techniques are improvements in imperceptibility, hiding information capacity, security, and robustness. In spite of numerous secure methodologies that have been introduced, there is an attempt to develop these techniques to make them more secure and robust [10].

2. Related work

Many research papers are focused on the combination of chaos theory with steganography. Some of these researches are as follows. Anees *et al*. in 2014 proposed a steganographic method based on a logistic, tangent delay ellipse reflecting cavity map system (TD-ERCS) within a nonlinear chaotic algorithm (NCA) for determining the pixel coordinate. The cover image was divided into two parts. The sensitive data was converted into binary. The most significant bits (MSBs) and LSBs of sensitive data were embedded into the upper and lower parts of the cover image, respectively. The results showed that the steganographic image is similar to the cover image [11].

Tiwari in 2014 suggested a method for image steganography using chaotic maps for embedding messages in a color image. The results illustrated that the method is highly capable of keeping the message secret [12].

Ghebleh and Kanso in 2014 proposed a method for embedding a binary message randomly in selected detail coefficients of the discrete wavelet transform of a cover image using a 3D chaotic cat map. The results showed that the proposed method has good imperceptibility and high sensitivity to the secret key [13].

Martnez-Gonzlez *et al*. in 2015 proposed a method for hiding text in color images. First, the data was encrypted based on a chaotic map. Then the encrypted data was hidden in a random way in a color image Bernoulli chaotic map. The results revealed that the proposed algorithm produced an improvement in the peak signal to noise ratio compared with similar algorithms' results [14].

Krishnagopal *et al*. in 2015 proposed an image hiding and encryption method. First, the cover image was encrypted using the logistic map and cat map. Then the encrypted image was embedded using a Lorenz map that defines the location of the pixels to be secreted in the cover. The results showed that the proposed method provides efficient security [15].

Rajendran and Doraipandian in 2017 suggested an image hiding method based on a symmetric key. The random symmetric key was generated via the 1D logistic map that was used for selecting the pixel coordinate for hiding the secret image. The results showed that the method has efficient security [16].

Ogras in 2019 introduced an image hiding algorithm using a least significant bit (LSB), Logistic map and XOR operation that was used to decode the message. The results confirmed that the method satisfied high visual quality and good security [17].

ALabaichi1 *et al*. in 2020 introduced a method for hiding a secret message in the LSB of the cover image using 3D Chebyshev and 3D logistic maps. The results showed that the method provides efficient data hiding and good visual quality of the steganographic image [9].

The main contribution of this paper is to introduce a new, effective, LSB-based image steganographic method that inserts a secret message into a cover image randomly, depending on a secure pseudorandom sequence generated by adapting a 3D cat map which is sensitive to initial state and controlled by the secret key.

The rest of the paper is organized as follows: The mathematical model of the 3D chaotic map is described in section 2. The proposed steganographic method is introduced in section 3. Section 4 clarifies the assessment of the proposed method and presents a comparison with other methods. Finally, section 5 presents the concluding explanations and future work.

3. The 3 D cat map

The cat map is a type of cut-out transformation that was introduced by Arnold [18]. The 2D Arnold cat map form is presented in Equation 1 [18]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} mod\ 1 \tag{1}$$

where

$A = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$,

a and b are control parameters, and

x and $y \in [0,1)$.

The 3D cat map is introduced by six control parameters, namely a_x, a_y, a_z, b_x, b_y and b_z, as in Equation 2 [18]

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = A \begin{bmatrix} x \\ y \\ z \end{bmatrix} mod\ 1 \tag{2}$$

where

$$A = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_z b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix} mod\ 1$$

4. The proposed steganography method

The proposed method aims to embed data using a secure structure of chaotic steganography, thereby ensuring better security. Rather than using the complete image for data hiding, a selection of the image band and pixel coordination are exploited, using the 3D cat chaotic map for embedding the sensitive message in the cover image. This increases the complexity encountered by the attackers. The cover image is in RGB color, in which each pixel is 24 bits (i.e. 8-bit for red, 8-bit for green and 8-bit for blue). The LSB embedding method was adopted and the data was embedded in eight bits out of 24 bits (3 significant bits form red, 3 significant bits from green and 2 significant bits from blue components).

Suppose that I_c is a color cover image with width $, w,$ and height $, h,$ in which the secret message represented by M is to be embedded. A stego-image denoted by I_s can be generated by function $\mathcal{F}$ that takes I_c and $M,$ as presented in Equation 3.

$$I_s = \mathcal{F}(M, I_c) \tag{3}$$

In the proposed method, $\mathcal{F}$ is the 3D cat map with an extension that generates a random sequence for picking the pixel location for data concealing. The domain of the 3D cat map in Equation 3 is the interval (0, 1). However when the 3D cat map is used for selecting pixel coordinates and the component of the cover image for data hiding, the following Equations 4, 5, and 6 are adopted. In this way, the pixels will regulate distinctive chaotic positions and, accordingly, the secret message will be inserted randomly.

$$x'' = floor(x' \times w) \tag{4}$$

$$y'' = floor(y' \times h) \tag{5}$$

$$z'' = floor(z' \times 3) \tag{6}$$

wherein the values $x'' \in [0, w), y'' \in [0, h)$, and $z'' \in [0, 2]$.

Algorithm 1 demonstrates the sketch of the proposed embedding of secret message in the RGB cover image.

Algorithm 1: the proposed embedding data

Input:

- I_c: cover image
- w: width of I_c
- h: height of I_c
- M: secret message of length l

Output

- I_s: stego-image

```
Decompose $I_c$ of size $w \times h$ into three components $R, G,$ and $B$
Set the secret parameters of the 3D cat map to produce secret keys $x', y'$ and $z'$ using Equation 2 with $x_0 = 0.8465$, $y_0 = 0.6394$ and $z_0 = 0.3795$
$\boldsymbol{for}\ i = 1\ to\ l$
    Convert $m_i$ to ASCII code and then to the binary representation, $m_b$
    Determine the pixel coordinate $(x'', y'')$ and the component $(z'')$ that is used to hide $m_i$ by calculating equation 4, 5 and 6.
    If $z'' = 0$ then
        Convert $R(x'', y'')$ to binary representation and insert 3 bits from $m_b$into the 3 LSBs of $R$.
        Transform the binary values to decimal values and store the result in $R_s(x'', y'')$.
    elseif
    If $z'' = 1$ then
        Convert $G(x'', y'')$ to binary representation and insert 3 bits from $m_b$into the 3LSBs of $G$
        Transform the binary values to decimal values and store the result in $G_s(x'', y'')$.
    elseif
    If $z'' = 2$ then
        Convert $B(x'', y'')$ to binary representation and insert 3 bits from $m_b$into the 2 LSBs of $B$.
        Transform the binary values to decimal values and store the result in $B_s(x'', y'')$.
    Endif
Endfor
Combine $R_s, G_s,$ and $B_s$ to get the stego-image $I_s$
```

The inverse of function $\mathcal{F}$ should be applied as presented in Equation 7 by the receiving party to retrieve the secret message from the stego-image. The receiving party performs the reverse steps of the embedding process and should be acquainted with the initial values of the 3D cat map to get the secret keys x', y' and z' for determining the pixel coordinate (x'', y'') and the component (z'') that is employed to extract the message M.

$$M = \mathcal{F}^{-1}(I_s) \tag{7}$$

5. RESULTS AND DISCUSSION

The proposed method was coded in MATLAB (R2014a). The experiments were conducted on a Dell computer with Intel(R) Core (TM) i3-3217U, CPU@ 1.80GHz, a Memory of 4.00 GB RAM and 64-bit system type. The six control parameters of the 3D cat map were set experimentally as $a_x =$

$a_y = a_z = 1$ and $b_x = b_y = b_z = 2$ and the initial values were set as $x_0 = 0.8465$, $y_0 = 0.6394$ and $z_0 = 0.3795$ for all the experiments. The performance of the proposed method was evaluated using MSE, PSNR [19], entropy [20], contrast, autocorrelation, energy, and homogeneity, over three standard images: Lena, Baboon and Peppers, of size 512×512.

Table- 1 quantifies the MSE and PSNR for the R, G and B components to show the quality of the stego-image acquired by the proposed method. It can be observed from the results given in the table that the proposed method can withstand statistical attacks and the distortion cannot be distinguished by human eyes considering the small values of MSE and large values of PSNR.

Table- 2 reports the results for entropy, contrast, autocorrelation, energy and homogeneity for each color component of the original image and the corresponding stego-image. It is clear from the results that the proposed method exhibits high visual quality.

Figure- 1 depicts the distribution of pixel values of Lena and the corresponding stego-image. As shown in the aforementioned figure, the histogram analysis does not expose any information to the attacker because of the high statistical similarity between the histogram of Lena, Baboon and Peppers and their stego-image. This means that the proposed method exhibits insignificant distortion of the cover image when the secret message is embedded**.**

Table 1- MSE and PSNR values for each color component of the three test images

Images	MSE			PSNR(dB)		
	R	**G**	**B**	**R**	**G**	**B**
Lena	0.0191	3.5450	2.8575	65.3118	42.6347	43.5710
Baboon	0.0179	1.8451	7.8831	65.5961	45.4705	39.1639
Peppers	0.0188	6.4443	4.1051	65.3886	40.0391	41.9975

Table 2-Statistical analysis for Lena, Baboon and Peppers and the corresponding stego- images

Metrics	**Images**	**Original image**			**Stego-image**		
		R	**G**	**B**	**R**	**G**	**B**
Entropy	Lena	7.2351	7.5676	6.9044	7.2352	7.5677	6.9044
	Baboon	7.5791	7.3246	7.6381	7.5791	7.3245	7.6381
	Peppers	7.2974	7.5814	7.1045	7.2975	7.5815	7.1049
Contrast	Lena	0.1647	0.2078	0.1624	0.1647	0.2148	0.1673
	Baboon	0.3946	0.4913	0.4976	0.3946	0.4952	0.5119
	Peppers	0.1807	0.2831	0.1722	0.1807	0.2934	0.1811
Autocorrelation	Lena	0.9657	0.9631	0.9271	0.9657	0.9619	0.9249
	Baboon	0.9262	0.8641	0.9249	0.9262	0.8630	0.9228
	Peppers	0.9558	0.9729	0.9494	0.9558	0.9719	0.9468
Energy	Lena	0.1680	0.1175	0.2192	0.1680	0.1173	0.2186
	Baboon	0.0893	0.0913	0.0768	0.0893	0.0912	0.0766
	Peppers	0.1577	0.1265	0.2044	0.1577	0.1263	0.2037
Homogeneity	Lena	0.9282	0.9162	0.9263	0.9282	0.9156	0.9255
	Baboon	0.8388	0.8079	0.8062	0.8388	0.8076	0.8054
	Peppers	0.9285	0.9118	0.9293	0.9285	0.9113	0.9284

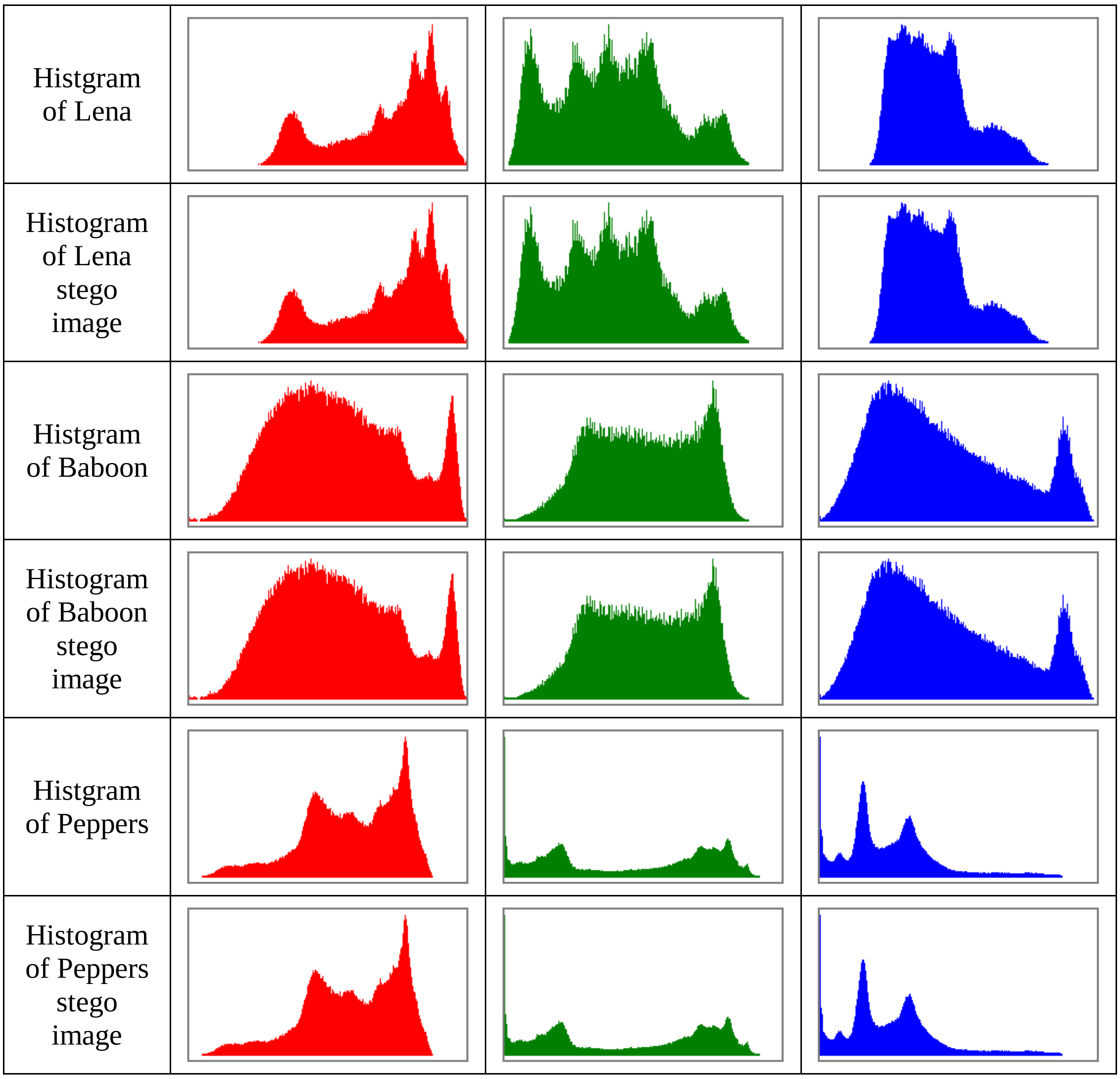

Figure 1- Histogram analysis for R, G, and B components of Lena, Baboon and Peppers images and the corresponding stego images

Comparisons were performed with the works of [6] and [9] to justify the performance of the proposed method, as shown in Table-3. Performance comparison results clarify that the proposed method revealed significantly improved performance in the quality of the stego-image over that reported by [6] and [9] regarding MSE and PSNR .

Table 3- Results of the proposed method against works in [9] and [6]

Method	**Image**	*MSE*			**Average *MSE***	*PSNR*(**dB**)			**Average *PSNR***
		R	G	B		R	G	B	
Proposed method	**Lena**	0.0072	0.1299	0.7384	0.2918	69.5746	46.9935	49.4476	55.3385
	Peppers	0.0053	0.5735	0.1214	0.2334	70.9174	44.0256	47.2872	54.0767
[6]	**Lena**	-	-	-	0.2499	-	-	-	53.8054
	Peppers	-	-	-	0.2503	-	-	-	53.2117
[9]	**Lena**	2.9967	2.0188	1.8811	2.2988	39.1357	39.1237	39.1989	39.1527

6. Conclusions

In this paper, a 3D chaotic cat map was adopted for designing an image-steganographic method. The 3D cat map outputs were employed to determine the pixel coordinate and color component that control the process of embedding a secret message in the cover image. It is shown that there is no detectable distortion in the stego-image (i.e. high visual quality) and the proposed method provides a high level of security by defeating various attacks, such as statistical attacks. Furthermore, it is concluded that the proposed method outperforms other methods regarding visual quality and security. Future work should include an investigation of the impact of different chaotic maps on the steganography**.**

REFERENCES

1. A. S. Ansari, M. S. Mohammadi, and M. T. Parvez. **2019**. "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", *International Journal of Computer Network and Information Security,* **1**: 11-25.
2. A. A. Attaby, M. M. Ahmed and A. K. Alsammak. **2018**. " Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3", *Ain Shams Engineering Journal*, **9**: 1965–1974.
3. M. Khairullah. **2019**. "A novel steganography method using transliteration of Bengali text", *Journal of King Saud University – Computer and Information Sciences*, **31**: 348–366.
4. L Laimeche, A Meraoumia, H Bendjenna. **2019**. "Enhancing LSB embedding schemes using chaotic maps systems, *Neural Computing and Applications*, pp. 1-19.
5. O. Evsutin, A. Kokurina and R. Meshcheryakov. **2018**. "Approach to the selection of the best cover image for information embedding in JPEG images based on the principles of the optimality", *Journal of Decision Systems*.
6. R. Bhardwaj and V. Sharma. **2010**. "Image Steganography Based on Complemented Message and Inverted bit LSB Substitution", *Procedia Computer Science*, **93**: 832 – 838.
7. A. Kumar and K. Pooja. **2010**. "Steganography- A Data Hiding Technique", *International Journal of Computer Applications*, **9**(7).
8. K. Karampidis, E Kavallieratou and G. Papadourakis. **2018**. "A review of image steganalysis techniques for digital forensics", *Journal of Information Security and Applications*, **40**: 217-235.
9. A. ALabaichi, M. Abid, K. Ali and A. Salih. **2020**. "Image Steganography Using Least Significant Bit and Secret Map Techniques", *International Journal of Electrical and Computer Engineering* (IJECE), **10**(1): 935-946.
10. M. C. Kasapbasi. **2019**. "A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption with Post-Quantum Security", *IEEE Access*, **7**: 148495-148510.
11. A. Anees, A.M. Siddiqui, J. Ahmed and I. Hussain. **2014**. "A Technique for Digital Steganography Using Chaotic Maps" *Nonlinear Dynamics*. **75**: 807–816**.**
12. Tiwari A. K., Rajpoot A., Shukla K. K., Karthikeyan S. **2015**. "A Robust Method For Image Steganography Based on chaos Theory", *International Journal of Computer Applications*, **113**(4): 0975 – 8887.
13. R. F. Martnez-Gonzlez, J. A. Daz-Méndez, L. P. Luengas, L. Palacios-Luengas and R. A. Vzquez-Medina. **2015**. "Steganographic Method Using Bernoulli’s Chaotic Maps", *Computers and Electrical Engineering*, **54**: 1–15.
14. M. Ghebleh and A. Kanso. **2014**. "A Robust Chaotic Algorithm for Digital Image Steganography", *Communications in Nonlinear Science and Numerical Simulation,* **19**(6): 1898-1907.
15. S. Krishnagopal, S. Pratap and B. Prakashimage, " Encryption And Steganography Using Chaotic Maps With A Double Key Protection", K.N. Das Et Al. (Eds.), *Proceedings of Fourth*

International Conference on Soft Computing for Problem Solving, Advances In Intelligent Systems And Computing, **336**: 67-78.

16. S. Rajendran and M. Doraipandian. **2017**. "Chaotic Map Based Random Image steganography Using LSB Technique", *International Journal of Network Security*, **19**(4): 593-598.

17. H. Ogras. **2019**. "An Efficient Steganography Technique for Images using Chaotic Bitstream", *International Journal of Computer Network and Information Security*, **2**: 21-27.

18. A. Kanso and M. Ghebleh. **2012**. "A Novel Image Encryption Algorithm Based on A 3D Chaotic Map", *Communications in Nonlinear Science and Numerical Simulation*, **17**(7): 2943-2959.

19. TaqiI. A., & Hameed S. M. **2020**. A New Beta Chaotic Map with DNA Encoding for Color Image Encryption. *Iraqi Journal of Science,* **61**(9): 2371-2384.

20. X. ShuangKui, J.Wu. **2018**. "A Modification-Free Steganography Method Based on Image Information Entropy", *Security and Communication Networks*, vol. 2018, Article ID 6256872, 8 pages, 2018