*Journal of **AI** and **D**ata **M**ining*
Vol 7, No 3, 2019, 377-383

DOI: 10.22044/JADM.2019.7510.1895

A New Method for Encryption of Color Images based on Combination of Chaotic Systems

H. Khodadadi[1*] and A. zandvakili [2]

1. Department of Computer Engineering, Minab Branch, Islamic Azad University, Minab, Iran.
2. Department of Computer Engineering, Jiroft Branch, Islamic Azad University, Jiroft, Iran.

Received 18 October 2018; Revised 17 December 2018; Accepted 16 February 2019

**Corresponding author:habib.khodadadi@iauminab.ac.ir (H.Khodadadi).*

Abstract

This paper presents a new method for encryption of color images based on a combination of chaotic systems, which make the image encryption more efficient and robust. The proposed algorithm generates three series of data ranged between 0 and 255 using a chaotic Chen system. Another Chen system is then started with different initial values, which are converted to three series of numbers from 0 to 10. The red, green, and blue values are combined with the three values for the first Chen system to encrypt pixel 1 of the image, while the values for the second Chen system are used to distort the combination order of the values for the first Chen system with the pixels of the image. The process is repeated until all pixels of the image are encrypted. The innovative aspect of this method is in combination with the two chaotic systems, which make the encryption process more complicated. The tests performed on the standard images (USC datasets) indicate the effectiveness and robustness of the proposed encryption method.

Keywords: *Chaos, Combination of Chaotic Systems, Encryption of Color Images, Chen Chaotic System.*

1. Introduction

The increasing use of information resources, the unprecedented growth of the Internet, and, at the same time, the manipulation of these resources by unauthorized individuals have made the security of information resources a major global challenge. This has resulted in widespread changes in the way people, organizations, and institutions live and work. Ensuring that unauthorized persons do not have access to the information that we do not want to share with others is one of the most important security challenges regarding the distribution of information on the Internet. Today, different encryption methods are used to prevent data abuse. Information encryption is a proper method used to maintaining information security. One of the important types of encryption is the encryption of visual data, for which, several methods have been designed so far. Due to its specific features, the application of chaos is very important for encryption. With their unique features such as sensitivity to initial value, pseudo-randomness, unpredictability, and non-periodicity, chaotic systems are so ideal for the encryption that the use of these systems is increasingly growing.

A look at the recent encryption algorithms shows that they are mostly based on chaotic systems. However, the small key space and the weak security are evident in 1D chaotic systems. In [1-16], various methods have been proposed for the encryption of images through chaotic systems, each having its own characteristics.

In the recent years, many algorithms have been proposed for image encryption based on permutation, in which the control parameters used in the permutation phase are usually assumed to be fixed in the entire process of encryption. However, a chaos-based encryption algorithm with variable control parameters is presented in [3].

The diffusion phase is performed by math operations in most chaos-based encryption algorithms, which limits the speed. Using a simple table look-up, a more efficient diffusion mechanism has been presented in [4].

A chaos-based image encryption method has been presented in [5], which uses random permutation.

The chaos-based image encryption method proposed in [6] encrypts each one of the R, G, and B components separately but simultaneously reduces their effect on each other.

A combination of genetic algorithm and chaos has been presented in [7], while a combination of chaos and cellular automata proposed for encryption has been presented in [8].

In [9], the original image has first been converted to several sections, each of which then replaced by chaotic numbers. The image pixels are encrypted using chaotic functions in the next step.

The robust chaos-based image encryption method of [10] employs a chaotic 3D design along with a zigzag scanning procedure to displace square blocks in the combination phase.

The chaos-based image encryption algorithms include mathematical operations for creating chaotic circuit from the chaotic system. These operations are normally time-consuming, and require strong processors. In order to overcome this weakness, an encryption method for fast generation of large permutations keys and diffusion based on the ordering of the Linear Diophantine Equation (LED) has been presented in [11]. The coefficients are integers and are dynamically generated from any chaotic system. In this method, the strong security and the low computational complexity are resulted only from one permutation of sorted solutions of LED.

In [12], a synchronization plan has been presented for two componential chaotic systems. The sufficient conditions to realize this synchronization are created through Laplace transformation. The introduced encryption algorithm encodes the original image using a non-linear function.

An effective adaptive model for chaos-based image encryption has been presented in [13]. In this paper, an efficient and fast encryption algorithm has been designed using a permutation-diffusion classic structure and a 2D chaotic system; this method is different from many existing unsafe systems. In this method, different simple images will have a stream of random characters even if images are different in a single bit.

In [14], a stack has been used in the encryption processes of image with the help of chaos. The order of pixels to be encrypted is determined by the stack and a chaotic system. Each pixel is then encrypted with another chaotic system.

In [15], a new image encryption algorithm has been proposed based on non-adjacent spatial multi-dimensional maps. In the proposed system, a pixel-bit replacement strategy is used that interconnects pixel-bit pages to each other without any additional storage space.

In [16], an image encryption algorithm has been presented based on the chaotic system and DNA sequencing operation. First, a simple image is encoded into a DNA matrix, and then a wave-based substitution plan is performed. The resulting chaos sequences are used by the 2D logistic chaos plan to replace the Row Circular Permutation (RCP) and the Column Circular Permutation (CCP). A row-to-row image diffusion method is then applied at the DNA level.

This paper introduces a new method for encryption of color images based on a combination of chaotic systems. In addition to increasing the key space, this allows for a more robust encryption system.

2. Chaotic systems

In the second half of the 20th century, a new scientific method and a very interesting theory, namely “chaos,” emerged in the field of modern physics and mathematics. This theory relates to systems whose dynamics show such a sensitive behavior to changes in initial values that their future behavior will no longer be predictable in the face of the change. These systems are called chaotic systems.

Chaotic systems are non-linear dynamical systems that are very sensitive to their initial conditions and show a pseudo-random behavior. A slight change in the initial conditions of such systems will lead to countless changes in the future. This phenomenon in the chaos theory is known as the “butterfly effect.”

Chaotic systems will remain stable in the chaos mode when they meet the requirements of the Lyapunov exponential equations. An important feature that makes this phenomenon great for encryption is the system definability while having a pseudo-random behavior. This makes the system output random in the eyes of attackers, while it is definable and recoverable for the decoder.

The chaotic systems that have been introduced so far can be divided into two general categories. The first group includes the chaotic systems that have certain physical interpretations, and are derived from dynamic equations of real systems such as Lorenz's chaotic systems [17]. The second group consists of chaotic systems that do not have any particular physical interpretations, and are merely mathematical models. In fact, these chaotic systems are used as indicators of evaluation in chaos control and synchronization. An example for these chaotic systems is the chaotic Chen system [18], introduced in 1999.

$$\begin{cases} \dot{x} = \mathrm{a}(\mathrm{y} - \mathrm{x}) \\ \dot{\mathrm{y}} = (\mathrm{c} - \mathrm{a})\mathrm{x} - \mathrm{xz} + \mathrm{cy} \\ \dot{\mathrm{z}} = \mathrm{xy} - \mathrm{bz} \end{cases} \quad (1)$$

The governing equations are shown in (1), where a, b, and c are the parameters. If a = 35 and b = 3, and c = [20, 28.4], the system is in a chaos mode. The chaotic behavior of this system is shown in figure 1.

$$x_{n+1} = \lambda x_n(1 - x_n), x_0 \in (0,1) \quad (2)$$

The logistic system is a simple chaotic system with the governing Equation (2), where the system shows a chaotic behavior for those values of λ that are in the [3.56, 4] range.

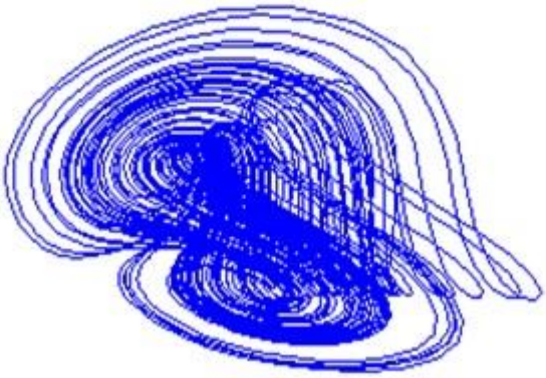

Figure 1. Chaotic behavior of Chen system.

3. Proposed method

The proposed algorithm uses two Chen chaotic systems to create a new method for image encryption. This algorithm involves the following steps:

Step 1: The Chen chaotic system is initiated with appropriate initial values, and after N_0 iterations, three series of values, i.e. X, Y, and Z, are generated.

$$X1 = rem(floor\left(\left(abs\big(X(i)\big) * (10^{14})\right)\right), 256) \quad (3)$$

Step 2: The X1, Y1, and Z1 series are generated according to (3) from the X, Y, and Z series, respectively.

Here, *rem* is the integer remainder function, *floor* is the integer part of the number, and *abs* is the absolute value. Therefore, numbers in the X1, Y1, and Z1 series are between 0 and 255.

Step 3: Another Chen chaotic system is run with different initial values, and after M_0 iterations, three series of values, i.e. P, Q, and R, are generated.

$$P1 = rem(floor\left(\left(abs\big(P(i)\big) * (10^{14})\right)\right), 11) \quad (4)$$

Step 4: The P1, Q1, and R1 series are generated according to (4) from the P, Q, and R series, respectively.

Numbers of these three series are between 0 and 10.

Step 5: The I, J, and K counters start with the initial value of 0.

Step 6: Counter L is set at 1.

Step 7: The tasks a to e are performed in a loop on image pixels, starting from the first one:

a. $I = I + P1(L)$

b. $J = J + Q1(L)$

c. $K = K + R1(L)$

d. The red, green, and blue pixel (R^p, G^p, and B^p) values are $XOR(\oplus)$ with $X1(I)$, $Y1(J)$, and $Z1(K)$, respectively.

e. $L = L + 1$

In step 7, a combination order of values of the main series with the pixels of the image is cluttered using the other three series ($P1$, $Q1$, and $R1$), i.e. the next number of the first Chen series does not necessarily combine with image pixels; rather, the next number can be 0 to 10 positions farther from the previous number depending on the value of the second Chen series. This makes the encryption process more difficult and complex. Performing these steps (Figure 2) on the encrypted image is enough for decoding it.

4. Computational results

This encryption idea was implemented using MATLAB and tested on the USC database images (http://sipi.usc.edu/database/). Figure 3 shows a sample image of 256 * 256 with a histogram of red, green, and blue channels, while an encrypted version of this image with a histogram of red, green, and blue channels and its decoded image are shown in figure 4. Figures 5 and 6 show the two versions of another image. The initial values for the first Chen system include a = 35, b = 3, and c = 26, while the initial values for the X, Y, and Z series are 8.2, -3.5, and -0.2, respectively. The initial values for the second Chen system are a = 35, b = 3, and c = 25, and the initial values for the P, Q, and R series are 10.64, -7.5, and 0.09, respectively. Moreover, M_0 is set to 2000 and N_0 is set to 3000 (values of the series before M_0 and N_0 iterations are not used). As it can be seen, this encryption idea is able to encrypt the image with a completely flat histogram.

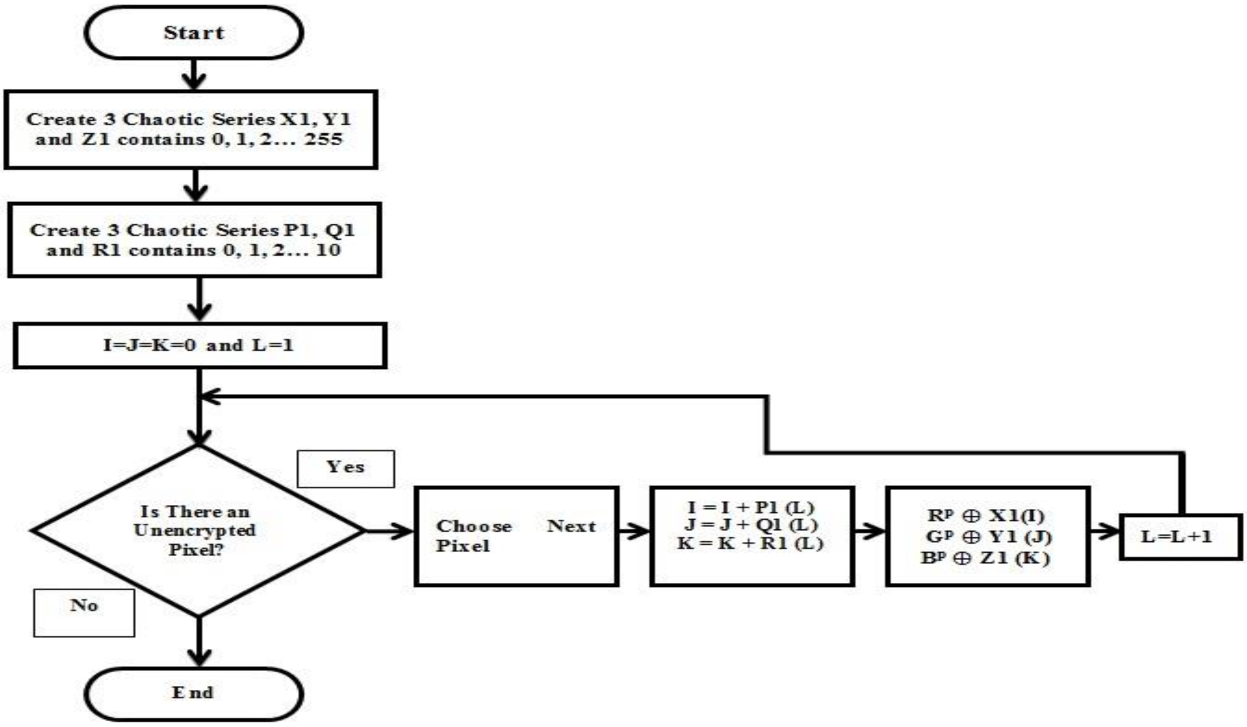
Start
Create 3 Chaotic Series X1, Y1 and Z1 contains 0, 1, 2... 255
Create 3 Chaotic Series P1, Q1 and R1 contains 0, 1, 2... 10
I=J=K=0 and L=1
Is There an Unencrypted Pixel?
Yes
No
Choose Next Pixel
I = I + P1 (L)
J = J + Q1 (L)
K = K + R1 (L)
R^P ⊕ X1(I)
G^P ⊕ Y1 (J)
B^P ⊕ Z1 (K)
L=L+1
End

Figure 2. Proposed encryption algorithm.

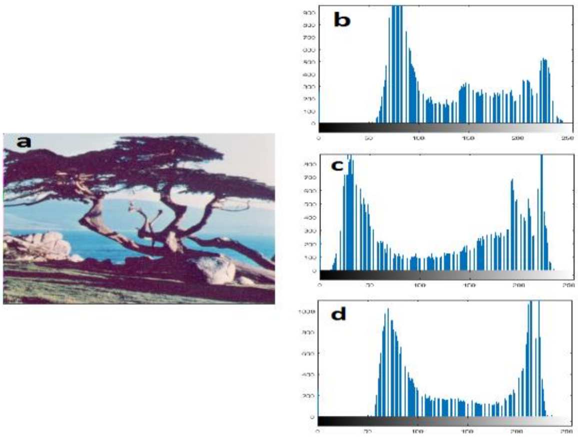

Figure 3. (a) Original image. (b), (c), and (d) histograms of red, green, and blue channels of the original image.

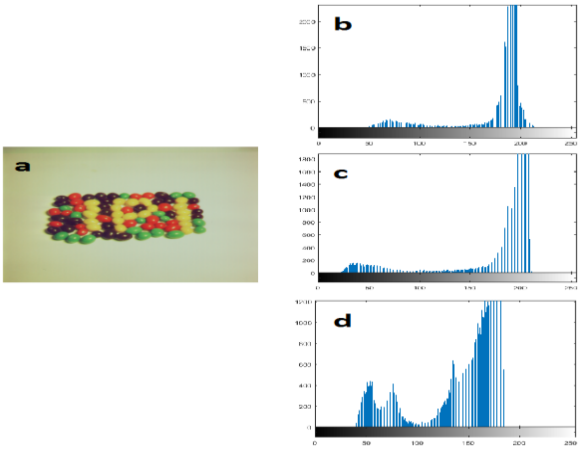

Figure 5. (a) Original image. (b), (c), and (d) histograms of red, green, and blue channels of the original image.

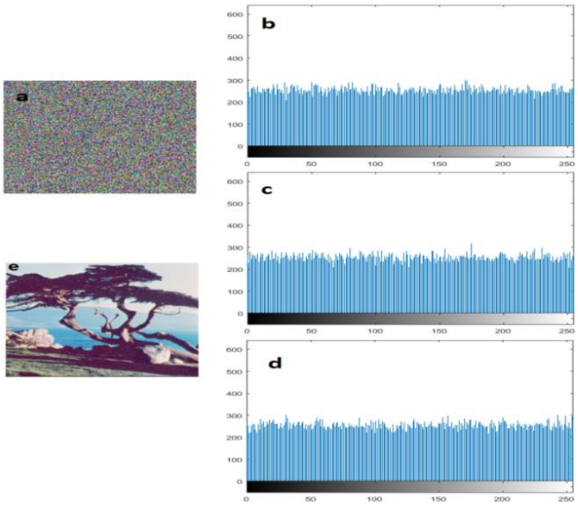

Figure 4. (a) The encrypted image of Figures (3-a), (b), (c), and (d) histograms of red, green, and blue channels of the encrypted image. (e) Decrypted image.

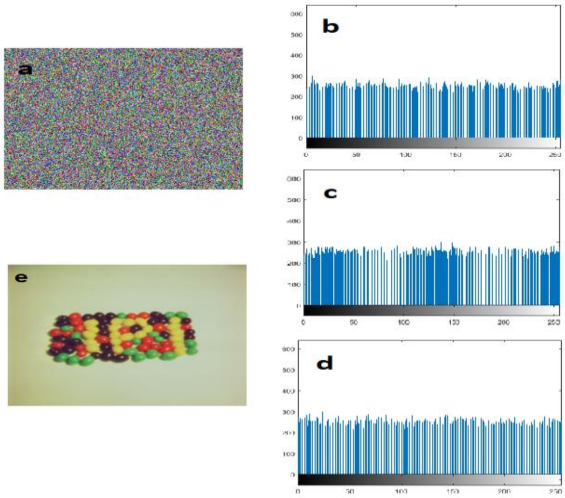

Figure 6. (a) The encrypted image of Figure (5-a). (b), (c), and (d) histograms of red, green, and blue (e) channels of the encrypted image. (e) Decrypted image.

4.1. Key space analysis

The key values of this method include the initial values of the two Chen systems, quantities of a, b, and c in the Chen systems, and values of M_0 and N_0, which have the appropriate key space. The 6 initial values of Chen systems require 32 bits each, counting for a total of 192 bits of space. Moreover, 6 values of a, b, and c in both systems require 16 bits each, i.e. a total of 96 bits of space. M_0 and N_0 each require 32 bits (large integer) or a total of 64 bits. Therefore, the total key space required is 352 bits, meaning that there are 2^{352} different combinations in the key space, which is a very large number. This means that the proposed algorithm is robust for the Brute Force attack.

4.2. Key sensitivity analysis

According to the tests, keys are very sensitive in our proposed method. In order to decode the encrypted image, we only slightly changed the value of one of the keys (from 8.2 to 8.20001), leaving others unchanged. The results of the decoded image along with its histograms are shown in figure 7.

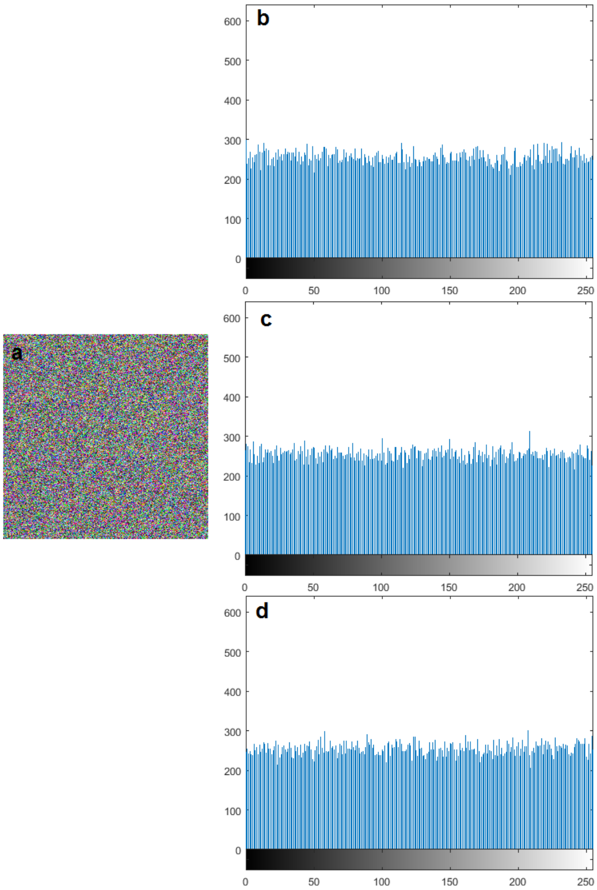

Figure 7. (a) The decrypted image of Figure (3-a) with different initial values (only 8.2 has been changed to 8.20001). (b), (c), and (d) are histograms of red, green, and blue channels.

As it can be seen, even knowing the exact values of all keys except one (even though the difference is very small) results in a failure in decoding the image, and the image can only be decoded if the exact values of all keys are known**.**

4.3. Analysis of similarity of neighboring pixels

Normally, values of neighbouring pixels are very similar in most parts of an image. Therefore, it is expected for the similarity of neighbouring pixels in an image to be very high. However, a good encryption algorithm should reduce the similarity of neighbouring pixels so that the possibility of detecting the pixel values by comparing them with neighbouring pixels is minimized [9]. The similarity of two neighbouring pixels in the horizontal, vertical, and diagonal directions in an original image with its encrypted version in the blue channel is shown in figure 8 (3,000 random neighbouring pixels were selected in each direction, and their values were displayed on the chart). As it can be seen, while the level of similarity is high in the original image, it is very low in the encrypted version, indicating a proper encryption.

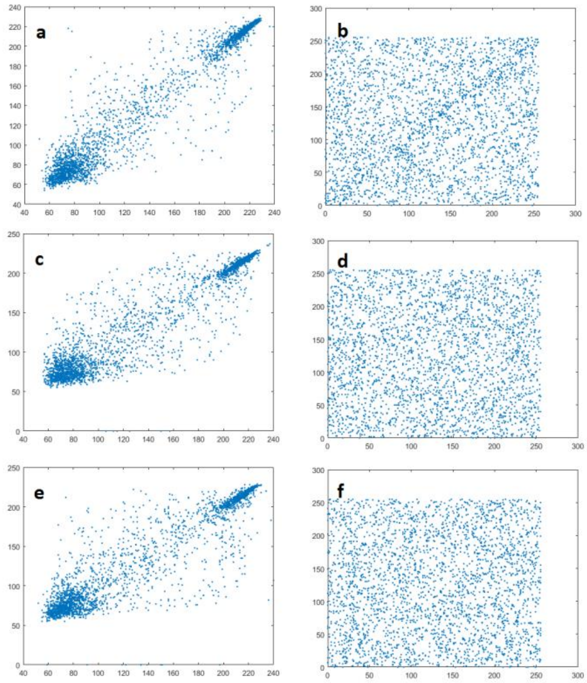

Figure 8. The degree of similarity of the two neighboring pixels in the blue channel from top to bottom in horizontal, vertical, and diagonal directions. Values of a, c, and e are for the original image, and b, d, and f are for the encrypted image.

4.4. Entropy analysis

The entropy feature of an image can determine its randomness.

$$\mathrm{H(S)} = \sum_{\mathrm{i}=0}^{N-1} \mathrm{P(S_i)} \log\left(\frac{1}{\mathrm{P(S_i)}}\right) \qquad (5)$$

This parameter is as shown in (5), where N is the number of gray levels of the image (e.g. in images with 8 bits, for storing each gray level N = 256) and $P(S_i)$ is the probability of occurrence of gray level i in this image. The entropy 8 for an image indicates its complete randomness. Table 1 shows the entropy values of the image in figure 3 before and after encryption. These values show a great capability of the proposed method in image encryption.

In table 2, the entropy rate of the LENA image encrypted with the proposed method in this paper is compared with several other methods, which confirms the superiority of our image encryption method.

Table 1. Entropy of original image in Figure 3 and its encrypted version.

Entropy of Original Image	Entropy of Encrypted Image
7.5371	7.9991

Table 2. Comparison of the entropy of LENA image encrypted with our method and several other references.

Ref	[8]	[11]	[16]	Our Proposed Algorithm
Information Entropy	7.9696	7.9992	7.9993	7.9998

5. Conclusion

In this paper, we proposed a new method for encryption of visual data based on chaotic systems. In this method, a series of Chen chaotic system, generated after initial pre-processing, were combined with image pixels to generate the encrypted image. The combination order of values of the first Chen series with pixels of the image was determined by another Chen system, which made the encryption process more complicated. The results of the performed tests indicated the effectiveness and robustness of the proposed method.

References

[1] Luo, J. & Shi, H. (2006). Research of Chaos Encryption Algorithm Based on Logistic Mapping. International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), Pasadena, CA, USA, 2006.

[2] Mazloom, S. & Eftekhari-Moghadam, A. M. (2009). Color image encryption based on Coupled Nonlinear Chaotic Map. Chaos, Solitons and Fractals, vol. 42, no. 3, pp. 1745–1754.

[3] Wang Y., et al. (2009). A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons and Fractals, vol. 41, no. 4, pp. 1773–1783.

[4] Wong, K., Kwok, B. S. & Yuen, C. (2009). An efficient diffusion approach for chaos-based image encryption. Chaos, Solitons and Fractals, vol. 41, no. 5, pp. 2652–2663.

[5] Yoon, J.W. & Kim, H. (2010). An image encryption scheme with a pseudorandom permutation based on chaotic maps. Communications in Nonlinear Science and Numerical Simulation, vol. 15, no. 12, pp. 3998-4006.

[6] Wang, X., Teng, L. & Qin, X. (2012). A novel colour image encryption algorithm based on chaos. Signal Processing, vol. 92, no. 4, pp. 1101-1108.

[7] Abdullah, A.H., Enayatifar, R. & Lee, M. (2012). A hybrid genetic algorithm and chaotic function model for image encryption. International Journal of Electronics and Communications (AEÜ), vol. 66, no. 10, pp. 806-816.

[8] Bakhshandeh, A. & Eslami, Z. (2013). An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Optics and Lasers in Engineering, vol. 51, no. 6, pp. 665-673.

[9] Mirzaei, O., Yaghoobi, M. & Irani, H. (2011). A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dynamics, vol. 67, no. 1, pp. 557-566.

[10] Ghebleh, M., Kanso, A. & Noura, H. (2014). An image encryption scheme based on irregularly decimated chaotic maps. Signal Processing: Image Communication, vol. 29, no. 5, pp. 618-627.

[11] Armand Eyebe Fouda J. S. et al. (2014). A fast chaotic block cipher for image encryption. Communications in Nonlinear Science and Numerical Simulation. vol. 19, no. 3, pp. 578-588.

[12] Xu Y., et al. (2014). Image encryption based on synchronization of fractional chaotic systems. Communications in Nonlinear Science and Numerical Simulation. vol. 19, no. 10, pp. 3735-3744.

[13] Huang, X. & Ye, G. (2014). An efficient self-adaptive model for chaotic image encryption algorithm. Communications in Nonlinear Science and Numerical Simulation. vol. 19, no. 12, pp. 4094-4104.

[14] Khodadadi, H. & Mirzaei, O. (2017). A stack-based chaotic algorithm for encryption of colored images. Journal of AI and Data Mining, vol. 5, no. 1, pp. 29-37.

[15] Ying-Qian, Z. & Xing-Yuan, W. (2015). A new image encryption algorithm based on non-adjacent coupled map lattices. Applied Soft Computing, vol. 26, pp. 10-20.

[16] Chai, X., Chen, Y. & Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. Optics and Lasers in Engineering, vol. 88, pp. 197-213.

[17] Lorenz, E.N. (1963). Deterministic Nonperiodic Flow. Journal of the Atmospheric Sciences, vol. 20, no. 2, pp. 130-141.

[18] Chen, G. & Ueta, T. (1999). Yet another chaotic attractor. International Journal of Bifurcation and Chaos, vol. 9, no. 7, pp. 1465-1466.

نشریه هوش مصنوعی و داده کاوی

روشی جدید به منظور رمزنگاری تصاویر رنگی بر مبنای ترکیب سیستم‌های آشوبناک

حبیب خدادادی [۱،*]و ابوذر زندوکیلی [۲]

[۱] گروه کامپیوتر، واحد میناب، دانشگاه آزاد اسلامی، میناب، ایران.

[۲] گروه کامپیوتر، واحد جیرفت، دانشگاه آزاد اسلامی، جیرفت، ایران.

ارسال ۲۰۱۸/۱۰/۱۸؛ بازنگری ۲۰۱۸/۱۲/۱۷؛ پذیرش ۲۰۱۹/۰۲/۱۶

چکیده:

در این مقاله، روش جدیدی به منظور رمزنگاری تصاویر رنگی ارائه شده است. اساس این روش بر مبنای استفاده از ترکیب سیستم‌های آشوبناک است که رمزنگاری تصویر را کاراتر و مقاوم‌تر نموده است. در این روش ابتدا با دادن مقادیر اولیه یک سیستم آشوبناک چن را شروع می‌کنیم و سپس با پردازش های اولیه سه سری این سیستم را به اعداد ۰ تا ۲۵۵ تبدیل می‌کنیم. سیستم چن دیگری را با مقادیر اولیه متفاوت شروع می کنیم و سپس اعداد این سری ها را به ۰ تا ۱۰ تبدیل می‌کنیم. با شروع از اولین پیکسل تصویر سه مقدار قرمز، سبز و آبی را با سه مقدار سیستم چن اول ترکیب کرده و این پیکسل رمزگذاری می‌شود. در این میان از اعداد سیستم چن دوم به منظور به هم ریختن ترتیب ترکیب اعداد سیستم چن اول با پیکسل های تصویر استفاده می کنیم. این عمل تا رمزنگاری تمام پیکسل‌های تصویر ادامه داده می‌شود. نوآوری این روش در نحوه ترکیب دو سیستم آشوبناک است که موجب پیچیده‌تر شدن فرآیند رمزنگاری می‌شود. آزمایشاتی که بر روی تصاویر استاندارد انجام شده است نشان‌دهنده کارا و مقاوم بودن این روش رمزنگاری می‌باشد.

کلمات کلیدی: آشوب، ترکیب سیستم‌های کیاتیک، رمزنگاری تصاویر رنگی، سیستم کیاتیک چن.