A Four-dimensional Conservative Chaotic System and Its Application in Image Encryption

Wei Li, Jingwen Liu#, Hongyan Jia*

College of Electronic Information and Automation, Tianjin University of Science and Technology, 300222, China

E-mail: jiahy@tust.edu.cn

#These authors contributed equally to this work.

www.tust.edu.cn

Abstract

In this paper, a four-dimensional conservative chaotic system is firstly analyzed and investigated. It is found that the four-dimensional conservative chaotic system shows some complex dynamics, such as multi-stability and strong pseudo-randomness. Secondly, based on pseudo-random sequences and two-dimensional discrete wavelet transform, an image encryption algorithm is realized. Finally, all the experiment results and the security analysis show that the algorithm show good encryption characteristics, which further prove the image encryption algorithm.

Keywords: Hamiltonian chaotic system, Pseudo-randomness, Image encryption, Wavelet transform

1. Introduction

With the rapid development of computer and network technology, multimedia information occupies an increasing proportion in the whole human digital communication. The necessary encryption and protection of private digital information has become a growing concern. Compared with text information, image data has unique characteristics such as large amount of data, high redundancy and strong correlation between adjacent pixels. These characteristics make the traditional encryption algorithms used for text encryption no longer suitable for image encryption[1,2]. Therefore, it is urgent to find a fast and secure encryption algorithm for image encryption[3-7].

Chaotic system has good pseudo-randomness, ergonomic, unpredictability and sensitivity to initial values and parameters and other unique characteristics[8-13]. Therefore, these characteristics make chaotic system very suitable for image encryption. At first, J. Matthews and A. Robert[14] put forward the concept of "chaos cipher" in 1989. Subsequently, many cryptography schemes are proposed based on chaos[15-30]. For example, Jeri Fridrich used reversible two-dimensional chaotic maps on a torus or square to create an image encryption algorithm for new symmetric blocks[15]. Wang et al. proposed an image encryption algorithm based on fractional-order one-dimensional chaotic mapping with large chaotic space[7]. Chai et al. proposed a block-obfuscated image encryption algorithm based on three-dimensional Brownian motion, using Logistic Tent system to generate the direction of motion of particles, and introduce block-obfuscated image based on position sequence group[19]. Wang et al. proposed an image encryption algorithm based on hidden attractor chaotic system and Knuth Seinfeld algorithm[30]. However, the proposed scheme is mainly designed for some grayscale images, which require that the color images and multimedia data must first be converted to the same mode as the grayscale images, and then the scheme can be used for encryption. All above image encryption algorithms are based on dissipate chaotic system (DCS), few image encryption algorithms based on conservative chaotic system (CCS) have been proposed. Although DCS may have good pseudo-randomness, it produces singular attractors in the fractal dimension. Therefore, it is easy to be attacked by reconstructing the attractor. At the same time, most of the orbit around the attractor is unreachable, so the ergodic property of DCS is poor. Compared with DCS, CCS does not generate attractors, which ensures that the attacker cannot reconstruct the attractor and crack the encryption scheme. Meanwhile, the dimension of CCS is consistent with that of the system, and it has better ergodicity than DCS.

In this paper, a conservative chaotic system is firstly analyzed. Subsequently, based on the conservative chaotic system and two-dimensional discrete wavelet transform, a new image encryption algorithm is proposed. Finally, the new image encryption algorithm is verified, and all the results are analyzed from the aspects of statistical analysis, difference analysis and speed. It shows that the algorithm has good security performance and operation speed, and significantly improves the key space.

2. A Four-dimensional Conservative Chaotic System

By studying the method of constructing four-dimensional conservative chaotic system by Qi et al., a new four-dimensional conservative chaotic system is constructed on the basis of the method, which can be described as:

$$\begin{cases} \dot{x}_1 = (\Pi_4 - \Pi_2)x_2x_4 + (\Pi_4 - \Pi_3)x_3x_4 \\ \dot{x}_2 = (\Pi_1 - \Pi_4)x_1x_4 + c\Pi_3x_3 \\ \dot{x}_3 = (\Pi_1 - \Pi_4)x_1x_4 - c\Pi_2x_2 \\ \dot{x}_4 = (\Pi_2 - \Pi_1)x_1x_2 + (\Pi_3 - \Pi_1)x_1x_3 \end{cases} \tag{1}$$

where x_1, x_2, x_3, x_4 are state variables, Π_1, Π_2, Π_3, and c are system variables. When letting $c = 0$, $(\Pi_1, \Pi_2, \Pi_3, \Pi_4) = (5, 6, 7, 8)$, and choosing different initial values and system parameters, the system can both rich periodic dynamics and chaotic dynamics. In order to further study the reasons for chaotic dynamics of the system (1) from the perspective of energy, it is first convert into Kolmogorov form as follows:

$$\dot{x} = J(x)\nabla H(x) = \begin{bmatrix} 0 & -x_4 & -x_4 & x_2 + x_3 \\ x_4 & 0 & c & -x_1 \\ x_4 & -c & 0 & -x_1 \\ -x_2 - x_3 & x_1 & x_1 & 0 \end{bmatrix} \begin{bmatrix} \Pi_1 x_1 \\ \Pi_2 x_2 \\ \Pi_3 x_3 \\ \Pi_4 x_4 \end{bmatrix} \tag{2}$$

Where, $J(x) = \begin{bmatrix} 0 & -x_4 & -x_4 & x_2 + x_3 \\ x_4 & 0 & c & -x_1 \\ x_4 & -c & 0 & -x_1 \\ -x_2 - x_3 & x_1 & x_1 & 0 \end{bmatrix}$, $H(x) = \frac{1}{2}(\Pi_1 x_1^2 + \Pi_2 x_2^2 + \Pi_3 x_3^2 + \Pi_4 x_4^2)$. It is found that the Jacoby matrix of system (1) is an antisymmetric matrix.

Then keep all the state variables and system variables same as the above except for $c = 3$, when changing initial value x_1, the Lyapunov exponent diagram of system (1) is shown in Fig. 1. It can be found when $x_1 \in (-1.8, 3.7)$, the system (1) shows a periodic or counter-periodic dynamics; when $x_1 \in (-20, -1.8) \bigcup (3.7, 20)$, the system (1) shows a chaotic dynamics. Next, set system variables $(\Pi_1, \Pi_2, \Pi_3, \Pi_4, c) = (5, 6, 7, 8, 3)$, when selecting initial values $(0, 5, -5, -3)$, system (1) shows a quasi-periodic attractor, when selecting initial values $(10, 5, -5, -3)$ system (1) shows a chaotic attractor, respectively, as shown in Fig. 2.

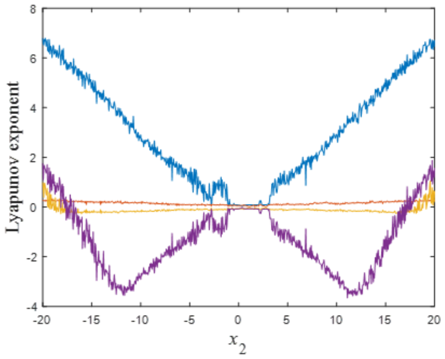
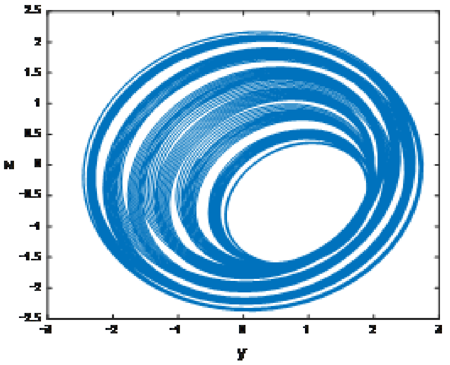
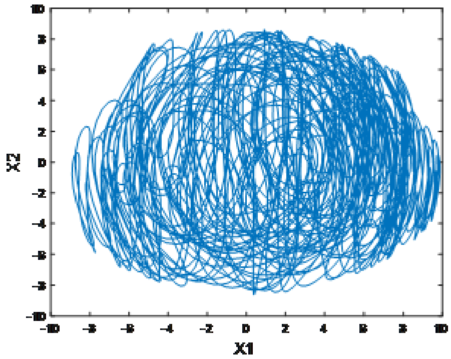


Fig. 1 Lyapunov exponent diagram of system (1)



(a) quasi-periodic attractor



(b) chaotic attractor

Fig. 2 Phase diagrams of system (1) when $c = 3$

3. Image Encryption Algorithm

3.1 Encryption process

In this paper, the initial parameters of the system (1) are used as the encryption algorithm keys, and the plain image can be scrambled and spread by pseudo-random sequences generated by the system (1). In addition, during the scrambling operation, two-dimensional discrete wavelet is used to transform and extract the low-frequency part of the image. Here, only the low-frequency part is scrambled to improve the calculation speed of the encryption algorithm, as shown in Fig. 3.

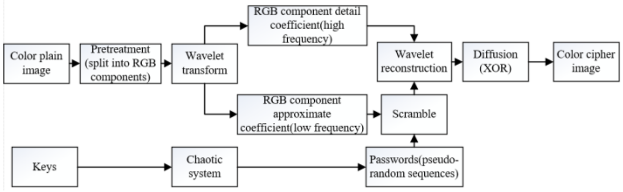

Color plain image
Pretreatment (split into RGB components)
Wavelet transform
RGB component detail coefficient(high frequency)
RGB component approximate coefficient(low frequency)
Wavelet reconstruction
Scramble
Diffusion (XOR)
Color cipher image
Keys
Chaotic system
Passwords(pseudo-random sequences)

Fig. 3 Encryption algorithm flowchart

The specific steps are as follows:

Step 1: To ensure the validity of the sequence, delete the first 2000 values of pseudo-random sequences $x- value$, $y- value$, $z- value$, $w- value$ generated by the system (1), and start counting from the 2001th value;

Step 2: Decompose the color picture I into three components, R, G, and B, denoted as I_R, I_G, I_B respectively;

Step 3: Extract the approximate coefficients and detail coefficients (horizontal coefficient ch1, vertical coefficient cv1, diagonal coefficient cd1) using the "db1" wavelet basis functions for the three components of I_R, I_G, I_B. Taking the R component as an example, the extracted two-dimensional array is marked as $R- ca1(i, j)$ $(i = 1, 2, ..., \frac{m}{2}, j = 1, 2, ..., \frac{n}{2})$, and the extracted two-dimensional array is converted into a one-dimensional column vector $R- ca1(k)$ $(k = 1, 2, ..., \frac{m}{2} ? \frac{n}{2})$ by column;

Step 4: Calculate from the 2001th value of $w- value$, and select $\frac{m}{2}' \frac{n}{2}$ values in turn, denoted as $w- value(p)$ $(p = 1, 2, ..., \frac{m}{2} ? \frac{n}{2})$. Sort $w- value(p)$ from small to large, and record the sorted row vector as $w_1- value(p¢)$ $(p¢= 1, 2, ..., \frac{m}{2} ? \frac{n}{2})$. If $p = k$, $R- ca1ï(p) = R- ca1(k)$, forming a new column vector $R- ca1ï(p)$. Finally, it is transformed into $\frac{m}{2}' \frac{n}{2}$ matrix through the "reshape" function, so as to realize the scrambling of the approximate coefficients ca1 of the R, G, and B components;

Step 5: Perform wavelet reconstruction on the approximate coefficients of the R, G, and B components after scrambling in Step 4 and the detail coefficients of the image before encryption, and finally get the R, G, and B components after scrambling, denoted as I_r, I_g, I_b;

Step 6: Calculate from the 2001th value of $x- value$, $y- value$, $z- value$, $w- value$, select $m' n$ values in turn, mark them as $x- value(p)$, $y- value(p)$, $z- value(p)$ $(p = 1, 2, ..., m? n)$, and perform the operation of equation (3-1), so that all elements in these three vectors are in the range of $[0, 255]$.

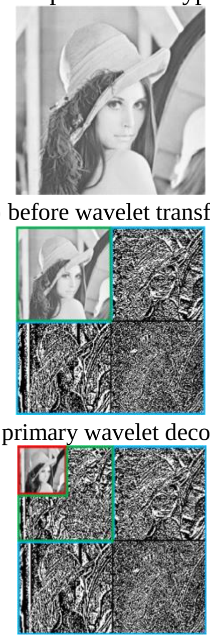
$$y_n = \mod(10000? y_n, 256) \qquad (2)$$

Step 7: Perform a bit wise XOR operation for $x- value(p)$, $y- value(p)$, $z- value(p)$ generated in Step 6 with the elements in the I_r, I_g, I_b matrix, and finally get the encrypted R, G, B components, denoted as $I¢_r, I¢_g, I¢_b$；；

Step 8: Reconstruct $I¢_r, I¢_g, I¢_b$ component generated in step 7, and finally get the color cipher text image I'.

3.2 2D discrete wavelet transform

In this paper, 2D discrete wavelet transform can be used to optimize the speed of the image algorithm. By 2D discrete wavelet transform, the image can be divided into low frequency components I_{LL}, high frequency components I_{HH}, vertical components I_{LH}, diagonal components I_{HL}. The R component of Lena after secondary discrete wavelet transform is shown in Fig. 4. It can be seen that most information of the image is concentrated in the upper left corner, i.e., I_{LL},, while the other parts contain little image information, which can be ignored. Therefore, in image encryption, only I_{LL}, of the image can be encrypted, greatly improving the speed of encryption.



(a) before wavelet transform

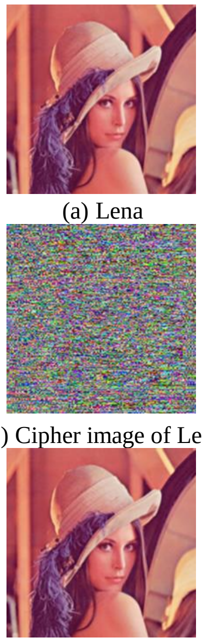
(b) after primary wavelet decomposition

(c) after secondary wavelet decomposition

Fig. 4 *R* component of Lena image before and after wavelet transform

3.1 Experiment results

In this subsection, an experiment for the image encryption algorithm is done by using some frequently-used color images whose size are 512×512, such as Lena, as shown in Fig. 5 (a). Set key as $(\Pi_1,\Pi_2,\Pi_3,\Pi_4,c) = (5,6,7,8,3)$ and $(x_1,x_2,x_3,x_4) = (3,5,-5,-3)$, respectively, and run the image encryption algorithm, the cipher image is obtained, as shown in Fig. 5 (b). Use the same keys, the decrypt images are also obtained by running decryption algorithm, as shown in Fig. 5 (c). It can be found that the decrypt images are consistent with the plain images, which shows the image encryption algorithm proposed in this paper is effective.



(a) Lena

(b) Cipher image of Lena

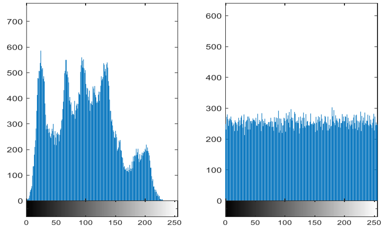
(c) Decrypt image of Lena

Fig. 5 Experiment results

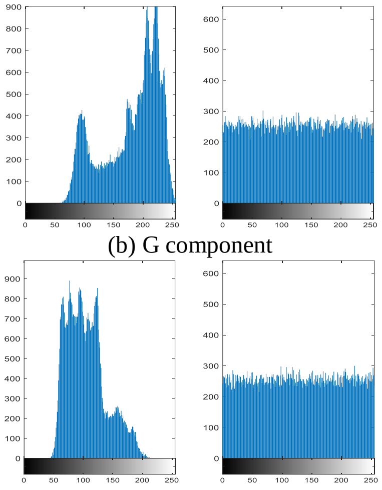
4. Security Analysis of Encryption Algorithm

4.1 Histogram analysis

The image histogram represents the distribution of pixel intensity values in the image. When the histogram of the image is flat and there is no fluctuation trend, it indicates that the encryption algorithm can resist the statistical attack well. Fig.6 shows the histogram of each component of the original image before and after encryption. It can be seen that after the encryption process, the original image with uneven histogram distribution is transformed into a cartographic image with uniform histogram distribution. The results also prove that the image encryption algorithm can resist statistical attacks very well.



(a) R component



(b) G component

(c) B component

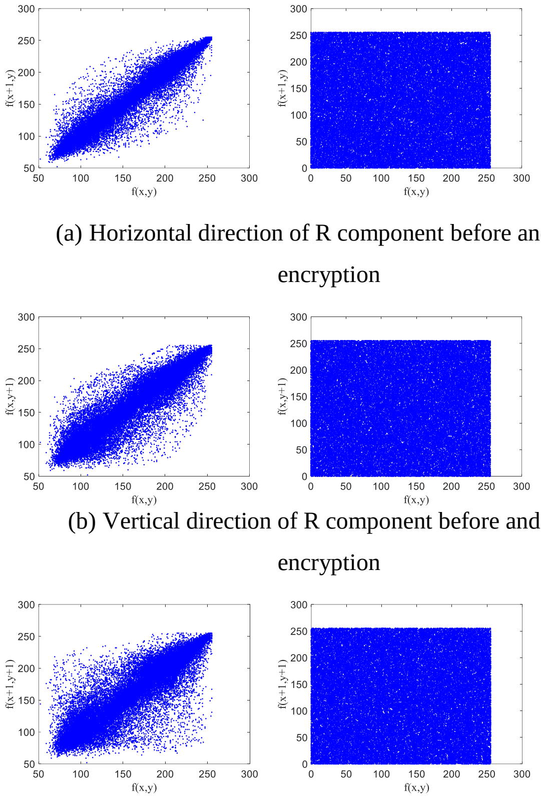
Fig. 6 Histogram of the plain image and the cipher image

4.2 Correlation analysis of adjacent pixels

The correlation between adjacent pixels is one of the important indicators to judge the security of the encryption algorithm. In this paper, a row and a column of pixels are selected from the original image and the encrypted image respectively, and the correlation coefficients between adjacent pixels are shown in Table 1. As can be seen from Table 1, in the plain image, pixels in the vertical, horizontal and diagonal directions are strongly correlated, and the correlation coefficient is basically close to 1. However, the correlation between adjacent pixels in the cipher image is relatively small, and the correlation coefficient is almost close to 0, indicating that weak correlation between adjacent pixels. In addition, correlation of the R component in the plain image and the cipher image is also given to further show difference between them, as shown in Fig. 7. It can be found that the distribution of adjacent pixels in the plain image is highly concentrated, which means a strong correlation. Whereas the distribution of adjacent pixels in the cipher image is random, it means a weak correlation.

Table 1 Corresponding correlation coefficients of plain image and cipher image

image	Plain image			Cipher image		
	R	G	B	R	G	B
Horizontal	0.97757	0.97161	0.95435	0.000756	0.007529	0.004363
Vertical	0.95550	0.94387	0.92538	0.002360	0.002484	0.001545
Diagonal	0.93215	0.91972	0.89641	0.004159	0.002781	0.000881



(a) Horizontal direction of R component before and after encryption

(b) Vertical direction of R component before and after encryption

(c) Diagonal direction of R component before and after encryption

Fig. 7 Correlation between adjacent pixels of R component

4.3 Information entropy analysis

Information entropy is used to characterize the strength of randomness of the system. For an image encryption algorithm with superior performance, the information entropy of the cipher image should be very close to 8. Table 2 shows the calculation results of the information entropy of the plain image and the cipher image. It can be seen that after encryption, the information entropy of the cipher image is closer to 8. Therefore, the algorithm has better information entropy characteristics, strong randomness, and good security.

Table 2 Information entropy of original and encrypted image

Test images	R component	R component	R component
Original image	7.1520	7.2598	6.9110
Cipher image	7.9982	7.9995	7.9986

4.4 Differential attack analysis

For encryption algorithms, NPCR (pixel change rate) and UACI (uniform average change intensity) are usually used to evaluate if they can resist differential attacks well. Generally speaking, the proposed image encryption algorithm can resist differential attacks well, when NPCR is close to 1 and UACI is close to 0.334. NPCR and UACI calculated based on the proposed encryption algorithm are shown in Table 3. It can be seen NPCR of each component is close to 1, and UACI is close to 0.334. Therefore, the algorithm can effectively resist differential attacks.

Table 3 Test results of NPCR and UACI

Index	R component	R component	R component
UACI	0.3365	0.3345	0.3336
NPCR	0.9978	0.9975	0.9967

5. Conclusion

This paper proposes a new image encryption scheme based on a four-dimensional conservative chaotic system and two-dimensional discrete wavelet transform. The four-dimensional conservative chaotic system is used to provide keys in the scrambling and diffusion process, two-dimensional discrete small transform is used to separate the high-frequency coefficients and low-frequency coefficients of the image, respectively. The encryption algorithm has passed various security tests and has strong reliability and security, which can provide technical preparation for the application of the encryption algorithm in confidential communication and data hiding.

References

1. Silva-Garc á, V.M, Flores-Carapia R, Renter á-M árquez, C, et al. Substitution box generation using Chaos: An image encryption application. *Applied Mathematicsand Computation*, 2018, 332:123-135.
2. Tang H, Sun Q, Yang X, et al. A network coding and DES based dynamic encryption scheme for moving target defense. *IEEE Access*, 2018, 6: 26059-26068.
3. Tang Y, Abdul Jalil M Khalaf, Karthikeyan Rajagopal, et al. A new nonlinear oscillator with infinite number of coexisting hidden and self-excited attractors. *Chin. Phys. B*, 2018, 27: 040502.
4. Liu S, Guo C, John T. Sheridan. A review of optical image encryption techniques. *Opt. Laser Technol*, 2014, 57: 327-342.
5. D. Coppersmith. The Data Encryption Standard (DES) and its strength against attacks. *IBM J. Res. Dev*, 1994, 38: 243-250.
6. Liu H, Wang X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt. Commun*, 2011, 284: 3895-3903.
7. Wang L, Song H and Liu P. Sheridan. A novel hybrid color image encryption algorithm using two complex chaotic systems. *Opt. Lasers Eng*, 2016, 77: 118-125.
8. Lin H, Wang C. Influences of electromagnetic radiation distribution on chaotic dynamics of a neural network. *Applied Mathematics and Computation*, 2020, 369: 124840.
9. Zhao Q, Wang C, Zhang X. A universal emulator for memristor, memcapacitor, and meminductor and its chaotic circuit. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2019, 29(1): 013141.
10. Zhang X, Wang C. Multiscroll hyperchaotic system with hidden attractors and its circuit implementation. *International Journal of Bifurcation and Chaos*, 2019, 29(09): 1950117.
11. Zhang X, Wang C, Yao W, et al. Chaotic system with bondorbital attractors. *Nonlinear Dynamics*, 2019, 97(4): 2159-2174.
12. Deng Q, Wang C. Multi-scroll hidden attractors with two stable equilibrium points. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2019, 29(9): 093112.
13. Yu F, Liu L, He B, et al. Analysis and FPGA realization of a novel 5D hyperchaotic four-wing memristive system, active control synchronization, and secure communication application. *Complexity*, 2019, 2019.
14. Robert A, J Matthews. On the derivation of a chaotic encryption algorithm. *Cryptologia*, 1989, 13: 29-42.
15. Jiri Fridrich. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *Int. J. bifurc. chaos*, 1998, 8: 1259-1284.
16. Tan J, Luo Y, Zhou Z, et al. Combined Effect of Classical Chaos and Quantum Resonance on Entan glement Dynamics. *Chin. Phys. Lett*, 2016, 33: 070302.
17. Mohamed Zakariya Talhaou, Wang X. A new fractional one dimensional chaotic map and its application in high-speed Image Encryption. *Signal Processing*, 2017, 141: 109-124.
18. Liu L, Miao S. An image encryption algorithm based on Baker map with varying parameter. *Multimed Tools Appl*, 2017, 76:16511.
19. Chai X, Gan Z, Yuan K, et al. An image encryption scheme based on three-dimensional Brownian motion and chaotic system. *Chin. Phys. B*, 2017, 26: 020504.
20. Wu J, Liao X, Yang B. Color Image Encryption Based on Chaotic Systems and Elliptic Curve ElGamal Scheme. *Signal Processing*, 2017, 141: 109-124.
21. Wang S, Wang C, Xu C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm. *Optics and Lasers in Engineering*, 2019, 128: 105995.

22. Wang X, Zhang J, Zhang F, et al. New chaotical image encryption algorithm based on Fisher Yatess scrambling and DNA coding. *Chin. Phys. B*, 2019, 28: 040504.
23. Mohamed Amine Midoun, Wang X, Mohamed Zakariya Talhaoui. A sensitive dynamic mutual encryption system based on a new 1D chaotic map. *Optics and Lasers in Engineering*, 2021, 139: 106485.
24. Chen H, Liu Z, Camel Tanougast, et al. A novel chaos based optical cryptosystem for multiple images using DNA-blend and gyrator transform. *Optics and Lasers in Engineering*, 2021, 138: 106448.
25. Li Y, Wang C, Chen H. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering*, 2017, 90: 238-246.
26. Li H, Wang Y, Zuo Z. Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms. *Optics and Lasers in Engineering*, 2019, 115: 197-207.
27. Yavuz E. A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme. *Optics & Laser Technology*, 2019, 114: 224-239.
28. Wang M, Wang X, Zhang Y, et al. A novel chaotic encryption scheme based on image segmentation and multiple diffusion models. *Optics & Laser Technology*, 2018, 108: 558-573.
29. Cheng G, Wang C, Chen H. A Novel Color Image Encryption Algorithm Based on Hyperchaotic System and Permutation-Diffusion Architecture. *International Journal of Bifurcation and Chaos*, 2019, 29(09): 1950115.
30. Zhou M, Wang C. A novel chaos based optical cryptosystem for multiple images using DNA-blend and gyrator transform. *Optics and Lasers in Engineering*, 2021, 138: 106448.

Authors Introduction

Mr. Wei Li

He received the B.S. degree from Tianjin University of Science and Technology, Tianjin, China. And now he is studying for a master's degree in electronic information at Tianjin University of Science and Technology.

Ms. Jingwen Liu

She is studying for a master's degree in electronic information at Tianjin University of Science and Technology.

Ms. Hongyan Jia

She received Ph. D. degree in control theory and control engineering from Nankai University in 2010. She is currently an associate professor of the department of automation in Tianjin University of Science and technology.