Multi-image Reorganization Encryption Based on S-L-F Cascade Chaos and Bit Scrambling

Xiaoming Song[1], Daihan Xu[2], Guodong Li[1,*] and Wenxia Xu[1]

[1]*School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin, Guangxi 541001, China*
[2]*School of computer science, Beijing University of Technology, Beijing, 100081, China*
E-mail: lgdzhy@126.com
[*]*Corresponding Author*

Received 01 April 2021; Accepted 11 May 2021;
Publication 24 June 2021

Abstract

Aiming at the problems of small value range of a single chaotic parameter, low sequence chaos, and transient effects, a composite chaotic system of cascaded Sine-Sine mapping, Logistic chaos and generalized third-order Fibonacci is proposed (S-L-F). The new system is highly sensitive to initial values, the maximum spectral entropy of the generated sequence can reach 0.95, and the value range of the parameter x is expanded to [0,4] compared with the traditional Logistic, indicating that the new system is suitable for generating pseudo-random sequences for image encryption. For the problem that the traditional multi-image encryption scheme can only encrypt images of the same type and size, the practicability is poor, and a multi-image encryption scheme based on image reorganization and biting is proposed. The algorithm recombines any number, different sizes and different types of images into a three-dimensional matrix, converts it into a binary matrix, performs bit-level scrambling and surface cyclic scrambling, and then

Journal of Web Engineering, Vol. 20_4, 1115–1130.
doi: 10.13052/jwe1540-9589.20410
© 2021 River Publishers

restores the scrambling matrix to decimal, and the chaotic sequence performs exclusive-or diffusion, and completes simultaneous encryption at one time, which greatly improves the encryption efficiency and scope of application. The NPCR of the ciphertext image is 0.9961, and the UACI is 0.3345, which proves that the ciphertext image can effectively resist the difference attack. The information entropy is greater than 7.999, which can effectively resist attacks. It has certain application value in image information security. Experimental analysis shows that the algorithm has high security and strong practicability.

Keywords: S-L-F Cascade Chaos, bit-level scrambling, Multi-image Encryption, Logistic chaos, Sine-Sine mapping.

1 Introduction

Chaotic system is a dynamic system, which is sensitive to the values put into it and the system parameters, and the trajectory of the system is unpredictable. Using chaos, it can be generated as a random sequence. As long as the initial value and system parameters are given, a fixed random sequence can be obtained. This reproducible pseudo-random sequence has a range of applications in the fields of information security. In recent years, the research on the construction of cascading chaos [1–5] and bit scrambling algorithm [6–8] has gradually been favored by researchers. Tian Miaomiao and Liu Ye [9] designed an picture encryption algorithm using a 5D hyperchaotic system combined with a four-element loop operation. Zhao Hongxiang [10] and others designed an algorithm based on an improved Henon map. Zhu Shuqin et al. [11] designed a class of quadratic polynomial chaos, and based on this, designed a pseudo-random number generator. Guo Yuan [12] and others constructed a generalized Fibonacci chaotic system that can generate a uniform chaotic sequence to generate random templates, and designed an image encryption algorithm with the key adaptively changing with the plaintext. Wang [13], Farah [14], etc. constructed a compound chaotic system based on Logistic mapping [15], Tent mapping, and sine mapping, and designed encryption algorithms by combining DNA encoding technology and S-box technology, respectively. Xian et al. [16] designed an encryption algorithm based on Chen chaotic system combined with chaotic sub-block scrambling and chaotic digital selective diffusion. Cheng et al. [17] designed an encryption scheme based on a hyperchaotic systems, pixel replacement and bit replacement methods. Wu et al. [18] designed an image encryption

scheme based on the Henon-Sine mapping. The parameter range of the mapping is very wide. Chai et al. [19] designed an image encryption scheme using hyperchaotic systems, cellular automata theory and DNA sequence manipulation. Li et al. [21, 22] designed encryption algorithms by generalized chaotic synchronization, and synchronizing two different chaotic systems makes the encryption effect better.

Section 2 introduces the construction and design of the S-L-F system. Section 3 introduces the detailed steps of the image encryption algorithm. Section 4 introduces the simulation results and algorithm security analysis. Section 5 is the conclusion.

2 Chaotic System Construction

Combining Sine-Sine mapping, Logistic chaos and generalized third-order Fibonacci, a cascaded chaotic system is constructed. The Sine-Sine chaotic map is

$$x_{n+1} = mod(\mu \sin(\pi x_n) \times 2^{14}, 1). \tag{1}$$

Logistic chaotic system is expressed as:

$$y_{n+1} = \mu y_n (1 - y_n) \tag{2}$$

$$y_0 = x_0 \tag{3}$$

Combining logistic and Sine-Sine with generalized third-order Fibonacci to construct a cascaded chaotic system is as follows:

$$F_n = mod(x_{n-1}y_{n-1}F_{n-1} + x_{n-2}y_{n-2}F_{n-2} + x_{n-3}y_{n-3}F_{n-3}, 1) \tag{4}$$

$$F_1 = mod(x_1 y_1 \times 2^{14}, 1)$$

$$F_2 = mod(x_2 y_2 \times 2^{14}, 1)$$

$$F_3 = mod(x_3 y_3 \times 2^{14}, 1) \tag{5}$$

In the system, $\mu \in (0.318, 1) \cup (1, 2) \cup (2, 3)$, $x_0 \in (0, 1)$. Figure 1 shows the sequence F_n distribution diagram obtained by the system after 5000 iterations.

Figure 2 shows the spectral entropy of the sequence obtained when the parameter μ takes different values.

It can be seen that the value range of μ is significantly larger than the traditional logistic, and the spectral entropy of the obtained sequence is also around 0.93, closing to the ideal value 1.

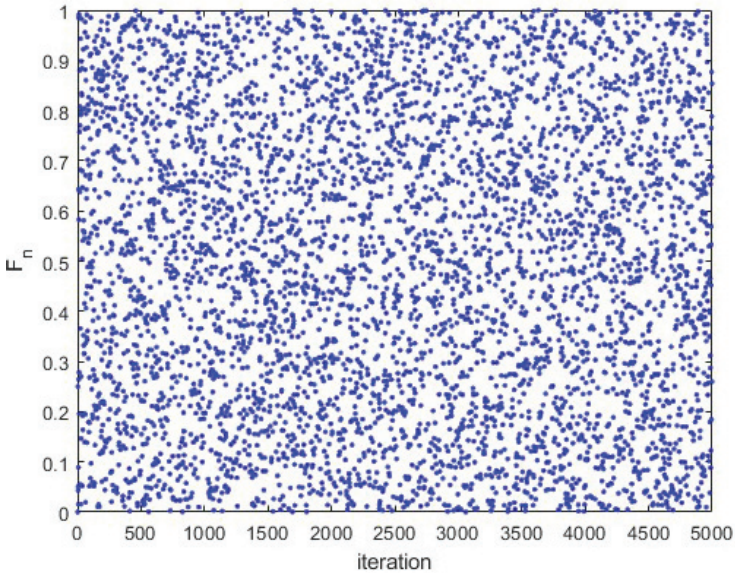

Figure 1 The sequence F_n distribution diagram obtained by the system after 5000 iterations.

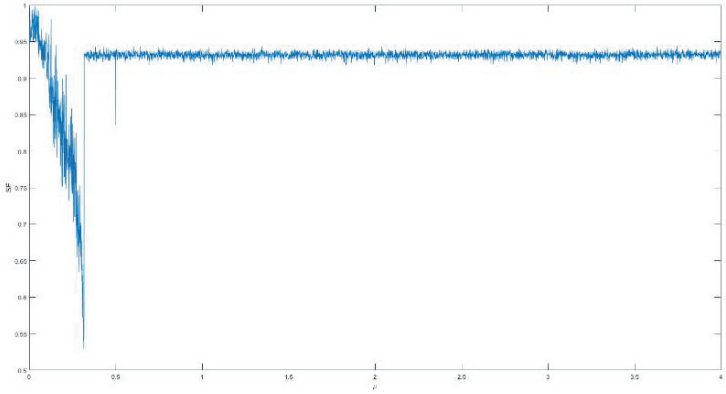

Figure 2 The relationship between parameter μ and the spectral entropy (SE) of the sequence.

Figure 3 shows the sequence $\{F_n\}$ generated after 1000 steps of initial value x_n and $x_n + 10^{-6}$ iteration. It can be seen that even the occurrence of initial values and small changes will greatly affect the generated sequence, indicating that the system has a strong initial value sensitivity.

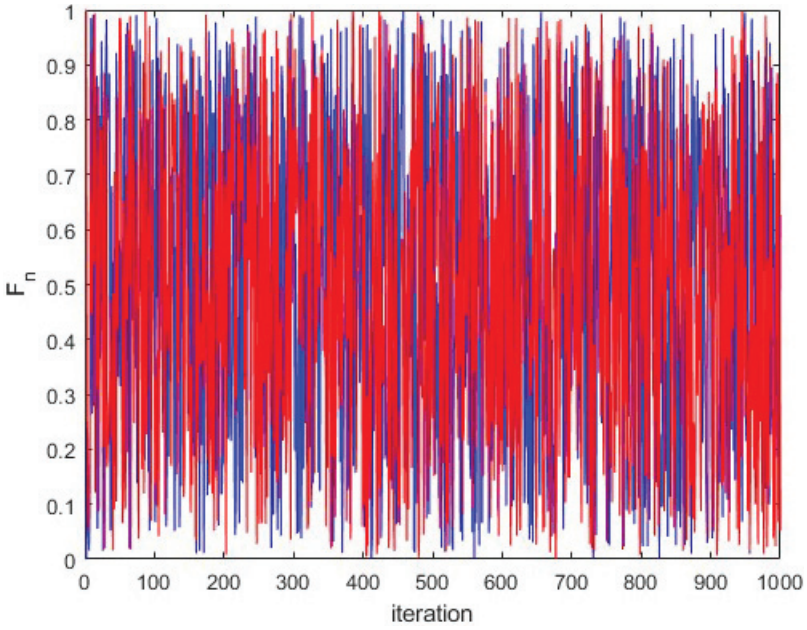

Figure 3 The sequence $\{F_n\}$ generated after 1000 steps of initial value x_n (blue) and $x_n + 10^{-6}$(red) iteration.

3 Proposed Scheme

Figure 4 shows the flow chart of the encryption algorithm.

Step 1 Image reorganization

Read M plaintext images, extract all the pixel values in sequence in the order of row first, then column, and put them into a pre-set $m \times n \times N$ matrix A. The calculation of N is given by Equation (6), where p is the total number of

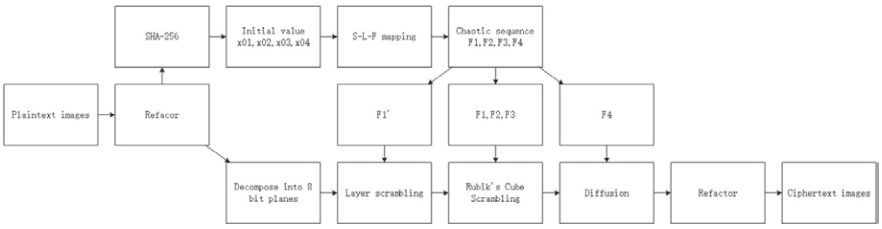

Figure 4 Flow chart of the designed scheme.

pixels of M plaintext images. If there is a vacancy in the nth layer of A, we fill it with an integer of $[0, 255]$.

$$N = \text{ceil}\left(\frac{p}{m \times n}\right), \quad i = 1, 2, \ldots, M \tag{6}$$

Step 2 Construct the chaotic sequence
Extract the first row of each layer of A into a two-dimensional matrix A'. Calculate the sum of all the elements of A and record it as S_A. Pass $A' + S_A$ into the SHA-256 algorithm to obtain a set of 256-bit hash values H. Revert every 8 bits of h as H set of binary numbers to a decimal vector $H' = \{h_1, h_2, \ldots, h_{32}\}$, and construct the initial values $x_{01}, x_{02}, x_{03}, x_{04}$ as follows.

$$\begin{aligned}
x_{01} &= mod\left(\frac{h_1 \oplus h_2 \oplus \cdots \oplus h_8}{256}, 1\right) \\
x_{02} &= mod\left(\frac{h_9 \oplus h_{10} \oplus \cdots \oplus h_{16}}{256}, 1\right) \\
x_{03} &= mod\left(\frac{h_{17} \oplus h_{18} \oplus \cdots \oplus h_{24}}{256}, 1\right) \\
x_{04} &= mod\left(\frac{h_{25} \oplus h_{26} \oplus \cdots \oplus h_{32}}{256}, 1\right)
\end{aligned} \tag{7}$$

Take the parameter μ and substitute the initial values x_{01}, x_{02}, x_{03}, and x_{04} into S-L-F for 1000 iterations, and then iterate $8 \times N$, m, n, $m \times n \times N$ times to get four chaotic sequence T_1, T_2, T_3, T_4. The chaotic sequence is transformed into an applicable sequence by the following processing. Among them, $\text{sort}_{\text{index}}()$ indicates that the sequence is arranged in ascending order, and the index of the corresponding point is taken.

$$\begin{aligned}
F_1 &= \text{ceil}(mod(T_1 \times 2^{10}, 2 \times (m + n))) \\
F_2 &= \text{ceil}(mod(T_2 \times 2^{10}, 2 \times (8 \times N + n))) \\
F_3 &= \text{ceil}(mod(T_3 \times 2^{10}, 2 \times (8 \times N + m))) \\
F_4 &= \text{ceil}(mod(T_4 \times 2^{10}, 256)) \\
F_1' &= \text{sort}_{\text{index}}(F_1)
\end{aligned} \tag{8}$$

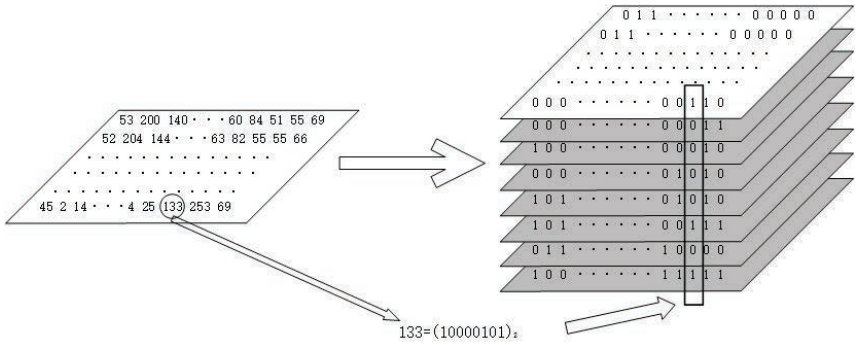

Figure 5 Convert a decimal plane to 8-layer binary plane.

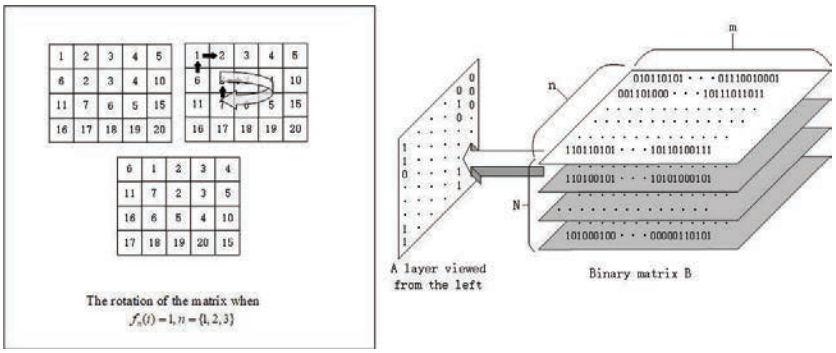

Figure 6 Select a layer from the left to perform surface cycle scrambling operation.

Step 3 Bit scrambling

Arrange the conversion binary of each layer of matrix A from high to low into 8-layer bit planes, as shown in the Figure 5, construct bit matrix B. The layers of the matrix B are scrambled according to the sequence F_1',

$$B'(:,:,i) = B(:,:,F_1'(i)) \tag{9}$$

and the scrambled matrix B' is combined with the sequence F_1, F_2, F_3 from top to bottom, from left to right, and from back to front, to perform surface cyclic scrambling. The specific scrambling method is shown in Figure 6.

Step 4 Image diffusion

Restore the bit matrix scrambled in the previous step to a decimal matrix C, then reconstruct the sequence F_4 into a $m \times n \times N$ matrix F_4', and finally perform a bitwise XOR operation on C and F_4' to obtain the ciphertext matrix

$P = [P_1, P_2, \ldots, P_N]$. Extracting $P = [P_1, P_2, \ldots, P_N]$ layer by layer is the ciphertext image.

4 Experimental Results Analysis

Figure 7 shows the encryption result of the algorithm on the three pictures. The choice of parameter value is $\mu = 2.51$, $m = n = 512$. Three pictures each has different size, one of them is a grayscale picture, and we also choose a picture with text information is selected to further enhance the universality of the algorithm proposed in this paper. Three images were tested on the Windows 10 operating system using Matlab R2018a and Intel Core i7-10750H CPU @ 2.60 GHz and 16.0 GB RAM. From Figure 7, it can be intuitively shown that the ciphertext image has no visual connection with the original image. In the following part, we will conduct a qualitative and quantitative analysis of the statistical properties of the ciphertext image to further prove the safety of the algorithm.

4.1 Histogram Analysis

Histogram can show the distribution of each color in a grayscale image. A good encryption scheme should be able to erase the statistical characteristics

Figure 7 The encryption results of the proposed algorithm.

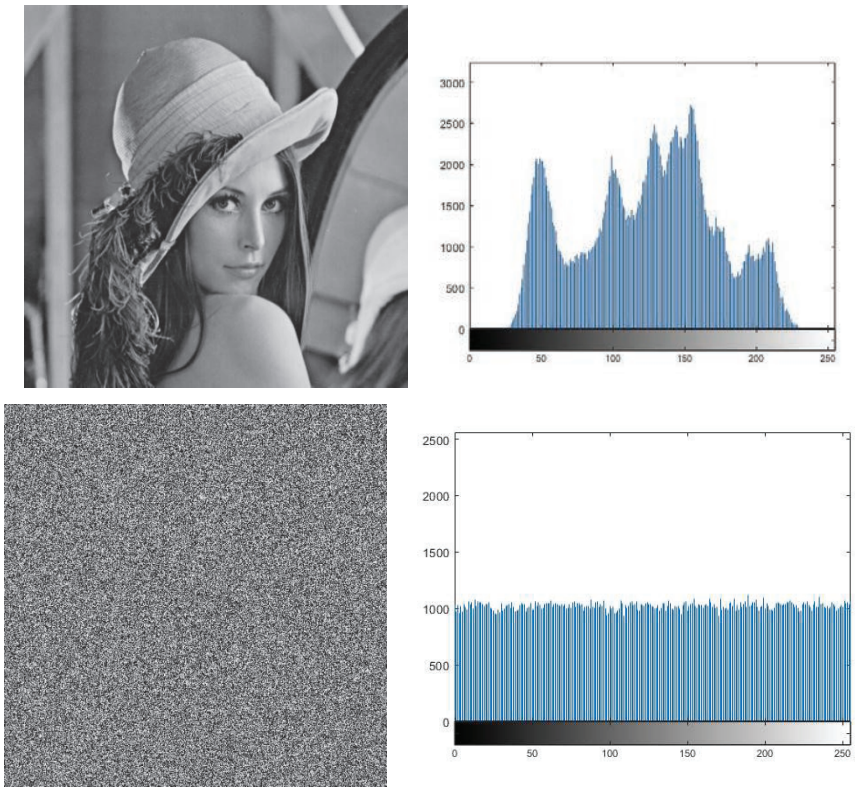

Figure 8 The corresponding histograms of the plaintext image and the ciphertext image.

of the original image, so that the attacker cannot obtain the plaintext image through the statistical properties, thereby protecting the original image information. Figure 8 shows the corresponding histograms of the plaintext and ciphertext image. It can be seen that some statistical characteristics of the plaintext image, while the pixel distribution of the ciphertext image is very even, which conceals its own statistical characteristics, indicating that the algorithm of the article can effectively resist statistical attacks.

We randomly selected 2500 points in the original image and the first ciphertext image, respectively, and calculated the correlation diagrams of their horizontal, vertical, and diagonal adjacent points as shown in the Figure 9. It can be seen from the figure that the neighboring points of the original image have obvious relevant statistical characteristics, and the neighboring points of the ciphertext image do not have obvious statistical characteristics.

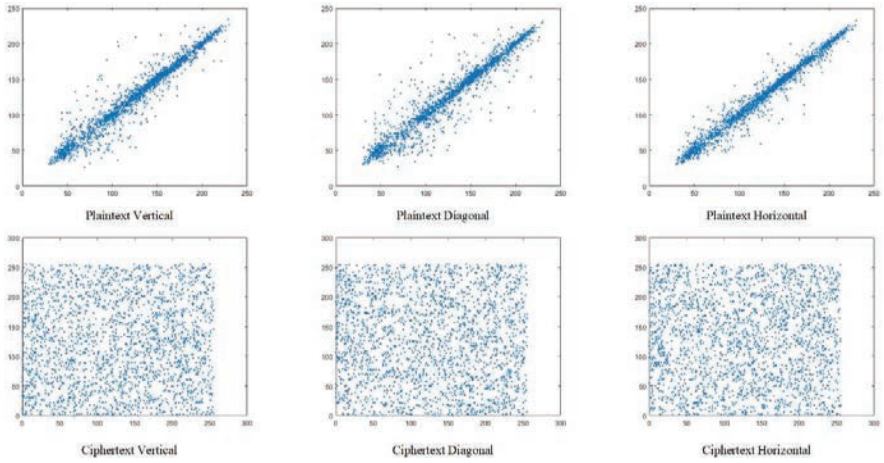

Figure 9 Correlation for the grey value image and its ciphertext image encrypted through the proposed scheme.

4.2 Differential Attack Analysis

The values of NPCR and UACI can reflect the number of changes in pixels of the ciphertext image before and after minor changes are made to the plaintext image and the magnitude of the change in pixel value. The calculation formula is:

$$NPCR = \frac{\sum_{i-1}^{M} \sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \tag{10}$$

$$\begin{cases} D(i,j) = 1, & if\ C(i,j) = C'(i,j) \\ D(i,j) = 0, & if\ C(i,j) \neq C'(i,j) \end{cases} \tag{11}$$

$$UACI = \frac{1}{M \times N} \left(\sum_{i,j} \frac{C(i,j) - C'(i,j)}{255} \right) \times 100\% \tag{12}$$

Among them, M and N represent the rows and columns number of the plaintext image, $C(i,j)$ and $C'(i,j)$ indicate the pixel value at the corresponding position of the ciphertext.

This article randomly selects a pixel of one image from multiple images, and adds 1 to the pixel value of this pixel. Table 1 present the NPCR and UACI value of our algorism. The NPCR value calculated from the ciphertext image and the original ciphertext image is 0.9961, and the UACI value is

Table 1 NPCR and UACI analysis

	Proposed	Ref. [23]
NPCR	0.9961	0.9923
UACI	0.3345	0.3303

Table 2 Entropy analysis

	Proposed	Ref. [22]	Ref. [24]
Entropy	7.9993	7.9417	7.9467

0.3345, indicating that the values of almost all pixels have changed, and the changes are large. This shows that our algorithm can counter the differential attacks well.

4.3 Entropy Analysis of Ciphertext

Information entropy can show the average amount of an information after excluding redundant information from a piece of information The calculation formula is:

$$H(s) = \sum_{i=0}^{255} P(s_i) \log_2 \frac{1}{P(s_i)} \tag{13}$$

Among them, s is the value of a random variable; $P(s_i)$ is the probability density function of the occurrence of s_i. If the probability of all values is equal, then $P(s_i) = \frac{1}{2^8}, i \in \{0, 1, 2, \ldots, 255\}$, means the entropy is 8. Therefore, in the image encryption algorithm, the closer the ciphertext image's entropy is to 8, it means that the encryption makes the image information more uncertain, which means that the scheme can resist attacks based on information entropy.

Table 2 present the entropy of the ciphertext image encrypted by our scheme. The information entropy of our ciphertext image is 7.9993, and compare with other paper than our information entropy obtained is closer to 8. Therefore, the algorithm in this paper can better resist statistical attacks.

5 Conclusion

This paper proposes a composite chaotic system of cascaded Sine-Sine mapping, Logistic chaos and generalized third-order Fibonacci. It also proposes a multi-image encryption algorithm based on bit scrambling, which can

complete multiple-image encryption at one time, which greatly improves the encryption efficiency and scope of application. After encryption, the NPCR value is 0.9961 and the UACI value is 0.3345, which proves that the ciphertext image can effectively resist the difference attack. The information entropy is greater than 7.9993, indicating that the ciphertext image well conceals the image characteristics of the plaintext. Experimental analysis shows that the proposed multi-image encryption algorithm has better encryption effect, strong key sensitivity, excellent security performance indicators, higher encryption efficiency, and can be used in image encryption.

Acknowledgements

The work presented is supported by the financial supports given by research outlay item–Guangxi Key Laboratory of cryptography and information security, and the Guangxi Natural Science Foundation 2018gxnsfaa138177.

References

[1] MENG J. Image encryption with cross colour field algorithm and improved cascade chaos systems. IET Image Processing, 2020, 14: 973–981.

[2] Yuan F, Li YX, Wang GY, A universal method of chaos cascade and its applications, Chaos: An Interdisciplinary Journal of Nonlinear Science 31, 021102 (2021).

[3] Zhao L, Bao LY, Ding HW. S-T linear coupled cascade chaos spread spectrum code and its performance analysis. Telecommunication Engineering, 2021, 61(2):218–223. (in Chinese)

[4] Jin Y, Yuan F, Li YX. Audio encryption method based on cascaded chaotic map. China Sciencepaper, 2020, 15(11):1247–1252+1276. (in Chinese)

[5] Zhao F, Li C, Liu C, et al. Image Encryption Algorithm Based on Sine-Logistic Cascade Chaos, 2019 5th International Conference on Control, Automation and Robotics (ICCAR), 2019, pp. 224–228.

[6] Zhu HG, Dai LW, Liu YT, Wu, LJ, et al. A three-dimensional bit-level image encryption algorithm with Rubik's cube method. Mathematics and Computers in Simulation, 2021, 185: 754–770.

[7] Li CL, Zhou Y, Li HM, et al. Image encryption scheme with bit-level scrambling and multiplication diffusion. *Multimed Tools Appl* (2021).

[8] Jing S, Guo Y, Chen W. Meaningful ciphertext encryption algorithm based on bit scrambling, discrete wavelet transform and improved chaos. IET Image Process. 2021; 15:1053–1071.

[9] MM, Liu Y, Gong LH. Image encryption algorithm based on chaos and quaternary system. Modern Electronics Technique, 2020, 43(23):49–53+57. (in Chinese)

[10] Zhao HX, Xie SC, Zhang JZ, et al. Fast image encryption algorithm based on improved Henon map. Application Research of Computers, 2020, 37(12):3726–3730. (in Chinese).

[11] Zhu SQ, Wang WH, Li JQ. Designing a class of quadratic polynomial chaotic maps and their pseudo random number generator. Computer Engineering and Applications, 2018, 54(09):84–88. (in Chinese).

[12] Guo Y, Xu X, Jing SW, et al. Optical Image Encryption Based on Spiral Phase Transform and Generalized Fibonacci Chaos. Journal of Electronics & Information Technology, 2020, 42(04): 988–996. (in Chinese)

[13] Xing YW, Mao ZZ. A new image encryption algorithm based on ladder transformation and DNA coding. Multimed Tools Appl (2021). https://doi.org/10.1007/s11042-020-10318-5

[14] M. A. Ben Farah, A. Farah, T. Farah. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dynamics, 2020, 99(4): 3041–3064.

[15] May RM. Simple mathematical models with very complicated dynamics. Nature. 1976, 261 (5560):459–467.

[16] Xian YJ, Wang XY, Yan XP, et al. Image Encryption Based on Chaotic Sub-Block Scrambling and Chaotic Digit Selection Diffusion. Optics and Lasers in Engineering, 2020, 134:106202.

[17] Cheng GF, Wang CH, Chen H. A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture. Int. J. Bifurc. Chaos, 2019; 20(9):1950115.

[18] Wu JH, Liao XF, Yang B. Image encryption using 2D hénon-sine map and dna approach. Signal Process, 2018; 153:11–23.

[19] Chai XL, Gan ZH, Yang K, et al. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. Signal Process Image Communication 2017; 52:6–19.

[20] Li GD, Pu Y, Yang B, et al. Synchronization between different hyper chaotic systems and dimensions of cellular neural network and its design in audio encryption . Cluster Computing, 2018, 22: 7423–7434.

[21] Li GD, Yang B, Pu Y, et al. Synchronization of Generalized Using to Image Encryption. International Journal of Pattern Recognition & Artificial Intelligence, 2017, 31(6).
[22] Mao J, Wang HY, Chen Y. Image encryption algorithm based on dynamic key selection and multi-direction diffusion. Optical Technique, 2018, 44(03): 278–286. (in Chinese).
[23] Khan JS, Ahmad J. Chaos based efficient selective image encryption. Multidimensional Systems and Signal Processing, 2019, 30(2):943–961.
[24] Lin Q, Wang YJ, Wang Q. The image encryption scheme with optional dynamic state variables based on hyperchaotic system. Scientia Sinica (Technologica), 2016, 46(09): 910–918. (in Chinese)

Biographies

Xiaoming Song is a graduate student. Become a student of the School of Mathematics and Computing Science of Guilin University of Electronic Technology in the fall of 2020. His work centers on chaos theory, discussing information and image encryption solutions based on chaos theory.

Daihan Xu is an undergraduate student at the Beijing Institute of Technology. She is interested in artificial neutral network and deep learning. At present, she works on data analysis, information security and image encryption, under supervision of Prof. Guodong Li.

Guodong Li is a professor at the School of Mathematics and Computational Science, Guilin University of Electronic Technology. He was a professor in the Department of Applied Mathematics of Xinjiang University of Finance and Economics. His current research interests include information security, image processing, and data mining.

Wenxia Xu is an associate professor at the School of Mathematics and Computational Science, Guilin University of Electronic Technology. She was a professor in the Department of Applied Mathematics of Xinjiang University of Finance and Economics. Her current research interests include information security, image processing, and data mining.