

Image encryption algorithm based on multiple chaotic systems and improved Joseph block scrambling

Dingkang Mou(牟定康) and Yumin Dong(董玉民)

Citation: Chin. Phys. B, 2024, 33 (**10**): 104205. DOI: 10.1088/1674-1056/ad6257
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

High-quality ghost imaging based on undersampled natural-order Hadamard source

Kang Liu(刘炕), Cheng Zhou(周成), Jipeng Huang(黄继鹏), Hongwu Qin(秦宏伍), Xuan Liu(刘轩), Xinwei Li(李鑫伟), and Lijun Song(宋立军)
Chin. Phys. B, 2024, 33 (**9**): 094204. DOI: 10.1088/1674-1056/ad62e1

Single exposure passive three-dimensional information reconstruction based on an ordinary imaging system

Shen-Cheng Dou(窦申成), Fan Liu(刘璠), Hu Li(李虎), Xu-Ri Yao(姚旭日), Xue-Feng Liu(刘雪峰), and Guang-Jie Zhai(翟光杰)
Chin. Phys. B, 2023, 32 (**11**): 114204. DOI: 10.1088/1674-1056/ace764

Optical encryption scheme based on spread spectrum ghost imaging

Jin-Fen Liu(刘进芬), Yue Dong(董玥), Le Wang(王乐), and Sheng-Mei Zhao(赵生妹)
Chin. Phys. B, 2023, 32 (**7**): 074202. DOI: 10.1088/1674-1056/acbf27

A probability theory for filtered ghost imaging

Zhong-Yuan Liu(刘忠源), Shao-Ying Meng(孟少英), and Xi-Hao Chen(陈希浩)
Chin. Phys. B, 2023, 32 (**4**): 044204. DOI: 10.1088/1674-1056/ac981e

Ghost imaging based on the control of light source bandwidth

Zhao-Qi Liu(刘兆骐), Yan-Feng Bai(白艳锋), Xuan-Peng-Fan Zou(邹璇彭凡), Li-Yu Zhou(周立宇), Qin Fu(付芹), and Xi-Quan Fu(傅喜泉)
Chin. Phys. B, 2023, 32 (**3**): 034210. DOI: 10.1088/1674-1056/ac6edd

---

Image encryption algorithm based on multiple chaotic systems and improved Joseph block scrambling

Dingkang Mou(牟定康) and Yumin Dong(董玉民)[†]

College of Computer and Information Science, Chongqing Normal University, Chongqing 400047, *China*

(Received 19 June 2024; revised manuscript received 8 July 2024; accepted manuscript online 12 July 2024)

With the rapid development of digital information technology, images are increasingly used in various fields. To ensure the security of image data, prevent unauthorized tampering and leakage, maintain personal privacy, and protect intellectual property rights, this study proposes an innovative color image encryption algorithm. Initially, the Mersenne Twister algorithm is utilized to generate high-quality pseudo-random numbers, establishing a robust basis for subsequent operations. Subsequently, two distinct chaotic systems, the autonomous non-Hamiltonian chaotic system and the tent-logistic-cosine chaotic mapping, are employed to produce chaotic random sequences. These chaotic sequences are used to control the encoding and decoding process of the DNA, effectively scrambling the image pixels. Furthermore, the complexity of the encryption process is enhanced through improved Joseph block scrambling. Thorough experimental verification, research, and analysis, the average value of the information entropy test data reaches as high as 7.999. Additionally, the average value of the number of pixels change rate (NPCR) test data is 99.6101%, which closely approaches the ideal value of 99.6094%. This algorithm not only guarantees image quality but also substantially raises the difficulty of decryption.

Keywords: mersenne twister algorithm, DNA coding confusion, pixel XOR operation, improved Joseph block scrambling

PACS: 42.30.Va, 07.05.Pj **DOI:** 10.1088/1674-1056/ad6257

1. Introduction

With the rapid development of information technology, digital images have been widely used in many fields, such as medical imaging, communication transmission, and social media, and play an indispensable role in modern society. However, the accompanying image security and privacy protection issues are receiving increasing attention. In this context, image encryption technology has gradually attracted widespread research interest as a key information security measure.[1,2] Scientific research in the field of image encryption mainly focuses on how to effectively protect the content security of digital images during storage, transmission, and processing to prevent unauthorized access and malicious tampering.[3]

Early image encryption algorithms mainly focused on single chaotic systems, pixel scrambling, or XOR operations.[4,5] However, in recent years, the field of image encryption has undergone profound interdisciplinary crossover and has been widely and deeply studied.[6,7] Lai *et al*. developed a two-dimensional hyperchaotic map by combining mathematical functions and sine chaotic maps, and proposed a cross-channel color image encryption algorithm that can effectively resist various illegal attacks.[8] Zhang *et al*. developed a multi-image encryption algorithm that integrates row-column confusion and closed-loop bidirectional diffusion. This algorithm notably enhances encryption efficiency while maintaining adequate security.[9] Guo *et al*. introduced a dual-channel image encryption and authentication algorithm utilizing computational ghost imaging, demonstrating promising application potential.[10] Chen *et al*. established a framework for creating super-enhanced memristive hyperchaotic maps, derived four chaotic maps, and utilized them in the design of image encryption algorithms.[11] Gong *et al*. studied a dual-color image watermarking algorithm based on geometric correction by combining least squares support vector regression with quaternion fractional-order orthogonal Fourier–Mellin matrix. Their algorithm has good robustness and imperceptibility.[12] Jiang *et al*. proposed a quantum image encryption algorithm based on the dual quantum image model and hyperchaotic system, which enhanced the ability to resist attacks and interference.[13] Zhou *et al*. studied a multi-color image encryption algorithm based on a bit-level extension algorithm and verified the effectiveness and reliability of the algorithm through comprehensive analysis.[14] Zhou *et al*. proposed a multi-image encryption algorithm based on quaternion discrete fractional-order Chebyshev differential matrix transformation and cross-coupled chaotic system. The algorithm performs double-layer encryption processing in the vertical and horizontal directions of the image.[15] In the field of physics, advanced technologies such as optical image encryption and quantum image encryption have emerged.[16,17] Simultaneously, the field of computer science is actively exploring image encryption techniques related to neural networks and deep learning.[18–20] Research in the field of biology also involves DNA-based image encryption methods.[21,22] These interdisciplinary studies not only provide a rich theoretical foundation for image encryption but also introduce innovative ideas that have beneficially promoted the further development and application expansion of image encryption technology.[23]

[†]Corresponding author. E-mail: dym@cqnu.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

In this study, we designed a color image encryption scheme based on multiple chaotic systems and improved Joseph block scrambling. The main contributions of our study are as follows. (I) Based on the Mersenne Twister algorithm, we have developed a high-quality pseudo-random number generator. This generator can produce highly random and unpredictable keys, greatly enhancing the security of data encryption. (II) The random chaotic sequences generated by the autonomous non-Hamiltonian chaotic system[26,27] and the tent-logistic-cosine chaotic mapping[28,29] can effectively control the encoding and decoding process of DNA to meet various security requirements and application scenarios. (III) Based on the principles of the Joseph algorithm, we propose an enhanced Joseph block scrambling technique. This technology aims to increase the complexity and unpredictability of the image encryption process, ensuring the confidentiality and integrity of the image during transmission and storage.

In Section 2, we discuss related research works on color image encryption schemes. Sections 3 and 4 provide a detailed description of the specific process and steps involved in color image encryption. Section 5 deeply analyzes the research results and experimental data obtained, comprehensively evaluating the feasibility of the proposed scheme. The last section summarizes the color image encryption schemes and anticipates future developments in the field of image encryption.

2. Related work

2.1. Pseudo-random number generator

As a high-quality pseudo-random number generator in the field of computer science application design, the Mersenne Twister algorithm is known for its long period and good statistical properties.[24] We developed a dice game using the Mersenne Twister algorithm and utilized it as the key for the color image encryption algorithm.[25] The game costs \$0 to start, and two dice are rolled simultaneously in each round. When the numbers on the two dice are the same, the player will receive a bonus five times the value of the random number. If the numbers are different, the random number bonus will be doubled and deducted.

$$\text{Total} = \begin{cases} 5 \times \text{random}_{\text{bonus}}, & \text{dice}_1 = \text{dice}_2, \\ -\text{random}_{\text{bomus}}, & \text{dice}_1 \neq \text{dice}_2. \end{cases} \tag{1}$$

Figure 1 shows the trend chart resulting from 100 sets of comparative experiments and 1000 simulations. The data shows a high degree of complexity and lacks regularity.

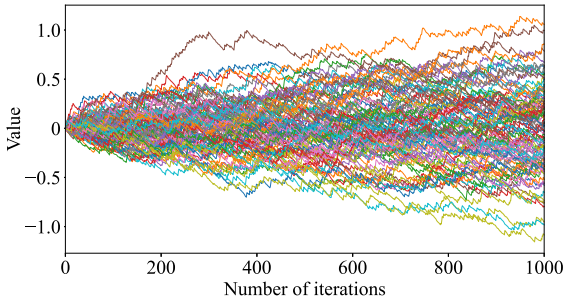


Fig. 1. Pseudo-random number generator.

2.2. Autonomous non-Hamiltonian chaotic system

Based on the foundation of Hamiltonian chaotic systems, autonomous non-Hamiltonian chaotic systems are highly sensitive to small changes in the initial conditions. Its trajectory is complex and random, making it difficult to predict accurately.[26,27] The expression is as follows:

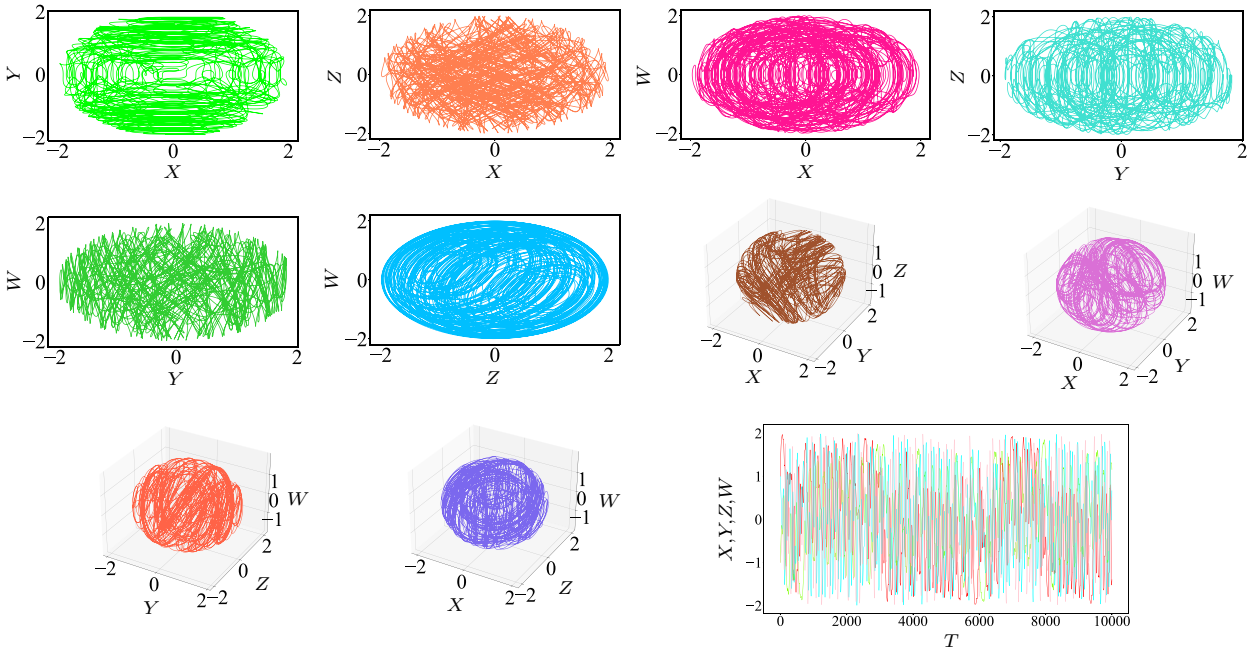


Fig. 2. Motion trajectories in different dimensions.

$$\begin{cases} x = a \cdot y \cdot w, \\ y = x \cdot z, \\ z = -x \cdot y + b \cdot w, \\ w = -c \cdot x \cdot y - d \cdot z. \end{cases} \tag{2}$$

When the parameter $a = b = c = d = 2$ and the initial condition $x = z = 1, y = w = -1$, Fig. 2 vividly shows the motion trajectory of the four-dimensional autonomous non-Hamiltonian chaotic system in different dimensions.

2.3. TLC chaotic mapping

The TLC chaotic mapping introduces the cosine trigonometric function based on the tent chaotic mapping and the logistic chaotic mapping, thus creating a new composite chaotic mapping.[28,29] TLC chaotic mapping not only retains its basic properties but also enhances the complexity and diversity of the system, leading to richer chaotic dynamic behaviors. The expression is as follows:

$$p(i+1) = \begin{cases} \cos(\pi(2 \cdot r \cdot p(i) + 4 \cdot (1-r) \cdot p(i) \cdot (1-p(i)) - 0.5)), & p(i) < 0.5, \\ \cos(\pi(2 \cdot r \cdot (1-p(i)) + 4 \cdot (1-r) \cdot p(i) \cdot (1-p(i)) - 0.5)), & p(i) \geq 0.5. \end{cases} \tag{3}$$

When the parameter $r = 0.987654321$ and the initial condition $p = 0.456789123$, Fig. 3 fully presents the overall situation of the TLC chaotic mapping.

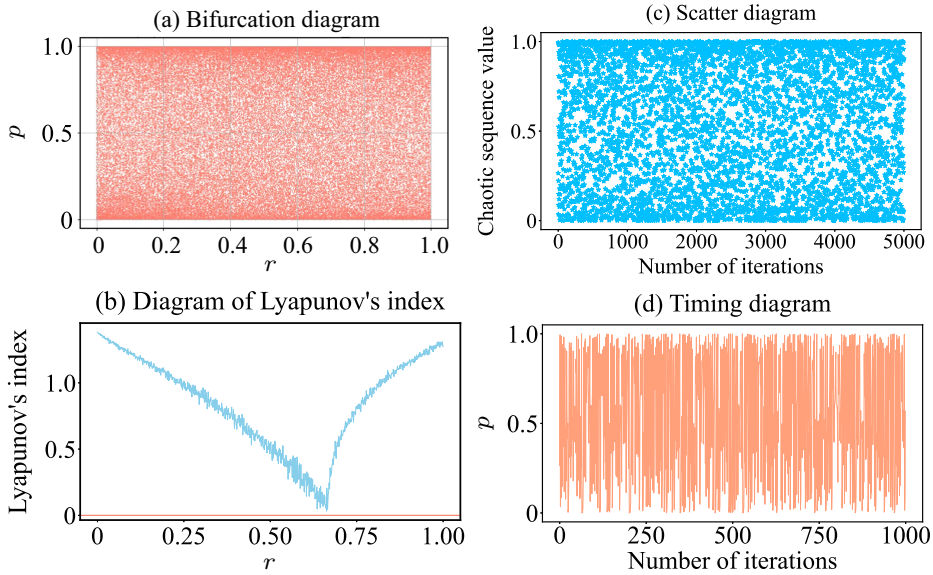


Fig. 3. Random sequence distribution of TLC chaotic mapping.

2.4. DNA coding

In the field of image encryption, DNA coding significantly enhances the security of encryption algorithms, and improves the confidentiality and integrity of image data by converting image pixel data into DNA sequences. This is achieved by leveraging the unique combination and sequence properties of DNA. The detailed DNA coding rules are shown in Fig. 4.

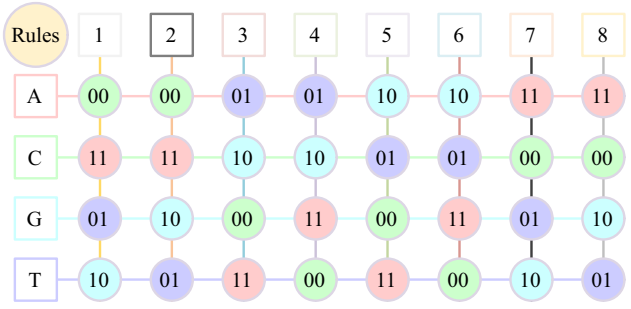


Fig. 4. DNA coding rules.

DNA coding technology utilizes a combination of mathematical operations, including addition, subtraction, and XOR, to enhance the complexity of the encryption process. This ensures that data is not easily tampered with or leaked during transmission and storage. The specific calculation method is shown in Fig. 5.

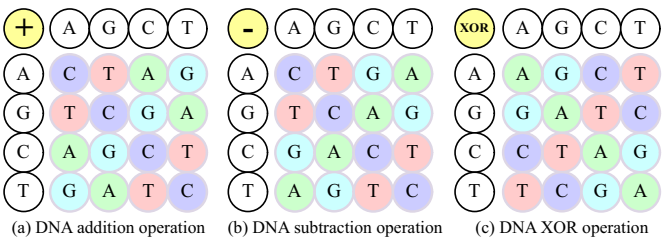


Fig. 5. DNA computing operations.

2.5. Improved Joseph problem

The Joseph problem is a classic puzzle in mathematics and computer science. It arranges a group of objects in a cir-

cle, starting from a specific point, and counting in a cycle according to fixed rules. Whenever the count reaches a certain number, the current object will be removed until only one object is left.[30,31]

We have improved the Joseph problem. After each traversal, we reverse the sequence after object U and place it in front of object U. At the same time, the sequence in front of object U is arranged in positive order and placed behind object U. This process is then iterated to achieve optimization. Figure 6 illustrates the detailed implementation of the enhanced Joseph problem, with 16 objects being arranged and nine as the initial value.

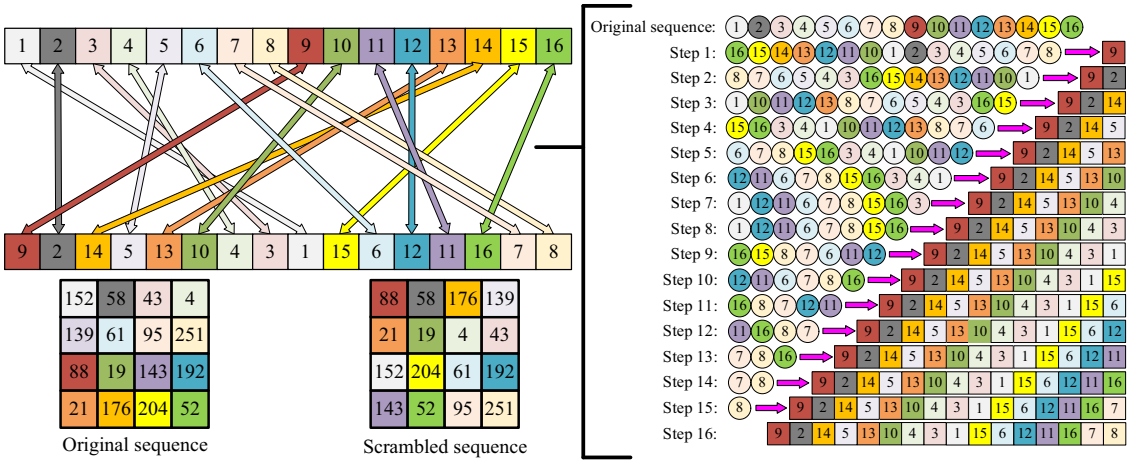


Fig. 6. Improved Joseph problem.

3. Color image encryption algorithm

3.1. Key generation

Based on the dice game introduced above, we simulated and recorded the results of each throw to generate a highly complex and irregular pseudo-random sequence $K = \{k_1, k_2, \ldots, k_n\}$. The random sequence K is then used as the initial key to demonstrate the complex and unpredictable behaviors of the two chaotic systems. The values of the initial key K are presented in Table 1.

Table 1. ISCM parameter values.

Parameter	Parameter values	Parameter	Parameter values
p_1	k_1 =0.6305649609929008	r_1	k_2 =0.37467144716866357
p_2	k_3 =0.8872061131379535	r_2	k_4 =0.47332341075940884
x	k_5 =0.47252460239982186	y	k_6 =0.31789340297042483
z	k_7 =0.7511157012734713	w	k_8 =0.6919659608146955

3.2. XOR confusion

Based on the initial condition of TLC chaotic mapping as $p_1 = k_1$, $r_1 = k_2$, we performed $3wh$ iterations to generate the chaotic random sequence P_{1_m}. Then, we use the chaotic random sequence P_{1_m} to perform XOR confusion operation on the pixel data of the entire color image to provide reliable protection for image transmission and storage.

$$\begin{cases} P_{1_m} = \mathrm{mod}(\mathrm{int}(p_{1_m} \times 10^8), 256), \\ \mathrm{New_Pixel}_m = \mathrm{Pixel}_m \oplus X_{1_m}, \end{cases} \quad m = 1, 2, \ldots, 3wh. \tag{4}$$

3.3. Pixel scrambling

Based on the initial condition of TLC chaotic mapping as $p_2 = k_3, r_2 = k_4$, we performed $3wh$ iterations to generate the chaotic random sequence P_{2_m}. At the same time, all pixel information of image G is merged into a sequence Seq of size $3wh$. Then, P_{2_m} and Seq are integrated into a two-dimensional array and arranged in ascending order according to the numerical relationship of P_{2_m}, which effectively scrambles the original pixel information in Seq to obtain a new sequence New_Seq. Finally, New_Seq is evenly assigned to the RGB channels of the color image and combined into a new scrambled image New_G.

$$\begin{cases} P_{2_m} = P_{2_1} : P_{2_3wh}; \\ \mathrm{Seq} = \mathrm{Seq}_1 : \mathrm{Seq}_{3wh}; \\ \mathrm{New_}G = G(\mathrm{New_sort(Seq)}). \end{cases} \tag{5}$$

$$\begin{cases} R = [\mathrm{New_}G(1) : \mathrm{New_}G(wh)], \\ G = [\mathrm{New_}G(wh+1) : \mathrm{New_}G(2wh)], \\ B = [\mathrm{New_}G(2wh+1) : \mathrm{New_}G(3wh)]. \end{cases} \tag{6}$$

3.4. DNA encoding and decoding

Based on the initial condition of TLC chaotic mapping as $x = k_5$, $y = k_6$, $z = k_7$, $w = k_8$, we performed $3wh$ iterations to generate the chaotic random sequence X, Y, Z, W. $X, Y, Z; W$ are used in four different ways to control the DNA encoding

process, including maximum, sum, average, and sum. The specific operation methods are shown in Table 2. The DNA encoding process can be flexibly controlled and optimized according to specific needs, making it suitable for various application scenarios and optimization goals. The decoding process of DNA is similar to the encoding process, and the detailed operational process is shown in Table 3.

Table 2. DNA encoding process.

No.	Control parameters	Chaotic segmentation	Encoding
1	$\text{Mod}(\text{Max}(X,Y,Z,W)\times 10^8,32)$	1,5,9,13,17,21,25,29	ACGT
2	$\text{Mod}(\text{Sum}(X,Y,Z,W)\times 10^8,32)$	2,6,10,14,18,22,26,30	CATG
3	$\text{Mod}(\text{Avg}(X,Y,Z,W)\times 10^8,32)$	3,7,11,15,19,23,27,31	GATC
4	$\text{Mod}(\text{Min}(X,Y,Z,W)\times 10^8,32)$	4,8,12,16,20,24,28,32	TCGA

Table 3. DNA encoding process.

No.	Control parameters	Chaotic segmentation	Encoding
1	$\text{Mod}(\text{Min}(X,Y,Z,W)\times 10^8,32)$	4,8,12,16,20,24,28,32	AGCT
2	$\text{Mod}(\text{Avg}(X,Y,Z,W)\times 10^8,32)$	3,7,11,15,19,23,27,31	CTAG
3	$\text{Mod}(\text{Sum}(X,Y,Z,W)\times 10^8,32)$	2,6,10,14,18,22,26,30	GTAC
4	$\text{Mod}(\text{Max}(X,Y,Z,W)\times 10^8,32)$	1,5,9,13,17,21,25,29	TGCA

3.5. Improved Joseph block scrambling

In the previous article, we discussed in depth how to improve the Joseph problem. Now, we introduce this optimization strategy into the scenario of image block scrambling. We divide the image into 8×8 block matrices and start scrambling from an initial value of 2. By incorporating the improved Joseph algorithm into the image processing process, we can achieve a more diverse block scrambling. We applied the enhanced Joseph block scrambling operation to various images and presented the results in Fig. 7.

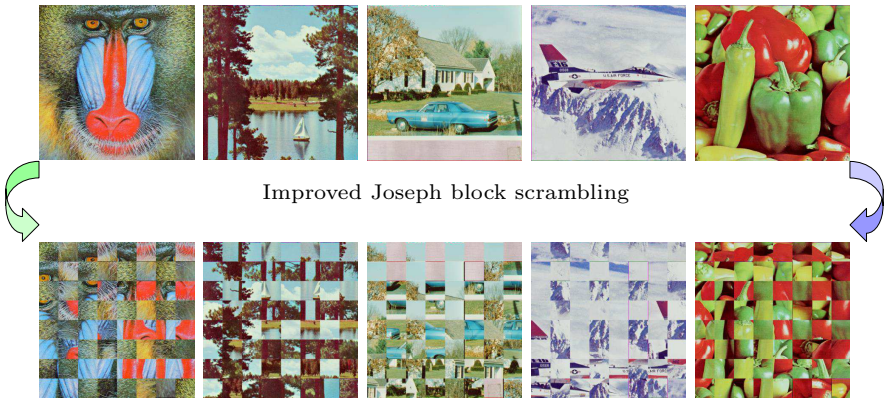


Fig. 7. Improved Joseph block scrambling effect.

4. Color image encryption and decryption process

4.1. Color image encryption process

The goal of image encryption is to ensure the security of image content to prevent unauthorized access or interpretation. By processing the image, unauthorized users or systems can be effectively prevented from obtaining image information. The following will briefly explain the steps of the color image encryption algorithm we proposed.

Step 1 Generate an unpredictable random sequence $K=\{k_1,k_2,\ldots,k_n\}$ using a high-quality pseudo-random number generator based on the Mersenne Twister algorithm, and use K as the initial key.

Step 2 Set the parameter value of the TLC chaotic mapping to $p_1=k_1$, $r_1=k_2$ and iterate $3wh$ times to generate a chaotic sequence P_{1_m}.

Step 3 Use the chaotic sequence P_{1_m} to perform an XOR operation on the pixel data of the image to enhance the complexity of image encryption.

Step 4 Set the parameter value of the TLC chaotic mapping to $p_2=k_3$, $r_2=k_4$ and iterate $3wh$ times to generate the chaotic sequence P_{2_m}.

Step 5 Use the chaotic sequence P_{2_m} to confuse the image information.

Step 6 Set the parameter value of the autonomous non-Hamiltonian chaotic system to $x=k_5,y=k_6,z=k_7,w=k_8$, and iterate $3wh$ times to generate the chaotic sequence X, Y, Z, W.

Step 7 Use the chaotic sequence X, Y, Z, W in different ways to control the DNA encoding process to ensure data security and reliability.

Step 8 Use the chaotic sequence X, Y, Z, W to control the operation of DNA decoding in a similar way.

Step 9 Improved Joseph block scrambling processing. We use a block matrix with an 8×8 resolution to introduce more detailed changes in image processing.

4.2. Color image decryption process

Image decryption is a highly complex and sophisticated process with the goal of successfully restoring an encrypted image to its original state. Our color image decryption process is essentially the reverse operation of the image encryption process. During this process, the information in the ciphertext will be carefully analyzed and processed to restore the original features and details of the image.

5. Experimental results and analysis

The hardware environment of the experiment includes an AMD Ryzen 7 5800H processor with a main frequency of 3.20 GHz and 16.0 GB of RAM. All simulation experiments are implemented in the Python 3.9 environment.

Our proposed algorithm focuses on processing images with a resolution of 512×512 (it can actually be applied to any resolution). The algorithm can preserve the integrity of the original image and minimize pixel distortion to an imperceptible level. The experimental results are shown in Fig. 8.

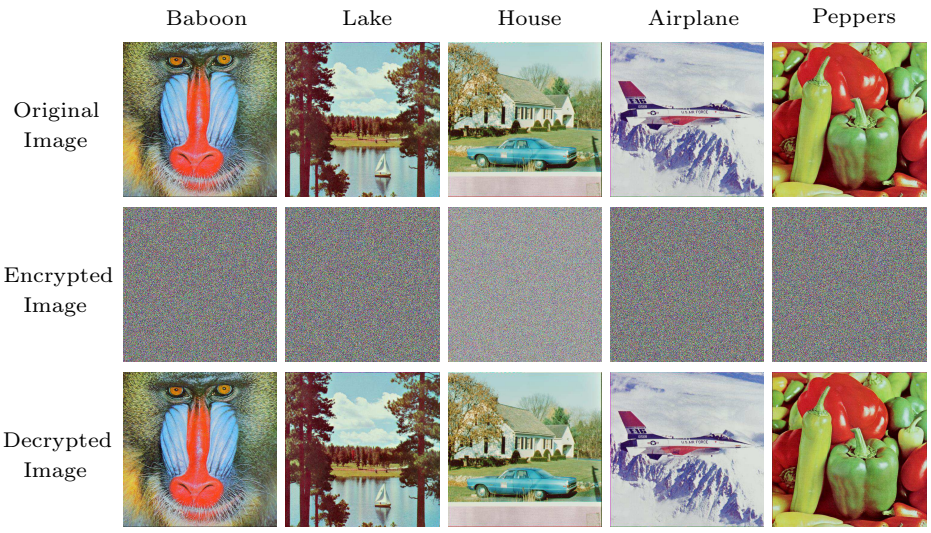


Fig. 8. Experimental effect comparison.

5.1. Fourier spectrum analysis

Fourier spectrum analysis is used to transform images from the spatial domain to the frequency domain for a comprehensive analysis of the contribution of various frequency components in the image. This process aids in gaining a profound understanding of the structure, texture, and characteristics of the image.[32] We conducted Fourier spectrum analysis on both the original image and the encrypted image, and present the detailed experimental results in Fig. 9. Experimental analysis demonstrates that the encryption process scrambles the pixel data of the image, resulting in blurred features of the original image and effectively safeguarding the image's privacy.

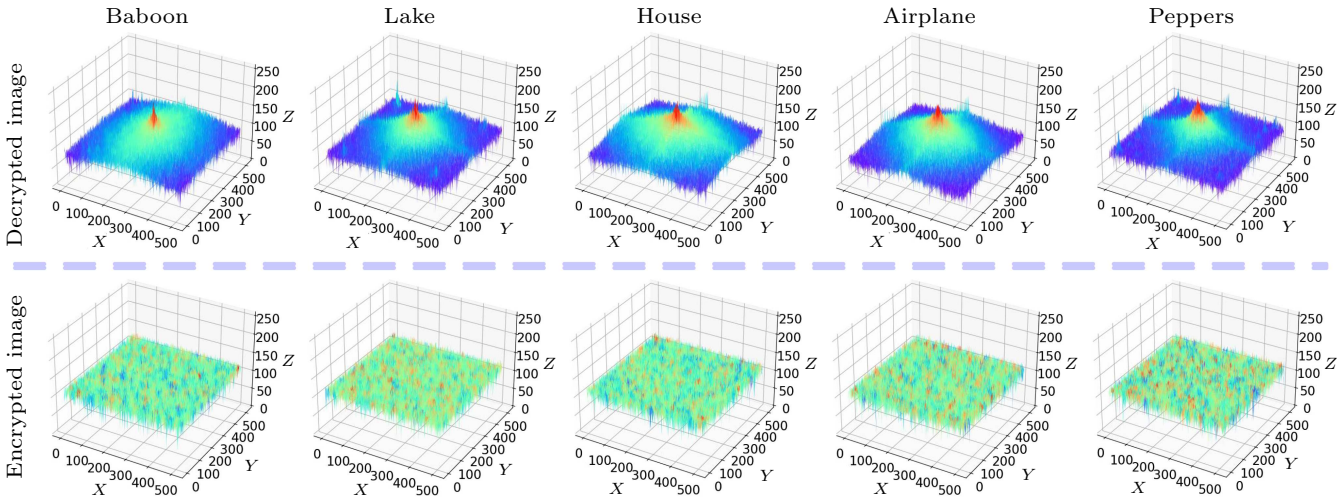


Fig. 9. Fourier spectrum analysis.

5.2. Correlation analysis of adjacent pixels

Adjacent pixel correlation analysis plays a significant role in evaluating image encryption algorithms in terms of privacy protection and preventing data leakage. It has become an important criterion for measuring the security performance and effectiveness of image encryption.[33] The calculation formula is as follows:

$$R_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{7}$$

$$\mathrm{cov}(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))(y_i - E(y)), \tag{8}$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i, \tag{9}$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))^2, \tag{10}$$

where R_{xy} is the correlation between adjacent pixels, $\mathrm{cov}(x,y)$ is the covariance between the two pixels x and y, $\sqrt{D(x)}$ is the standard difference, $D(x)$ is the variance, and $E(x)$ is the mean.

We conducted a correlation analysis of adjacent pixels on multiple encrypted images and presented the results in Fig. 10. Moreover, we selected the image "Baboon" as the focus of our research and conducted a comprehensive comparison with other image encryption algorithms. The detailed experimental data are recorded in Table 4. The results show that the algorithm we proposed can not only maintain image privacy but also successfully ensure the security of data.

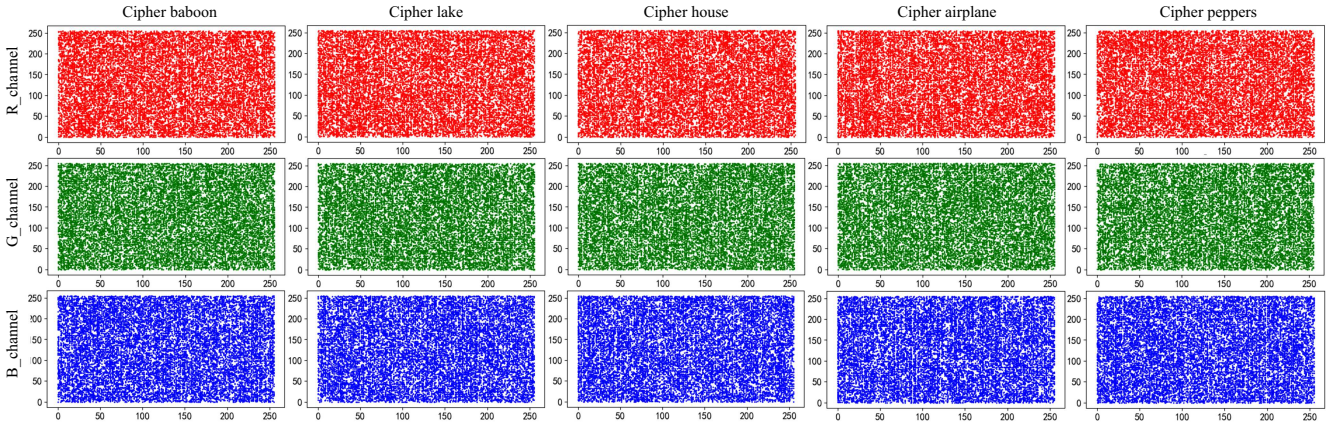


Fig. 10. Effect of adjacent pixel correlation on encrypted image.

Table 4. Comparison data of adjacent pixel correlation analysis.

Test	Component	Cipher baboon	Ref. [34]	Ref. [35]	Ref. [36]	Ref. [37]
Horizontal	red	–0.0002	–0.0023	–0.0031	0.0006	0.0014
	green	–0.0047	0.0014	–0.0046	–0.0065	–0.0081
	blue	0.0042	0.0029	0.0056	–0.0021	–0.0089
Vertical	red	–0.0022	–0.0041	–0.0052	0.0016	0.0046
	green	–0.0005	–0.0044	–0.0049	–0.0007	0.0008
	blue	0.0018	–0.0033	–0.0022	0.0015	0.0001
Diagonal	red	–0.0010	–0.0019	0.0074	0.0022	0.0003
	green	0.0027	–0.0055	–0.0059	0.0027	0.0053
	blue	0.0020	–0.0004	–0.0043	0.0010	0.0017

5.3. Peak signal-to-noise ratio analysis

Peak signal-to-noise ratio (PSNR) is widely used to compare the similarity between the original signal and the processed signal to evaluate the quality of signals, such as images and audio. The calculation expression is as follows:

$$\mathrm{MSE} = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(I(i,j) - I'(i,j)\right)^2, \tag{11}$$

$$\mathrm{PSNR} = 10 \cdot \log_{10}\frac{(2^n - 1)^2}{\mathrm{MSE}}. \tag{12}$$

Here MSE is the mean square error, $I(i,j)$ and $I'(i,j)$ are the data information of the original image and the encrypted image at the pixel position (i,j), respectively.

We conducted PSNR analysis on the three independent RGB channels of both the original image and the encrypted image. The specific experimental data are shown in Table 5. The results show significant differences in each channel between the encrypted image and the original image.

Table 5. PSNR analysis data display.

Component	Baboon	Lake	House	Airplane	Peppers
Red	8.7668	9.4917	8.6969	8.1482	9.0995
Green	9.2308	7.7503	8.3429	7.8428	7.6256
Blue	8.3814	7.5119	8.3781	7.9535	7.6500
Average	8.7930	8.2513	8.4726	7.9815	8.1250

5.4. Histogram analysis

Histogram analysis is utilized to unveil the distribution characteristics of pixel values in digital images. When the pixel value distribution is more uniform, it indicates that the encrypted image is irregular and complex, which effectively reduces the risk of information leakage. As shown in Fig. 11, our research solution successfully obfuscated the image data, demonstrating its broad application prospects in areas such as data protection and privacy security.

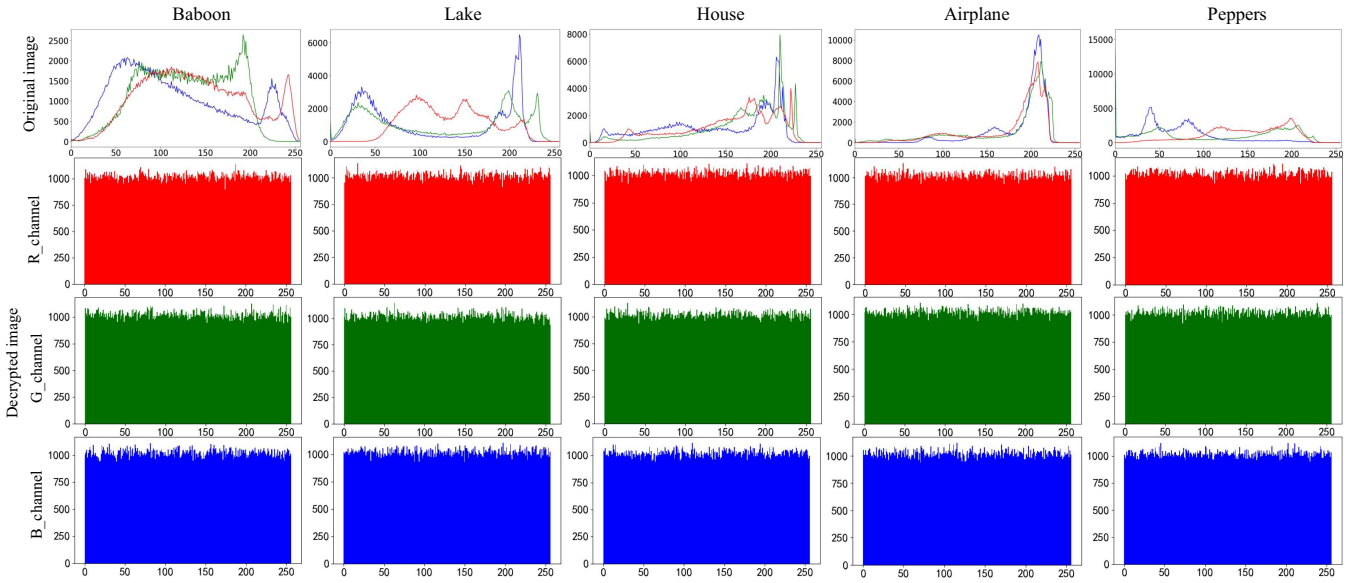


Fig. 11. Histogram analysis results.

5.5. Key sensitivity analysis

Key sensitivity analysis aims to evaluate the sensitivity of image encryption algorithms to key changes, and to quantify the performance of the algorithms in maintaining robustness and security in a scientific manner.[38] In this evaluation, the number of pixels change rate (NPCR) and the unified average change intensity (UACI) are two key indicators, and the ideal values are 99.6094% and 33.4635%, respectively. These metrics can accurately measure the differences between encrypted images caused by changes in encryption keys. The calculation formulas are shown below:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \tag{13}$$

$$\mathrm{UACI} = \frac{\sum_{i,j} (C_1(i,j) - C_2(i,j))}{255 \times W \times H} \times 100\%, \tag{14}$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j), \\ 1, & C_1(i,j) \neq C_2(i,j), \end{cases} \tag{15}$$

where $C_1(i,j)$ is the pixel information of the encrypted image at (i,j), and $C_2(i,j)$ is the pixel information after the key has been slightly changed.

Table 6. Key sensitivity analysis data.

Test	Channel	Baboon	Ref. [39]	Ref. [40]	Ref. [41]	Ref. [23]
NPCR	red	99.6067	99.5964	99.6085	99.5880	99.5911
	green	99.6014	99.6345	99.6085	99.5880	99.5865
	blue	99.6223	99.6220	99.6073	99.5880	99.6292
	average	99.6101	99.6176	99.6081	99.5880	99.6023
UACI	red	33.4228	33.3934	33.4434	33.4273	29.5137
	green	33.4892	33.4142	33.4728	33.4635	28.0464
	blue	33.4710	33.3956	33.4580	33.7951	30.8671
	average	33.4610	33.4011	33.4580	33.5620	29.4757

We take the image "Baboon" as the research object, first encrypt it, then make a small adjustment to the key k_2 by $k_2 + 10^{-10}$, and encrypt it again. Subsequently, key sensitivity tests were performed on two different encrypted images, and the complete experimental data is shown in Table 6. The results show that our proposed algorithm performs well in handling minor changes in the key and maintains a high level of sensitivity.

5.6. Information entropy analysis

In the field of image encryption, information entropy analysis is widely used to evaluate the performance of encryption algorithms. It helps accurately measure the randomness and irregularity of images. The closer the information entropy value is to the ideal value of 8, the higher the uncertainty of the image and the more complex it is. The calculation formula is as follows:

$$H(x) = -\sum_{i=1}^{L} P(x_i) \log_2 P(x_i), \tag{16}$$

where x_i is the gray value of the image, and $P(x_i)$ is the probability of x_i, the unit of information entropy is a bit.

We conducted information entropy analysis on the encrypted images to assess the effectiveness of the proposed scheme in terms of privacy protection and information security. At the same time, the classic image "Baboon" was chosen as the reference object for comparison, and the data for information entropy analysis is presented in Table 7. The research findings indicate that our approach demonstrates notable advantages in information entropy analysis compared to other algorithms, highlighting its superior security features.

Table 7. Comparative data of information entropy analysis (Unit: bit).

Images	Algorithm	Red	Green	Blue	Average
Baboon	proposed algorithm	7.99930	7.99920	7.99919	7.99923
Lake	proposed algorithm	7.99923	7.99922	7.99931	7.99925
House	proposed algorithm	7.99928	7.99930	7.99935	7.99931
Airplane	proposed algorithm	7.99928	7.99938	7.99924	7.99930
Peppers	proposed algorithm	7.99928	7.99929	7.99940	7.99932
Baboon	Ref. [42]	7.9913	7.9916	7.9917	7.99153
Baboon	Ref. [43]	7.9969	7.9964	7.9972	7.99683
Baboon	Ref. [44]	7.9965	7.9963	7.9967	7.99650

5.7. Analysis of anti-noise attack

The significance of noise attack resistance analysis lies in enhancing the security and robustness of encryption systems, thereby ensuring that privacy is effectively protected and can adapt to changes in real-world situations. After being tested and verified with various levels of noise interference, the proposed solution is fully illustrated in Fig. 12. The research results show that our algorithm can restore most of the data information in the original image and enhance the overall security level.

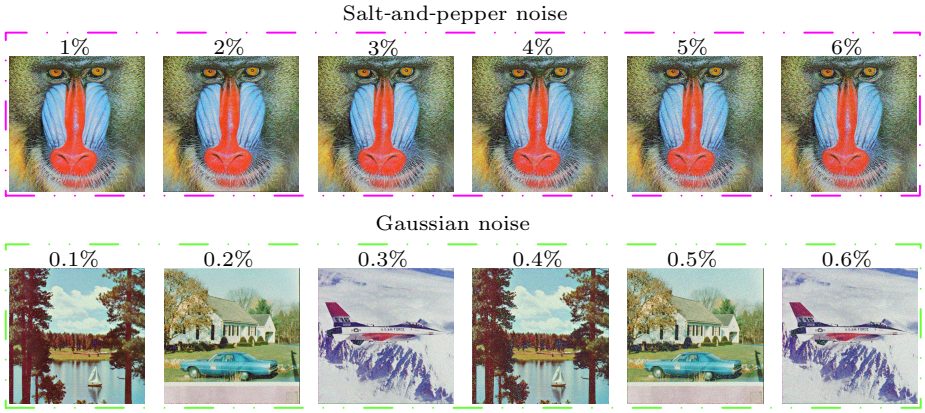


Fig. 12. Anti-noise attack effect.

5.8. Analysis of anti-cropping attack

Images may become corrupted due to transmission errors, storage issues, or human manipulation. Analysis of resistance to cropping attacks can help in designing fault-tolerant encryption schemes to ensure that decryption and information recovery can be performed even if part of the image is lost or damaged. We apply a cropping attack at random positions on the encrypted image and then decrypt it, as shown in Fig. 13. The results demonstrate that our algorithm can successfully restore the information of the original image and maintain data integrity and privacy even when subjected to various levels of cropping attacks.

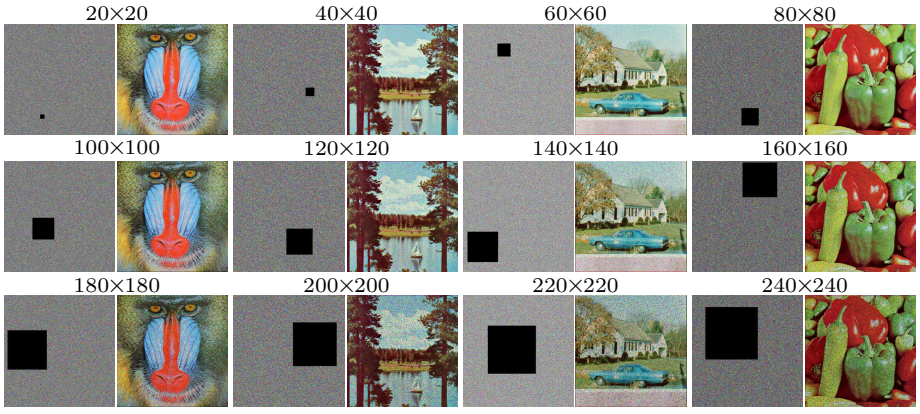


Fig. 13. Anti-cropping attack effect.

6. Discussion and conclusion

This study proposes an innovative color image encryption algorithm to address the image security challenges posed by the rapid development of information technology. The algorithm's core involves utilizing a high-quality pseudo-random number generator based on the Mersenne Twister algorithm to

enhance the complexity of the key space. Additionally, the algorithm integrates autonomous non-Hamiltonian chaotic systems and tent-logistic-cosine chaotic mapping to manage the DNA encoding and decoding process, enabling image scrambling and multi-dimensional confusion. Furthermore, the algorithm's unpredictability is effectively heightened through the enhanced Joseph block scrambling technology. Experimental results demonstrate that this comprehensive encryption strategy not only ensures image quality but also significantly increases the difficulty of decryption. Looking ahead, research in the field of image encryption will focus more on integration with other cutting-edge technologies, such as quantum computing, artificial intelligence, and big data analysis, to adapt to ever-changing application scenarios. This cross-domain collaborative innovation can not only enhance the security of image encryption algorithms but also play a crucial role in a broader range of applications.

Data availability statement

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Acknowledgements

Project supported by the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (Grant No. SKLACSS–202208), the Natural Science Foundation of Chongqing (Grant No. CSTB2023NSCQ-LZX0139), and the National Natural Science Foundation of China (Grant No. 61772295).

References

[1] Wang X, Liu C and Jiang D 2022 *Chaos Soliton. Fract.* **164** 112625
[2] Huang X, Dong Y and Ye G 2023 *Frontiers of Computer Science* **17** 173804
[3] Su Y, Wang X and Lin S 2022 *Chin. Phys. B* **31** 110503
[4] Zhou Y, Bao L and Chen C L P 2014 *Signal Processing* **97** 172
[5] Lai Q, Wan Z and Zhang H 2022 *IEEE Transactions on Neural Networks and Learning Systems* **34** 7824
[6] Zhou N R, Wu J W and Chen M X 2024 *International Journal of Theoretical Physics* **63** 100
[7] Ye G, Liu M and Yap W S 2023 *Nonlinear Dyn.* **111** 13535
[8] Lai Q and Liu Y 2023 *Expert Systems with Applications* **223** 119923
[9] Zhang Z, Mou J and Banerjee S 2024 *Chin. Phys. B* **33** 020503
[10] Guo Z, Chen S H and Zhou L 2024 *Applied Mathematical Modelling* **131** 49
[11] Lai Q, Yang L and Chen G 2023 *IEEE Transactions on Industrial Electronics* 2023
[12] Gong L H and Luo H X 2023 *Optics & Laser Technology* **167** 109665
[13] Jiang S X, Li Y and Shi J 2024 *Chin. Phys. B* **33** 040306
[14] Zhou N R, Hu L L and Huang Z W 2024 *Expert Systems with Applications* **238** 122052
[15] Zhou N R, Tong L J and Zou W P 2023 *Signal Processing* **211** 109107
[16] Qasim I M and Mohammed E A 2023 *Opt. Commun.* **533** 129262
[17] Hu M, Li J and Di X 2023 *Nonlinear Dyn.* **111** 2815
[18] Zhou Q, Wang X and Jin M 2023 *Optics and Lasers in Engineering* **162** 107415
[19] Xu S, Wang X and Ye X 2022 *Chaos Soliton. Fract.* **157** 111889
[20] Zhou S, Zhao Z and Wang X 2022 *Chaos Soliton. Fract.* **161** 112380
[21] Wu Y, Zhang L and Berretti S 2022 *IEEE Transactions on Industrial Informatics* **19** 2089
[22] Huang Z W and Zhou N R 2022 *Optics & Laser Technology* **149** 107879
[23] Alexan W, Alexan N and Gabr M 2023 *Fractal and Fractional* **7** 287
[24] Machicao J and Ngo Q Q 2021 *Information Sciences* **558** 1
[25] Chan E Y S and Corless R M 2023 *SIAM Review* **65** 261
[26] Wu A, Cang S and Zhang R 2018 *Complexity* 2018
[27] Cang S, Wu A and Wang Z 2017 *Nonlinear Dyn.* **89** 2495
[28] Hua Z, Zhou Y and Huang H 2019 *Information Sciences* **480** 403
[29] Shao S, Li J and Shao P 2023 *IEEE Access* **11** 27477
[30] Wang L, Cao Y and Jahanshahi H 2023 *Optik* **275** 170590
[31] Wang X and Sun H 2020 *Optics & Laser Technology* **122** 105854
[32] Yu S S, Zhou N R and Gong L H 2020 *Optics and Lasers in Engineering* **124** 105816
[33] Lai Q, Hu G and Erkan U 2023 *Applied Mathematics and Computation* **442** 127738
[34] Chai X, Zhi X and Gan Z 2021 *Signal Processing* **183** 108041
[35] Zhang J, Yin B and Deng X 2021 *Multimedia Tools and Applications* **80** 27155
[36] Khalil N, Sarhan A and Alshewimy M A M 2021 *Optics & Laser Technology* **143** 107326
[37] Zhang Y Q, He Y and Li P 2020 *Optics and Lasers in Engineering* **128** 106040
[38] Wang X, Liu C and Jiang D 2022 *Information Sciences* **610** 300
[39] Samiullah M, Aslam W and Nazir H 2020 *IEEE Access* **8** 25650
[40] Zhang Q and Han J 2021 *Multimedia Tools and Applications* **80** 13841
[41] Alexan W, ElBeltagy M and Aboshousha A 2022 *Symmetry* **14** 443
[42] Teng L, Wang X and Yang F 2021 *Nonlinear Dyn.* **105** 1859
[43] Elkandoz M T and Alexan W 2022 *Multimedia Tools and Applications* **81** 25497
[44] Alexan W, Elkandoz M and Mashaly M 2023 *IEEE Access* **11** 11541