frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 09 May 2023
DOI 10.3389/fphy.2023.1191793

Check for updates

OPEN ACCESS

EDITED BY
Teddy Craciunescu,
National Institute for Laser Plasma and Radiation Physics, Romania

REVIEWED BY
Kehui Sun,
Central South University, China
Shaobo He,
Central South University, China

*CORRESPONDENCE
Ling Lu,
✉ lvling@njmu.edu.cn

RECEIVED 22 March 2023
ACCEPTED 25 April 2023
PUBLISHED 09 May 2023

CITATION
Zhang H, Sun W and Lu L (2023), Chaotic encryption algorithm with scrambling diffusion based on the Josephus cycle.
Front. Phys. 11:1191793.
doi: 10.3389/fphy.2023.1191793

Chaotic encryption algorithm with scrambling diffusion based on the Josephus cycle

Huijie Zhang[1], Weizhen Sun[1] and Ling Lu[1,2]*

[1]School of Biological Science and Medical Engineering, Southeast University, Nanjing, China, [2]School of Biomedical Engineering and Informatics, Nanjing Medical University, Nanjing, China

Digital images are characterized by high redundancy and strong interpixel correlation. Breaking the correlation between data and improving sensitivity are crucial to protecting image information. To effectively achieve this goal, a chaotic encryption algorithm based on Josephus cycle scrambling diffusion is proposed in this paper. First, the adaptive key is generated by the Hash function to generate the initial value of the chaotic system, which is highly related to the plaintext image. The generation of the adaptive key can effectively resist plaintext attacks. Second, the pseudorandom sequence generated by the two-difference chaotic mapping is applied as the step sequence and direction sequence of Josephus traversal and optimizes Josephus traversal via variable steps and directions; the ranks of plain-text images are scrambled by the Josephus cycle to break the strong correlation between pixels. Finally, the initial cipher-text is divided into blocks to complete the Josephus cycle scrambling diffusion of image blocks, intrablock pixel bits and bit planes. The double permutations at the pixel level and bit level break the high correlation between pixels. Compared with the previous studies, our algorithm's average entropy of encrypted images is 7.9994, which has slightly improved. The correlation coefficient of the cryptographic image fluctuates up and down by approximately 0. In addition, the algorithm has the advantages of a large key space, high key sensitivity, anti-robust attack, and feasible encryption efficiency.

KEYWORDS

image encryption, chaotic mapping, Josephus cycle, security analysis, attacks

1 Introduction

Due to the epidemic, increasing interpersonal communications have been moved to the internet. As a result, users' demands for privacy protection and information security are gradually becoming urgent. Unlike text data, digital images, as a kind of two-dimensional information commonly used online, possess considerable data volume, high redundancy and strong interpixel correlations. Therefore, traditional encryption methods are not applicable for encrypting images, while the existing encryption algorithms for digital images generally have the disadvantages of complicated encryption processes and long time consumption, which no longer satisfy the demands of image encryption.

Chaos theory was first introduced by mathematician Matthews [1] into the field of cryptography; however, it was not until 1998 that Fridrich [2] proposed an image encryption algorithm based on chaotic mapping, which opened a new era of this particular algorithm's rapid development. American mathematician Claude Shannon [3] suggested the classical structure of image encryption based on a chaotic system to be scrambling-diffusion. In the scrambling phase, the positions of image pixels are varied so that their distribution is as random as possible, destroying the similarity between neighboring pixels in the plain-text image. In the diffusion phase, the pixel values interact with each other and change randomly to hide the plain-text image information [4–6]. The security of the encryption effect of this algorithm based on chaotic systems is mainly determined by the structure of this encryption algorithm and the performance of the adopted chaotic systems [7].

According to the confusion system used for encryption, chaotic encryption algorithms can be classified into two types: continuous chaotic encryption algorithms and discrete chaotic encryption algorithms. Continuous chaotic systems consist of one-dimensional higher-order nonlinear differential equations or multivariate first-order differential equations, while discrete chaotic systems comprise iterative mappings, i.e., difference equations. Low-dimensional continuous chaotic systems were previously applied to cryptography in chaos theory because of their simple structure and easy implementation. For example, Gao et al. [8] proposed an image encryption algorithm based on the typical Lorenz and Chen systems.

Due to its small or discontinuous chaotic range, resulting in an uneven distribution of the output chaotic sequence, C. Pak [9], R.A. Elmanfaloty [10] improved the structures of different one-dimensional chaotic systems to effectively increase the chaotic range of chaotic systems and improve the uniformity of chaotic system distribution and the key space of encryption algorithms. Wang et al. [11] proposed a chaotic image encryption algorithm with a perceptual model based on a high-dimensional Loranz chaotic system and a perceptual model of a neural network. Cheng et al. [12], based on a five-dimensional super multiwing chaotic system, designed a chunkwise scrambling algorithm with mixed R, G, and B components to enhance the dependency among the components and improve the scrambling efficiency. Discrete chaotic systems include one-dimensional chaotic mappings and high-dimensional chaotic mappings. One-dimensional chaotic mappings such as logistic mappings, segmented linear chaotic mappings, and Tent are used for image encryption because of their simple structure and fast calculation, such as those of the digital image encryption algorithm based on logistic mapping proposed by Wang et al. [13]. However, their one-dimensional discrete chaotic mapping interval is narrow, multiple period windows will lead to a small cipher space, and the attacker can analyze and attack the chaotic mapping used, which is proven to be insecure [14]. To overcome the shortcomings of one-dimensional chaotic mappings, researchers have proposed many different methods to construct chaotic mappings. Hua et al. [15] proposed a two-dimensional logic-based tuned sinusoidal mapping and used it for image encryption. Due to truncation and rounding errors, the chaotic trajectory can be trapped in a cycle when the device is operated with finite accuracy [16]. [17] proposed extending the time for chaotic mappings to enter a cycle with extended accuracy, which is also limited in its effectiveness since the accuracy cannot be scaled up infinitely. Another approach is to combine multiple mappings together by cascading or switching [12]. Both cascading and switching ignore the interactions between multiple mappings, and their combination's effect depends on the superiority of the strategy. Chai et al. [38] proposed an image encryption scheme based on multiobjective optimization and block compressed sensing. However, those methods based on chaotic systems only scramble the plaint image pixel position, which does not change the entropy and histogram values of the plaintext. This means that the capacity to defend against statistical attacks is poor.

Additionally, some nonchaotic encryption schemes have been used for image encryption at the bit level. The Arnold transform, geometry transform, and E curve transform are classical image scrambling algorithms that are nonchaotic. Hua et al. [28] proposed a two-dimensional plane scrambling algorithm based on Josephus travel. Yu and Yang [35] proposed a symmetric algorithm applied in remote sensing images, which improved encryption security. A dynamic bit-flipping diffusion encryption algorithm is proposed in the literature. Zhu et al. [36] proposed a three-dimensional bit-level image encryption algorithm using Rubik's cube method.

Inspired by the above literature, we combine image bit-level and bit-level encryption and propose an image encryption method with high security and sensitivity by combining a new two-dimensional differential chaotic map and an improved Joseph cycle. In this paper, we propose an image encryption method with high security and sensitivity by combining a new

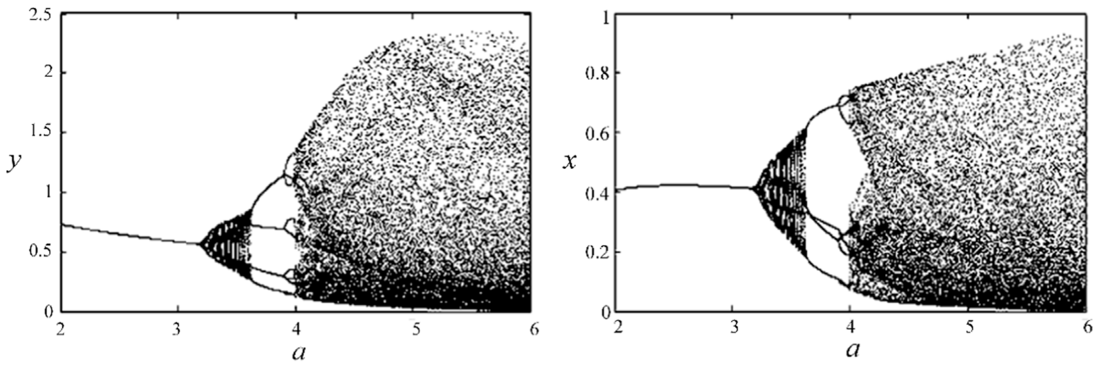


FIGURE 1
Bifurcation diagram for the range $2 \leq a \leq 6$ with respect to *x, y*.

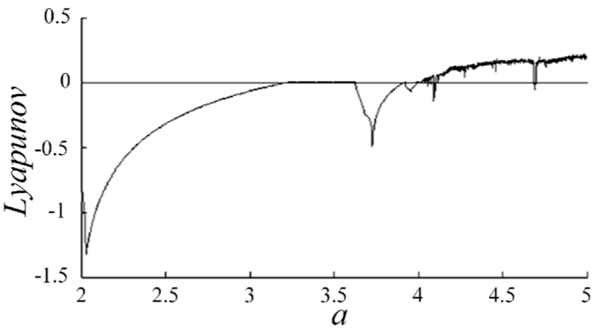


FIGURE 2
Lyapunov exponent plots for $2 \le a \le 5$

two-dimensional differential chaos mapping and an improved Josephus cycle. The image chunking strategy is utilized to enhance the algorithm scrambling efficiency; the improved Josephus cycle enables dynamic variable-step and variable-direction Josephus scrambling diffusion. The scrambling-diffusion of encrypted images is carried out in two dimensions: pixel bits within a block and pixel bit planes within a block, which can effectively reduce the correlation between adjacent data, and the scrambling effect of encrypted images is more random and effective [18]. Also used the adaptive key, which came from the sum and average of the plain-text image, while the method in this paper adopted the hash value of the plain-text image as the adaptive key, which is more sensitive to plain-text changes.

In this paper, the security of the algorithm is verified and compared with related algorithms in terms of correlation and information entropy. The experimental results show that the algorithm in this paper encrypts images with uniform pixel distribution and low interpixel correlation and can effectively resist common attacks with high security.

2 Basic theory

2.1 Chaotic systems

2.1.1 Two-dimensional differential chaotic map

A chaotic system is a nonlinear dynamic system. It has randomness, sensitivity to initial conditions, nonperiodicity and long-term unpredictability. It is suitable for image encryption with a large amount of data and high correlation. Two-dimensional chaotic mapping contains fewer periodic windows in branching graphs, a larger range of chaotic parameters, and faster operation compared to one-dimensional chaotic mapping, and these properties are consistent with cryptographic characteristics, so two-dimensional chaotic mapping is often used in key generators. Combined with the Nicholson-Bailey model [40] in the study of biological populations, the two-dimensional difference equation to be studied in this paper is proposed as follows, which is a variation of Nicholson-Bailey model [41].

$$\begin{cases} y_{n+1} = y_n \exp\left(r\left(1 - y_n\right) - a x_n\right) \\ x_{n+1} = y_n\left(1 - \exp\left(-a x_n\right)\right) \end{cases} \tag{1}$$

The r is chosen as 3, the initial point is arbitrarily set between [0, 1], and Eq. 1 is iterated 1,000 times. Figure 1 shows the bifurcation diagram of parameter a about x and y in the interval [2, 6]. From the figure, we can see that it is a curve at [2, 3.22], so the equation converges at this stage. When a = 3.23, the Hopf branch appears, and periodic motion occurs at [3.23, 3.62]. At [3.63, 3.90], the image contains a 4-terminal curve, which means a motion of 4-cycle. When the equation is greater than 3.91, as a increases, there is no regularity at the beginning, and the equation gradually enters chaos.

2.1.2 Lyapunov exponent

The Lyapunov exponent is an important index to verify the randomness and chaotic characteristics of chaotic sequences. If the Lyapunov exponent of the chaotic system is positive, the chaotic system has chaotic characteristics. The larger the positive value is, the better the chaotic characteristics of the chaotic system are.

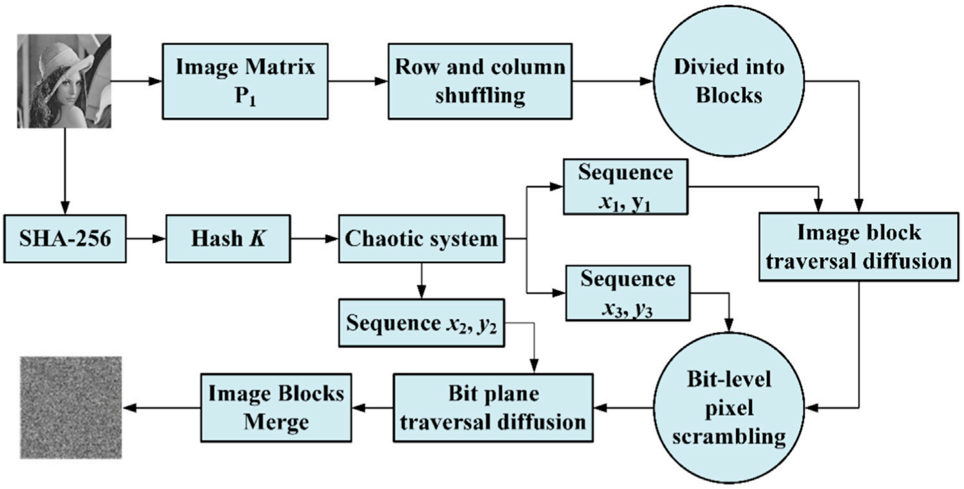


FIGURE 3
General frame of the encryption scheme.

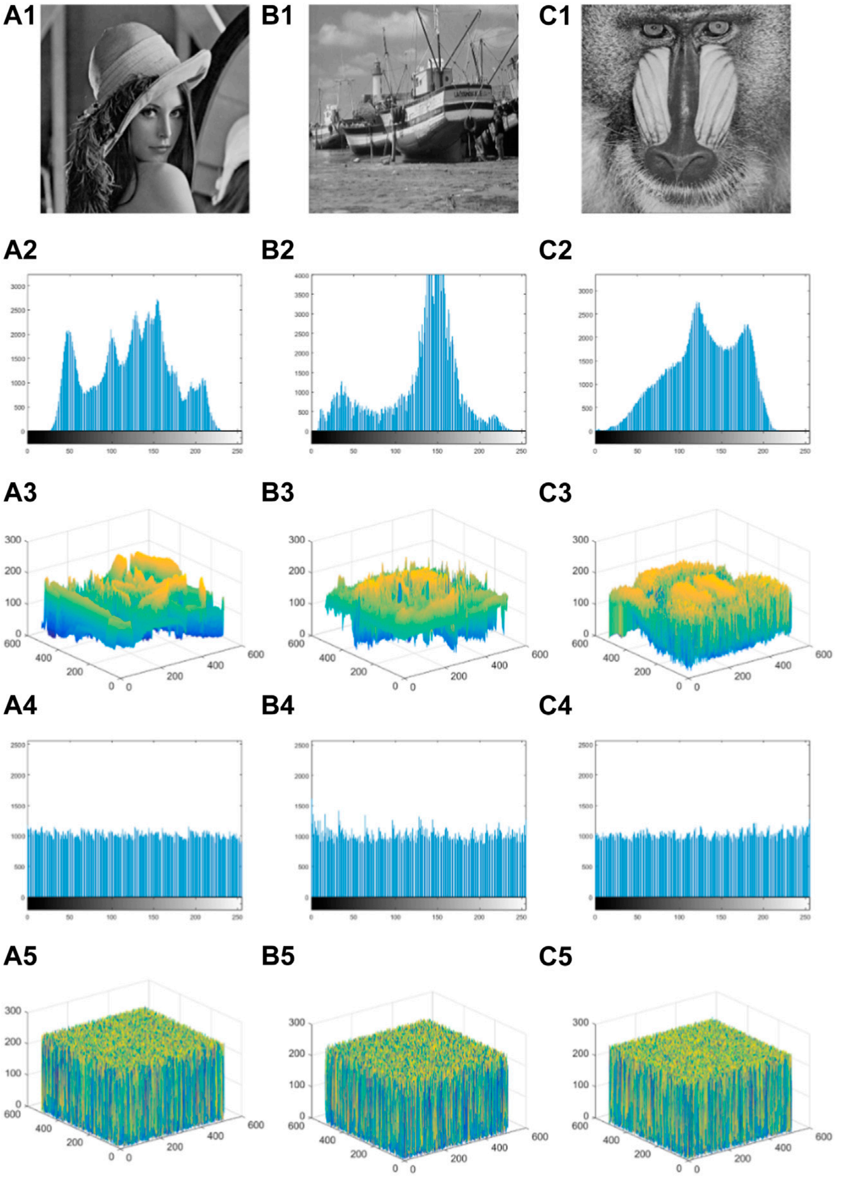


FIGURE 4
Plain-text histogram and cryptographic histogram for different images.

It can be seen from Figure 2, when $a > 4.04$, the Lyapunov exponent is greater than zero, which indicates that the equation enters a chaotic phenomenon. Figure 2 verifies that the Lyapunov exponent diagram of this 2D difference equation agrees with the bifurcation diagram, and the equation shows rich dynamic behavior as the parameter a changes in the interval [2, 6].

2.1.3 Stability analysis of chaotic systems

The immovable points of the nonlinear iterative equations are used as a powerful tool to describe the evolution of the system dynamics. System (1) contains immobile points that satisfy the $F = (x^*, y^*)$ equation as:

$$\left.\begin{aligned} y^* &= y^* \exp\left(r\left(1-y\right)-ax^*\right) \\ x^* &= y^*\left(1-\exp\left(-ax^*\right)\right) \end{aligned}\right\} \tag{2}$$

The solution is:

$$\begin{cases} x_1^* = \dfrac{(r-\ln Q)(Q-1)}{Qr} \\ y_1^* = 1-\dfrac{\ln Q}{r} \end{cases} \tag{3}$$

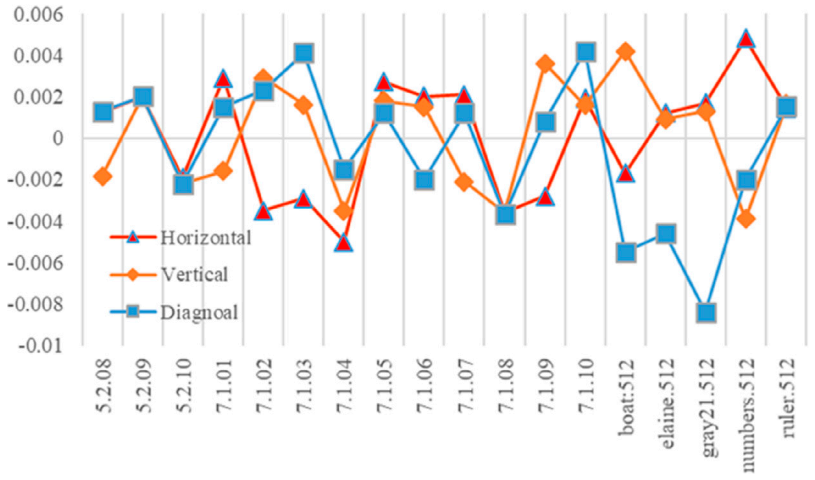
Among them:

$$Q = e^{ax^*} \tag{4}$$

The positive equilibrium point of Eq. 1 is expressed as $E^* = (x^*, y^*)$, and based on Eq. 3, the positive equilibrium point cannot be solved analytically.

To discuss the stability of the equilibrium point, model (1) is written in the following equations:

TABLE 1 Correlations of ciphertext images.



$$\begin{cases} x(n+1) = F_1(x_n, y_n) \\ y(n+1) = F_2(x_n, y_n) \end{cases} \tag{5}$$

Adding a small permutation Δx and Δy at the n pair of equilibrium points, the equation evolves at the $n + 1$ pair as follows:

$$\begin{cases} x(n+1) + \Delta x_{n+1} = F_1(x_n, y_n) + \Delta x_n \\ y(n+1) + \Delta y_{n+1} = F_2(x_n, y_n) + \Delta y_n \end{cases} \tag{6}$$

To obtain a linear stability analysis, the Taylor expansion of the above equation is given as:

$$\begin{pmatrix} \Delta x_{n+1} \\ \Delta y_{n+1} \end{pmatrix} = \begin{pmatrix} \frac{\partial F_1}{\partial x} & \frac{\partial F_1}{\partial y} \\ \frac{\partial F_2}{\partial x} & \frac{\partial F_2}{\partial y} \end{pmatrix}_{x^*, y^*} \begin{pmatrix} \Delta x_n \\ \Delta y_n \end{pmatrix} \tag{7}$$

For the equilibrium point $E_0 = (0, 0)$:

$$\begin{pmatrix} \frac{\partial F_1}{\partial x} & \frac{\partial F_1}{\partial y} \\ \frac{\partial F_2}{\partial x} & \frac{\partial F_2}{\partial y} \end{pmatrix}_{0,0} = \begin{pmatrix} e^r & 0 \\ 0 & 0 \end{pmatrix} \tag{8}$$

where the characteristic roots are $\lambda_1 = e^r$ and $\lambda_2 = 0$, with the parameter $r > 0$, which leads to $|\lambda_1| > 1$, indicating that the equilibrium point $E_0 = (0, 0)$ is unstable.

For positive equilibrium point $E^* = (N^*, P^*)$:

$$\left. \begin{aligned} \frac{\partial F_1}{\partial N}\Big|_{E^*} &= 1 - r - \ln Q \\ \frac{\partial F_1}{\partial P}\Big|_{E^*} &= \frac{-a(r + \ln Q)Q}{r} \\ \frac{\partial F_2}{\partial N}\Big|_{E^*} &= 1 - Q \\ \frac{\partial F_2}{\partial N}\Big|_{E^*} &= \frac{a(r + \ln Q)Q}{r} \end{aligned} \right\} \tag{9}$$

Given the matrix:

$$A = \begin{pmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{pmatrix} \tag{10}$$

where the characteristic equation of $G_{11} = \frac{\partial F_1}{\partial N}|_{E^*}, G_{12} = \frac{\partial F_1}{\partial P}|_{E^*}, G_{21} = \frac{\partial F_1}{\partial N}|_{E^*}, G_{22} = \frac{\partial F_1}{\partial N}|_{E^*}$ is:

$$\begin{vmatrix} G_{11} - \lambda & G_{12} \\ G_{21} & G_{22} - \lambda \end{vmatrix} = 0 \tag{11}$$

Additionally, revised as:

$$Q(\lambda) \equiv \lambda^2 - B\lambda + C = 0 \tag{12}$$

where $B = G_{11} + G_{12}, C = G_{11}G_{22} - G_{21}G_{12}$,

$Q(\lambda)$ is an upper-concave para-curve, while the equation's root as the positive equilibrium point becomes asymptotically stable when the following conditions are satisfied.

Solving the condition for asymptotic stability of the positive equilibrium point as:

$$-1 - C < B < 1 + C, C < 1 \tag{13}$$

2.2 Josephus cycle

Josephus cycle [37] is a classical problem of mathematical application: it is known that individuals (denoted by the numbers 1,2,3,4, n, respectively) are sitting around a round table. Starting with the person numbered 1, the person who has counted to m comes out of the column; the sequence started from 1 again and repeated until all the people come out of the column. Based on the order of the columns, a sequence is obtained: Josephus sequence. Available at $J = f(S, l)$, this is S for the total number of elements, l for the step size, and J for the Josephus sequence.

To increase the diversity of Josephus, this paper introduces the pseudorandom sequence generated by a chaotic system as the dynamic step of the Josephus cycle based on the original rule; using the parity of the pseudorandom sequence as the dynamic direction, the Josephus function is further extended to $J = f(S, l, r, D)$.

TABLE 2 NPCR and UACI values of cipher-text images (%).

Teat image	NPCR			UACI		
	Reference [24]	Reference [25]	Perposed	Reference [24]	Reference [25]	Perposed
5.2.08	99.960	99.6070	99.7085	33.692	33.4734	33.4695
5.2.09	99.876	99.6106	99.6989	33.548	33.4572	33.4610
5.2.10	99.654	99.6096	99.7012	33.454	33.4575	33.4580
7.1.01	99.957	99.6095	99.6945	33.648	33.4726	33.4506
7.1.02	99.918	99.6117	99.7102	33.465	33.4563	33.4409
7.1.03	99.849	99.6123	99.6968	33.273	33.4535	33.4606
7.1.04	99.991	99.6114	99.6978	33.202	33.4475	33.4572
7.1.05	99.942	99.6099	99.6982	33.830	33.4559	33.4608
7.1.06	99.670	99.6064	99.6979	33.627	33.4515	33.5106
7.1.07	99.983	99.6068	99.6986	33.609	33.4638	33.4600
7.1.08	99.818	99.6097	99.6995	33.375	33.4536	33.4610
7.1.09	99.874	99.6112	99.6989	33.530	33.4729	33.4679
7.1.10	99.697	99.6096	99.6979	33.438	33.4605	33.4665
boat.512	99.715	99.6084	99.7002	33.374	33.4434	33.4492
elaine.512	99.746	99.6095	99.7010	33.379	33.4746	33.4700
Gray21.512	99.643	99.6074	99.6998	33.507	33.4588	33.4672
Numbers.512	99.653	99.6102	99.6899	33.388	33.4477	33.4576
Ruler.512	99.637	99.6092	99.6996	33.415	33.4637	33.4566
Mean	99.910	99.6095	99.6700	33.486	33.459	33.4605
STD	0.1312	0.00171	0.00445	0.1551	0.0094	0.0142
Pass/all	All	All	All	14/18	All	All

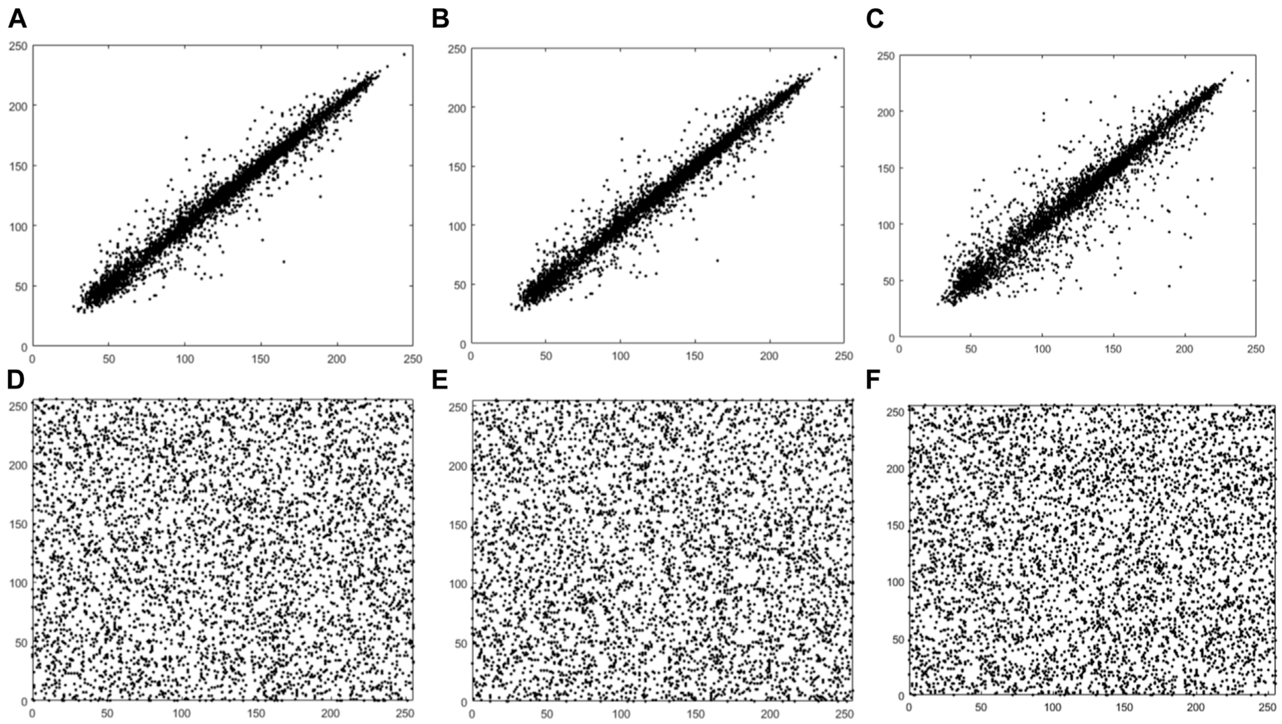


FIGURE 5
Correlations of adjacent pixels in the horizontal **(A,D)**, vertical **(B,E)**, and diagonal **(C,F)** directions before and after Lena encryption.

2.3 Combined scrambling diffusion of bits and bit planes

The pixels of a grayscale map are generally composed of 8-digit binary, where the amount of binary information varies greatly from position to position. For example, a "1" in the eighth bit represents 128 (2^7), while the lowest bit "1" represents 1 (2^0). The information contained in each bit is proportional as follows:

$$p(i) = \frac{2^{i-1}}{\sum_{i=1}^{8} 2^{i-1}} \quad i = 1, 2, 3, 4, 5, 6, 7, 8 \tag{14}$$

From Eq. 14, it can be seen that as the bits increase, the proportion of information contained in the bits increases. Therefore, the bits of different bit positions are scrambled. Then, the scrambled bit planes are diffused by the bit positions. Finally, 8 bit planes are obtained after bit position diffusion, and these bit planes are reorganized into one pixel plane to obtain the image after bit position diffusion.

3 Image encryption algorithm

3.1 Encryption algorithm

The encryption scheme proposed in this paper mainly consists of five parts: image rank permutation, image block division, image block diffusion, bit-level scrambling diffusion and cipher-text image block combination. The proposed encryption scheme can be represented by a block diagram, as shown in Figure 3. The whole scheme can be divided into pixel diffusion and bit diffusion. First, an adaptive key is generated through a plain-text image for the chaotic system's initial values, and three pairs of pseudorandom sequences are generated. Second, to diffuse the image via row and column shuffling and divide into blocks, one pair of pseudo random sequences is used for the modified Josephus traversal to finish the block scrambling diffusion. Third, another two pairs of pseudorandom sequences finish shuffling at the bit level for the pixel and bit plane. In combination with a modified Josephus traversal, the image is dislocated and diffused using a production-issue chaotic sequence.

3.2 Key generation

Adaptive keys are an effective method to improve the resistance of encrypted images to known plaintext attacks. As [19] described, independent key streams increase the possibility of selecting plaintext attacks. In contrast, generating adaptive keys from plain-text images can achieve a 1-time 1-classification effect. Of course, the plain-text image has to be highly dispersed into the keystream. For this reason, this paper uses the hash value of the plain-text image to construct the initial value of the chaotic system. Any small change in the image will result in a huge change in the hash value, and the initial value of the chaotic system will also change. Of course, the use of different system parameters and initial values determines the superiority of the cryptographic complexity of this chaotic sequence [20]. Showed that choosing appropriate parameters in the chaotic interval could make the autocorrelation property of the resulting chaotic sequence close to white noise. Therefore, in this paper, the adaptive key is processed and controlled to fall within the chaotic interval.

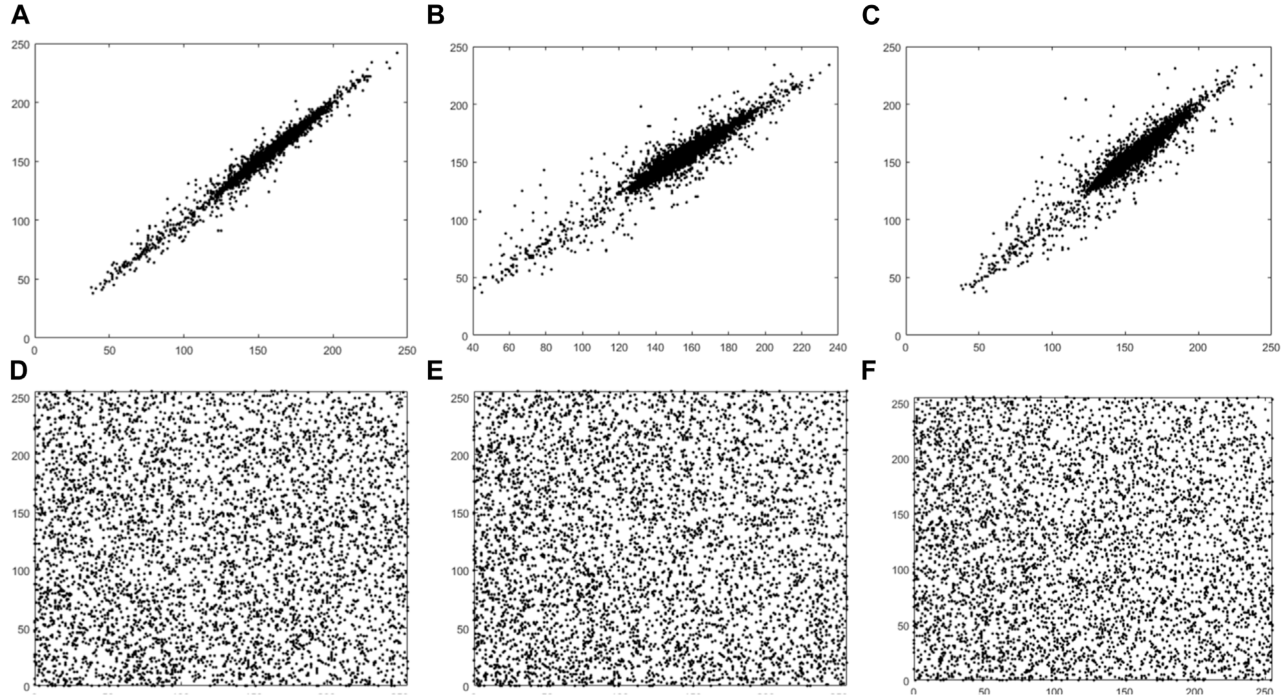


FIGURE 6
Correlations of adjacent pixels in the horizontal **(A,D)**, vertical **(B,E)**, and diagonal **(C,F)** directions before and after boat encryption.

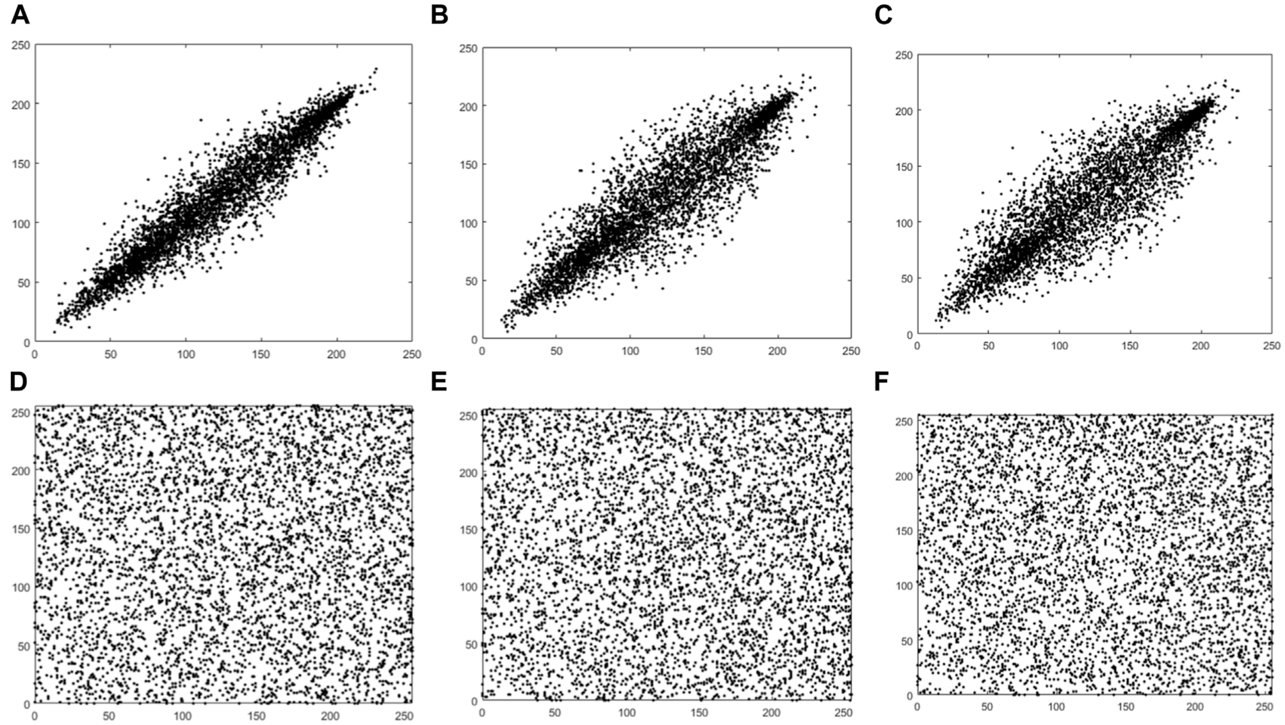


FIGURE 7
Correlations of adjacent pixels in the horizontal **(A,D)**, vertical **(B,E)**, and diagonal **(C,F)** directions before and after Feifei encryption.

TABLE 3 Information entropy of plaintext images and ciphertext images.

Textimage	Size	Plaintext images	Ciphertext images		
			Reference [22]	Reference [25]	Proposed
5.2.08	512 × 512	7.5237	7.9991	7.9993	7.9995
5.2.10		5.7056	7.9991	7.9993	7.9990
7.1.01		6.0274	7.9990	7.9991	7.9992
7.1.02		4.0045	7.9991	7.9992	7.9996
7.1.04		6.1074	7.9992	7.9993	7.9993
7.1.05		6.5632	7.9992	7.9992	7.9992
7.1.06		6.6953	7.9992	7.9993	7.9996
7.1.07		5.9916	7.9991	7.9993	7.9995
7.1.08		5.5034	7.9990	7.9993	7.9996
7.1.09		6.1898	7.9991	7.9992	7.9995
7.1.10		5.9088	7.9990	7.9993	7.9995
Boat.512		7.1914	7.9992	7.9994	7.9996
Elaine.512		7.5060	7.9992	7.9993	7.9994
Gray21.512		4.3923	7.9993	7.9994	7.9996
Numbers.512		7.7292	7.9994	7.9991	7.9995
Ruler.512		0.5000	7.9987	7.9992	7.9996
Mean		—	7.9991	7.9993	7.9994

Read the plain-text image $p(m,n)$, where m and n are the length and width of the image, respectively. Calculate the SHA-256 cipher-text value H of the image. Convert the cipher-text value to the initial value of the 2-D differential chaos system x_0, y_0, the parameter a, and the number of discarded terms c.

$$\left.\begin{array}{r} x_0 = hex2dec(H(1{:}\ 16)) \times 10^{-20} \\ y_0 = hex2dec(H(17{:}\ 32)) \times 10^{-20} \\ a = hex2dec(H(1{:}\ 16)) \times 10^{-20} + 4.04 \\ c = hex2dec(H(1{:}\ 16)) \times 10^{-20} + 1000 \end{array}\right\} \tag{15}$$

The initial values generated by Eq. 15 are brought into Eq. 1 to iterate the random sequence of $c + 21 \times m \times n$ to obtain two chaotic sequences x, y. To enhance the randomness of the chaotic sequences, the first c values are discarded, and the interval sampling method proposed by [21] is adopted for sequence sampling with a sampling interval of 12 to expand the x, y sequence into four pseudorandom sequences of x_1, x_2, y_1, y_2, and [21] revealed that x_1, x_2 are independent and y_1, y_2 are independent. The even positions of x_1, x_2 are extracted to form a new random sequence x_3, and the even positions of y_1, y_2 are extracted to form a new random sequence y_3.

3.3 Image scrambling encryption

First read in the image P through the row/column permutation into P_1. Second, we divide the scrambled image P_1 of size $M \times N$ into $m \times n$ non-overlapping blocks $P_1 = \{P_i \mid i = 1, 2, \cdots, k\}$, where $k = \frac{M \times N}{m \times n}$ is the number of blocks, and each block has $m \times n$ pixels, i.e., $P_{1_i} = \left\{P_{1_{i,j}} \mid j = 1, 2, \cdots, m \times n\right\}$.

The image block scrambling process can be divided into the following 3 steps.

Step 1 Interblock scrambling. In this paper, we give a cyclic traversal method with variable step length and direction. The method is combined with a chaotic system, in which the chaotic sequence x_1, y_1 is used as the direction and step sequence, and when the Josephus traversal cycle is performed on the image blocks, the cycle direction is determined first, and then the traversal is performed according to the step length.

Step 2Block built-in scrambling protects pixel bit scrambling and bit plane scrambling.

Step 2.1. Pixel bit position scrambling uses the chaotic sequence x_3, y_3 as a variable direction, variable step sequence to traverse the pixel's bits in a cycle.

Step 2.2. Bit plane scrambling, image blocks are all composed of 8 bit planes, using chaotic sequences x_2, y_2, with directional sequences, step sequences, and cyclic traversal of the bit values within the bit planes.

Step 3 Splice the cipher-text image blocks to obtain the cipher-text image.

3.4 Image recovery

The decryption process is the reverse of the encryption process, and the main steps are as follows:

Input: Ciphertext image, SHA-256 cipher-text value H.

Out: Plaintext image.

TABLE 4 Comparison of local Shannon entropy.

Test image	Size	Reference [23]	Reference [22]	Reference [25]	Proposed
5.2.08	512 × 512	7.902,793	7.902,831	7.902,038	7.902,658
5.2.09		7.902,972	7.903,028	7.902,722	7.902,726
5.2.10		7.902,464	7.903,511	7.902,478	7.902,646
7.1.01		7.903,339	7.903,252	7.902,012	7.902,714
7.1.02		7.902,649	7.903,313	7.902,484	7.902,660
7.1.03		7.902,493	7.903,103	7.902,833	7.902,698
7.1.04		7.903,261	7.902,625	7.902,047	7.902,685
7.1.05		7.902,714	7.902,435	7.902,568	7.902,669
7.1.06		7.902,563	7.902,675	7.902,022	7.902,712
7.1.07		7.903,185	7.902,813	7.902,398	7.902,683
7.1.08		7.902,805	7.902,668	7.902,137	7.902,697
7.1.09		7.903,070	7.902,632	7.902,142	7.902,657
7.1.10		7.902,929	7.902,486	7.902,171	7.902,706
Boat.512		7.902,697	7.902,885	7.902,046	7.902,438
Elaine.512		7.902,755	7.902,805	7.902,632	7.902,642
Gray21.512		7.903,661	7.903,106	7.902,718	7.902,495
Numbers.512		7.902,545	7.903,263	7.902,067	7.902,368
Ruler.512		7.902,896	7.902,848	7.902,004	7.902,549
Mean		7.902,877	7.902,904	7.902,307	7.902,633
STD		0.000324	0.000303	0.0002931	0.000102
PASS/ALL		ALL	ALL	ALL	ALL

Step 1The ciphertext image I is converted into a 2-D moment of size M × N array.
Step 2Generated the key sequences $\{x_1, x_2, x_3, y_1, y_2, y_3\}$ as the method in Section 3.1
Step 3Block built-in scrambling protects pixel bit scrambling and bit plane scrambling.

Step 3.1. Joseph traversal with sequence $\{x_3, y_3\}$, which uses as a variable step size and variable direction is used to complete the scrambling of the image bit plane.

Step 3.2. Joseph traversal with sequence $\{x_2, y_2\}$, which uses as a variable step size and variable direction is used to complete the scrambling of the pixel bit plane.

Step 4. Joseph traversal with sequence $\{x_1, y_1\}$, which is used as variable astep size and variable direction is used to scramble the image pixel blocks, and a new image matrix is obtained, which is the plaintext image.

4 Security analysis

The effectiveness of the proposed encryption algorithm is verified from histogram, correlation, differential attack, key space, information entropy, clipping and noise attacks using data from the USC-SIPI 'Miscellaneous' database.

4.1 Histogram analysis

The more uniform the histogram is, the looser the relationship between the pixel intensity value and the number of pixels, the more random the image is, and the more difficult it is for an attacker to recover the original image through a histogram analysis attack.

Figure 4 shows the histograms and pixel distributions of the three images of Lena, Boat, and Feifei in the testing database, where the first row is the plain-text image, the second is the histogram of the plain-text image, the third is the pixel distribution of the plain-text image, and the fourth and fifth are the histograms and pixel distributions of the cipher-text obtained from encryption of the corresponding plain-text. Both the histogram and the pixel distribution of the plain-text image present significant differences, i.e., uneven distribution. The difference between the histogram and the pixel distribution of the obtained cipher text is relatively insignificant, and the comparison shows that the pixel distribution of the cipher text is more uniform than that of the plain text. This is because the Josephus cyclic scrambling diffusion of bit positions and bits at the bit level changed the bit values composed of the plain-text image's bit planes so that the pixel value distribution of

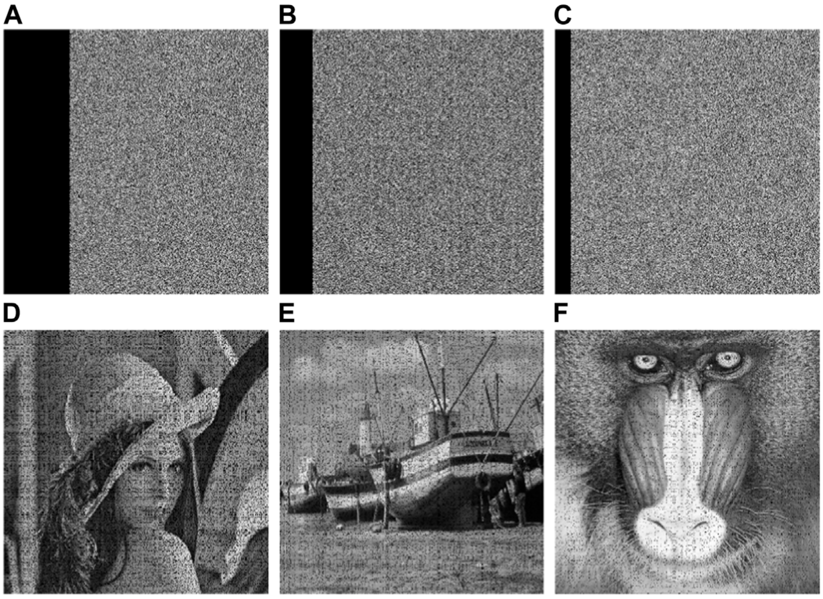


FIGURE 8
Encryption results after clipping attack **(A)** Encryption of Lena's 1/4 clipping, **(B)** Encryption of Boat's 1/8 clipping, **(C)** Encryption of Feifei's 1/16 clipping.

the reconstructed pixel planes tends to be uniform. Therefore, the algorithm in this paper was proven to have a good ability to resist statistical analysis.

To test the uniformity of the histogram, a chi-square test was used, which is computed by the following equation.

$$\chi^2 = \frac{1}{255}\sum_{i=0}^{255}\left(hist_i - \frac{1}{256}\sum_{i=0}^{255}hist_i\right)^2 \tag{16}$$

where $hist_i$ is the pixel value frequency (0–255). The lower the chi-square value, the better the consistency. To the significant level of α is fixed, so $P\left\{\chi^2 \geq \chi^2_\alpha(n-1)\right\} = \alpha$, then $\chi^2 \prec \chi^2_\alpha(n-1)$ satisfies the desired condition.

When $\alpha = 0.01, 0.05, 0.1; \chi^2_{0.01}(255) = 310.45739$, $\chi^2_{0.05}(255) = 293.24783, \chi^2_{0.1}(255) = 284.33591$, the plaintext image and the encrypted image χ2 points. When the significance level was $\alpha = 0.05$, all ciphertext images [39] passed the test.

4.2 Correlation analysis

The neighboring pixel values of plain-text images are very close to each other and have a strong correlation. Breaking the correlation between pixels is important to resist statistical analysis attacks. Correlation analysis is used to test the strength of the correlation between image pixels. The correlation between ordinary image pixels is usually extremely high, and the correlation coefficient of an image usually tends to be close to 1. If the correlation between adjacent or most pixels can be broken instead, then if the correlation and the correlation coefficient are reduced, it is more resistant to statistical analysis attacks. The correlation coefficient is calculated using the following equation:

$$\left.\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N}x_i \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2 \\ \operatorname{cov}(x,y) &= \frac{1}{N}\sum_{i=1}^{N}[x - E(x)][y - E(y)] \\ \gamma_{xy} &= \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}} \end{aligned}\right\} \tag{17}$$

Randomly selected 5,000 pairs of pixel points, the statistical results of the correlation between the horizontal, vertical and diagonal directions of the original image and the cipher-text image in the test database are shown in Table 1, from which it can be seen that the number of prior relationships in the three directions of the cipher-text image fluctuates up and down around x = 0, indicating that the correlation between the pixels of the adjacent images of the plain-text is very low, revealing that the proposed encryption method is reliable and secure.

Figures 5–7 visualizes the correlation results before and after encryption. The plain-text images are strongly correlated in three directions. After the proposed encryption algorithm, the correlation of neighboring pixels is substantially weakened. It is this structure and characteristics of the plain-text image that make it resistant to statistical attacks.

4.3 Differential attack analysis

The differential attack is a deciphering method to attack the encryption algorithm by analyzing the degree of cipher-text change

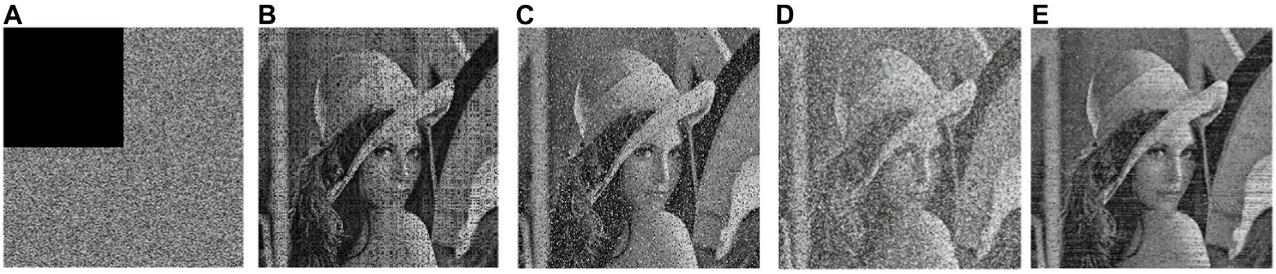


FIGURE 9
Decryption results after noise attack: **(A)** decryption of "Lena" with noise intensity of 0.25, **(B)** decryption of "Ship" with noise intensity of 0.10, and **(C)** Decryption of "Baboon" with noise intensity of 0.05.

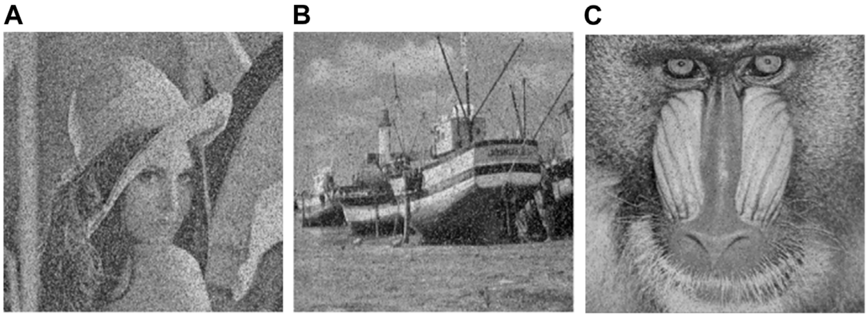


FIGURE 10
Comparison of decryption results after clipping attack: **(A)** 1/4° clipping of the encrypted "Lena", **(B)** Decryption by the algorithm proposed in this paper, **(C)** Decryption by the algorithm proposed in [25], **(D)** Decryption by the algorithm in [26], **(E)** Decryption by the algorithm in [27].

due to the subtle difference in plain-text. To analyze the resistance of the proposed encryption algorithm to the differential attack, this paper observes the degree of difference between the cipher-text images after two encryptions by changing the pixel value at any point in the plain-text image. If the degree of difference is large, the proposed algorithm is able to resist the differential attack effectively. The pixel change rate (NPCR) and the pixel average change intensity (UACI) are usually measured using the expressions of NPCR and UACI as follows:

$$\left.\begin{aligned} NPCR &= \frac{1}{M \times N}\sum_{i}^{M}\sum_{j}^{N} D(i,j) \times 100\% \\ D(i,j) &= \begin{cases} 1, I_1(i,j) \neq I_2(i,j) \\ 0, I_1(i,j) = I_2(i,j) \end{cases} \\ UACI &= \frac{\sum_{i}^{M}\sum_{j}^{N}\left|I_1(i,j) - I_2(i,j)\right| D(i,j)}{255 \times M \times N} \times 100\% \end{aligned}\right\} \tag{18}$$

where I_1, I_2 is the two plain-text images to be encrypted with only one pixel difference. For an arbitrary NPCR and UACI, expect 100% and 33.4635%.

The NPCR and UACI pairwise scores of the test images were analyzed. The mean value of NPCR and the standard deviation of UACI of the proposed method in this paper are 99.6700 and 0.0045, respectively. The mean value and standard deviation of UACI are 33.4605 and 0.0142, respectively. The comparison shows that the NPCR, UACI of the proposed encryption algorithm is very close to the theoretical value, and its labelling difference is the smallest among the compared methods. This indicates that the proposed method has better sensitivity. In addition, the significance level of our images is set to 0.05, and then the critical values of NPCR and UACI corresponding to different sizes are calculated. Compared with the approaches of [22, 23], the proposed method exhibits the same pass rate, but the mean value of the encrypted images in this paper is closer to the theoretical value of 33.4605%, but the standard deviation 0.0142 of the encryption algorithm in this paper fell between the two comparative works, indicating that the encryption algorithm in this paper can better resist the differential attack, but the stability of the ability to resist the split attack is between the two comparative methods.

4.4 Key space analysis

To effectively resist brute force attacks, the key should have a sufficiently large key space in addition to a strong sensitivity. The size of the key space is determined by the number of keys; the larger the number of keys, the larger the key space of the encryption algorithm, and the stronger its ability to resist brute-force attacks.

The security key factors of the encryption algorithm in this paper are five, which are two parameters of the system, two initial

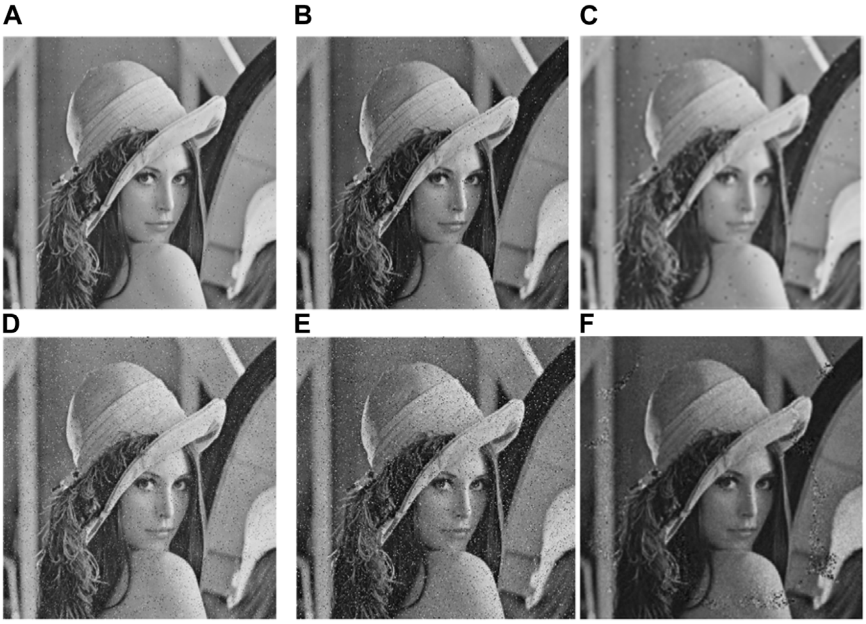


FIGURE 11
Comparison of decryption results after noise attack: **(A)** decrypted after a 1% noise attack by the proposed algorithm, **(B)** decrypted after a 1% noise attack by the algorithm in [25], **(C)** decrypted after a 1% noise attack by the algorithm in [42], **(D)** decrypted after a 5% noise attack by the proposed algorithm, **(E)** decrypted after a 5% noise attack by the algorithm in [25], and **(F)** decrypted after a 5% noise attack by the algorithm in [42].

values of the chaotic system and the order of chaos taking m. The sensitivity of both chaotic parameters and chaotic initial values is 10^{-15}, then the key capacity of this encryption algorithm is $10^{15} \times 10^{15} \times 10^{15} \times 10^{15} = 10^{60}$, which is greater than 2^{100}, therefore, it can be considered that this image encryption process has a strong resistance to exhaustive attacks.

4.5 Information entropy analysis

Information entropy is a test of uncertainty and is calculated as in Eq. 19.

$$H(m) = -\sum_{k=0}^{2^N-1} p(m_i)\log_2 p(m_i) \tag{19}$$

$p(m)$ denotes the probability of occurrence of information m. For grayscale images, information m has 256 states, the minimum value is 0 and the maximum value is 255. When the information entropy is eight, it indicates that the information is completely random, that is, the larger the cipher-text information entropy is, the more secure it is. Table 3 provides the image information entropy using the proposed encryption algorithm, and by comparing with the methods of [24, 25], the cipher-text image information entropy 7.9994 proposed in this paper is closer to the ideal value of eight. Its randomness is better than that of the compared methods.

The information entropy can better reflect the overall randomness of the image, while the local information entropy can better reflect the microscopic randomness of the image. Local information entropy is an improved information algorithm that selects nonoverlapping regions in an image and calculates the evaluation information entropy of these regions, which is calculated as in Eq. 20:

$$\overline{H_{(k,T_B)}(S)} = \frac{1}{k}\sum_{i=1}^{k} H(S_i) \tag{20}$$

k denotes the number of regions, T_B denotes the number of pixels in the selected regions, and $\overline{H_{(k,T_B)}(S)}$ denotes the local information entropy. Let $k = 30$, and the confidence interval of local information entropy is [7.900,573,7.904,227] when the significance level is 0.05. The local information entropy of the test image is shown in Table 4, and the encryption algorithm proposed in this paper and those in [22, 23, 25] are all within the confidence interval. However, the mean value of 7.902,633 of the proposed algorithm in this paper is better than that of [25]. The standard deviation in this paper is 0.000102, which is smaller than those of the three compared methods. The local randomness of the image encrypted by the proposed algorithm is also better than the three compared methods in terms of stability performance.

4.6 Clipping attack and noise attack

A clipping attack is an attack method that intercepts and destroys or removes part of the data of a cipher-text image during transmission. Usually, the clipped part is a region in the image with strong interpixel correlation, and the lost information is difficult to recover. Therefore, breaking the interpixel correlation is a measure of the clipping resistance performance of the image encryption algorithm. If the strong interpixel correlation of the

TABLE 5 SSIM between the cover image and stego image.

Test image	Proposed
Boat.512	0.9785
Elaine.512	0.9797
Gray21.512	0.9794
Numbers.512	0.9786
Ruler.512	0.9812

image leads to decryption, it may fail when the cipher-text image after the loss of information does not provide enough valid information. In this paper, by combining two-dimensional difference mapping with the Josephus cycle, the image is dislocated using a chunking strategy with uniform pixel distribution, and when the cipher-text image is clipped, the clipped part is not a complete distinction in the original image but is scattered in various regional points so that the clipped image still retains enough information to enable it to recover the corresponding plain-text image. The following test images of Lena et al. shown in Figure 8 are clipped by 1/16, 1/8, and 1/4 (the pixels at the clipped position are all 0, and the clipped sample is shown in Figure 10), and the decrypted image of the clipped cipher-text image is shown in the second row of Figure 8. The algorithm in this paper has certain recovery ability when subjected to clipping attacks, and the encryption algorithm in this paper can resist certain clipping attacks.

Figure 9 shows the effect of Lean reduced by different decryption algorithms at the same degree of clipping, and it can be seen that the proposed encryption algorithm is different from [25]. There is almost no difference between the proposed encryption algorithm and [25], but it is significantly better than the algorithms in [26, 27].

Image noise is the unnecessary or redundant interference information that exists in image data. In the process of image acquisition or transmission, due to the influence of image sensor material, working environment, transmission channel, etc., the image may receive noise contamination, which will have a certain impact on the decryption of the terminal image. Therefore, the ability to resist certain noise attacks is an indicator of the performance of image encryption algorithms. In this paper, we use pepper noise to simulate noise contamination in transmission and add different intensities of pepper noise to the cipher image to test the anti-noise ability of the algorithm in this paper.

Figure 10 shows the results obtained by restoring the test cipher-text image after adding pretzel noise with noise densities of 0.25, 0.10, and 0.05. From this, it can be seen that the greater the noise intensity, the deeper the impact on the image and the poorer the quality of the decrypted image, but the algorithm in this paper can still distinguish the main information of the original image from the overall effect, which indicates that the algorithm in this paper can tolerate a certain degree of noise and has a certain anti-interference ability.

Figure 11 shows the individual results of using the encryption algorithms proposed in this paper and [25, 26] for cipher-text image restoration under noise attacks. The first column shows the proposed algorithm in this paper, the second column shows the results of [25], and the third column is the results of [42]. The first row is a 1% noise attack, and the second row is a 5% noise attack. By comparing the decrypted images under the same noise interference, it can be seen that the decryption algorithm in this paper outperforms the other two encryption algorithms.

4.7 Lossless and perceived encryption analysis

The proposed method is lossless encryption. We use the value of the peak signal measure noise ratio (PSNR) to calculate the difference between the plain and cipher images. When the value of PSNR between the plain image and the cipher image is minimal, the encryption performance is better. In contrast, the PSNR value between plain and decrypted images must be infinity to prove that the encryption is lossless. PSNR can be calculated by Eq. (21)

$$PSNR = 10 \times \log_{10} \left(255^2 / \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left| I(i,j) - I'(i,j) \right|^2}{255}\right. \tag{21}$$

where I is the plain image, I′ is the image cipher or image decrypt depending on the calculation of the encryption or decryption process and the pixel coordinates are i, j. The result measured by PSNR is presented in Table 3.

We also use structural similarity (SSIM) to measure the quality of the encryption proposed for the cipher image. In addition, SSIM is

TABLE 6 The running time of different algorithms.

Metric	Input images	Encryption(s)	Decryption(s)
Reference [29]	Lena	0.40585	—
Reference [30]		1.7351	3.4689
Reference [31]		0.3440	—
Reference [32]		10.8232	10.6952
Reference [33]		14.8401	14.9266
Reference [34]		0.329,276	0.217,033
Proposed		0.34498	0.2017

also used to measure the quality of the decrypted image from the distortion that occurs, which has a value between 0 and 1. A large value means that SSIM is better. The SSIM can be calculated by Eq. 22

$$SSIM = \frac{(2\mu_c\mu_s + C_1)(2\sigma_{CS} + C_2)}{(\mu_c{}^2 + \mu_s{}^2 + C_1)(\sigma_c{}^2 + \sigma_s{}^2 + C_2)} \tag{22}$$

where C_1 and C_2 are two constants, c represents the cover image and s means the stego image. Moreover, represent the average and the standard deviation, respectively. The result measured by SSIM is presented in Table 5.

4.8 Encryption time and encryption complexity analysis

In this section, we chose an image named Lena, which is a representation to compare the encryption time with the other encryption schemes. Table 6 shows different algorithms' encryption times. Encryption is not the best, but it is the best in decryption since decryption does not need to recive the pseudorandom sequence.

The proposed algorithm's computational complexity mainly depends on the calculation of the integer data. The proposed encryption method's computational complexity is $\Theta(8(M+N) + \frac{N}{2} + \frac{M \times N}{2}) \leq \Theta(M \times N)$, where M and N represent the length and width of the image, respectively. Therefore, the encryption scheme is proposed with a high encryption speed.

5 Conclusion

To address the problems of weak security of current image encryption algorithms, this paper proposes a Josephus cycle image encryption algorithm based on a two-difference chaotic system. The chunking strategy is used to improve the efficiency of the scrambling diffusion, and the adaptive key generation algorithm is used to break the correlation between neighboring pixels through the scrambling diffusion of bit bits and bit planes by applying the rank transformation method and the Josephus cycle with variable step length and direction. Experimental evidence is conducted using USC-SIPI 'Miscellaneous' images, which are commonly used in encryption. The results show that the algorithm in this paper can effectively resist common attacks such as information analysis, brute force, noise, and clipping and can be applied to the encryption and transmission of image information. However, the algorithm in this paper also has certain shortcomings, and the bit-level encryption in this paper increases the complexity of the algorithm. To guarantee the security of the algorithm, it is complicated to choose the scrambling method, which affects the encryption speed, and if the algorithm is applied to fast mobile devices, the efficiency of the algorithm needs to be further improved.

Data availability statement

Publicly available datasets were analyzed in this study. This data can be found here: http://sipi.usc.edu/database/.

Author contributions

HZ provided the idea of algorithm. HZ and WS carried out the simulations, arranged the architecture, and drafted the manuscript. LL supervised the work and revised the manuscript. Both authors read and approved the final manuscript.All authors contributed to the article and approved the submitted version.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Matthews R. On the derivation of a "Chaotic" encryption algorithm. *Cryptologic* (1989) 13(1):29–42. doi:10.1080/0161-118991863745

2. Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. *Int J Bifurcation chaos* (1998) 8(6):1259–84. doi:10.1142/s021812749800098x

3. Shannon CE. Communication theory of secrecy systems. *Bell Syst Tech J* (1949) 28(4):656–715. doi:10.1002/j.1538-7305.1949.tb00928.x

4. Li CQ, Lin D, Lu JH. Cryptanalyzing an Image-Scrambling encryption algorithm of pixel bits. *IEEE Multimedia* (2017) 24(3):64–71. doi:10.1109/mmul.2017.3051512

5. Hua ZY, Yi S, Zhou Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process.* (2018) 144:134–44. doi:10.1016/j.sigpro.2017.10.004

6. Hu J, Han F. A pixel-based scrambling scheme for digital medical images protection. *J Netw Comput Appl* (2009) 32(4):788–94. doi:10.1016/j.jnca.2009.02.009

7. Zheng J, Luo Z, Zhang Q. An efficient image encryption algorithm based on multi chaotic system and random DAN coding. *Multimedia Tools Appl* (2020) 79:29901–21. doi:10.1007/s11042-020-09454-9

8. Gao T, Chen Z. Image encryption based on a new total shuffling algorithm. *Chaos, solitons and fractals* (2008) 38(1):213–20. doi:10.1016/j.chaos.2006.11.009

9. Pak C, An K, Jang P, Kim J. A novel bit-level color image encryption using improved 1D chaotic map. *Multimedia Tools Appl* (2018) 78(9):12027–42. doi:10.1007/s11042-018-6739-1

10. Elmanfaloty RA, Abou-Bakr E. An image encryption scheme using a 1D chaotic double section skew tent map. *Complexity* (2020) 2020:7647421–18. doi:10.1155/2020/7647421

11. Wang XY, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dyn* (2010) 62(3):615–21. doi:10.1007/s11071-010-9749-8

12. Cheng G, Wang C, Chen H. A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture. *Int J Bifurcation Chaos* (2019) 29(09):1950115. doi:10.1142/s0218127419501153

13. Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos. *Signal Process* (2012) 92:1101–8. doi:10.1016/j.sigpro.2011.10.023

14. Arroyo D, Diaz J, Rodriguez FB. Cryptanalysis of a one round chaos-based substitution permutation network. *Signal Process* (2013) 93:1358–64. doi:10.1016/j.sigpro.2012.11.019

15. Hua Z, Zhou Y. Image encryption using 2D logistic-adjusted-sine map. *Inf Sci* (2016) 339:237–53. doi:10.1016/j.ins.2016.01.017

16. Chen C, Sun K, He S. An improved image encryption algorithm with finite computing precision. *Signal Process* (2020) 168:107340. doi:10.1016/j.sigpro.2019.107340

17. Flores-Vergara A, Inzunza-Gonzalez E, Garcia-Guerrero E, López-Bonilla O, Rodríguez-Orozco E, Hernández-Ontiveros J, et al. Implementing a chaotic cryptosystem by performing parallel computing on embedded systems with multiprocessors. *Entropy* (2019) 21:268. doi:10.3390/e21030268

18. Niu Y, Zhang X. An image encryption algorithm based on filling curve and adjacent pixel bit scrambling. *J Electro Inf Tech* (2022) 44(3):1137–46.

19. Rehman AU, Liao X, Kulsoom A, Ullah S. A modified (Dual) fusion technique for image encryption using SHA-256 hash and multiple chaotic maps. *Multimedia Tools Appl* (2016) 75(18):11241–66. doi:10.1007/s11042-015-2851-7

20. Lin T, Xu Y. Experimental study of different parameters on chaotic stream ciphers forinformation encryption. *Acta Scientiarum Naturalium Universitatis Sunyatseni* (2004) 43(S2):101–4. doi:10.3321/j.issn:0529-6579.2004.z2.026

21. Huang L, Han G, Xiang J, Min L. Optimization of chaotic measurement matrix in compressive sensing. In: Proceedings of the 2nd International Conference on Digital Signal Processing; Tokyo (2018).

22. Alawida M, Samsudin A, Alshoura WH. An image encryption scheme based on hybridizing digital chaos and finite state machine. *Signal Process* (2019) 164:249–66. doi:10.1016/j.sigpro.2019.06.013

23. Himeur Y, Boukabou A. A robust and secure key-frames based video watermarking system using chaotic encryption. *Multimedia Tools Appl* (2018) 77(7): 8603–27. doi:10.1007/s11042-017-4754-2

24. Zhou Y, Bao L, Chen L. Image encryption using a new parametric switching chaotic system. *Signal Process* (2013) 93(11):3039–52. doi:10.1016/j.sigpro.2013.04.021

25. Xian Y, Wang X. Fractal sorting matrix and its application on chaotic image encryption. *Inf Sci* (2021) 547:1154–69. doi:10.1016/j.ins.2020.09.055

26. Cun Q, Tong X, Zhu W, Zhang M. Selective image encryption method based on dynamic DNA coding and new chaotic map. *Optik* (2021) 243:167286. doi:10.1016/j.ijleo.2021.167286

27. Chai X, Chen Y, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations,. *Opt Lasers Eng* (2017) 88:197–213. doi:10.1016/j.optlaseng.2016.08.009

28. Hua Z, Xu B, Jin F, Huang F. Image encryption using Josephus problem and filtering diffusion. *IEEE Access* (2021) 7:8660–74. doi:10.1109/access.2018.2890116

29. Girdhar A, Kapur H, Kumar V. A novel grayscale image encryption approach based on chaotic maps and image blocks. *Appl Phys* (2021) 127:39. doi:10.1007/s00340-021-07585-x

30. Yan X, Wang X, Xian Y. Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation. *Multimedia Tools Appl* (2021) 80:10949–83. doi:10.1007/s11042-020-10218-8

31. Ping P, Xu F, Mao Y, Wang Z. Designing permutation–substitution image encryption networks with Henon map. *Neurocomputing* (2018) 283:53–63. doi:10.1016/j.neucom.2017.12.048

32. Chai X, Gan Z, Yuan K, Chen Y, Liu X. A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural Comput Appl* (2019) 31:219–37. doi:10.1007/s00521-017-2993-9

33. Hu T, Liu Y, Gong L, Ouyang C. An image encryption scheme combining chaos with cycle operation for DNA sequences. *Nonlinear Dyn* (2016) 87:51–66. doi:10.1007/s11071-016-3024-6

34. Sakshi P, Thanikkaiselvan V. Image encryption using a spectrally efficient halton logistics tent (HaLT) Map and DNA encoding for secured. *Entropy* (2022).

35. Yu Z, Yang Z. Method of remote sensing image detail encryption based on symmetry algorithm. *J Ambient Intelligence Humanized Comput* (2021). doi:10.1007/s12652-020-02818-x

36. Hua Z, Zhou Y. Design of image cipher using block-based scrambling and image filtering. *Inf Sci* (2017) 396:97–113. doi:10.1016/j.ins.2017.02.036

37. Park J, Dogan A, TeıxeıraBlock R. Josephus Problem: When the reality is more cruel than the old story. *Hacettepe J Math Stat* (2021) 50:970–81.

38. Chai X, Fu J, Gan Z, Lu Y, Zhang Y. An image encryption scheme based on multi-objective optimization and block compressed sensing. *Nonlinear Dyn* (2022) 108: 2671–704. doi:10.1007/s11071-022-07328-3

39. Nakano K, Suzuki K. Known-plaintext attack-based analysis of double random phase encoding using multiple known plaintext-ciphertext pairs. *Appl Opt* (2022) 61: 9010–9. doi:10.1364/ao.469244

40. Nicholson A, Bailey V. *The balance of animal populations: Part I, in proceedings of the zoological society of landon*. Oxford, UK: Blackwell Publishing (1935). p. 551–98.

41. Hassan S, Ahluwalia D, Maddali RK, Manglik M. Computational dynamics of the nicholson-bailey models. *Eur Phys J plus* (2018) 133(349):2–22.

42. Zhou C, Wang X, Li H. Image encryption algorithm with matrix semi-tensor product. *Nonlinear Dyn* (2021) 105(1):859–76.