PLOS ONE

RESEARCH ARTICLE

A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling

Xingyuan Wang[1]*, Yining Su[1], Chao Luo[2], Chunpeng Wang[3]

1 School of Information Science and Technology, Dalian Maritime University, Dalian, China, **2** School of Information Science and Engineering, Shandong Normal University, Jinan, China, **3** School of Information, Qilu University of Technology (Shandong Academy of Sciences), Jinan, China

* xywang@dlmu.edu.cn

Citation: Wang X, Su Y, Luo C, Wang C (2020) A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling. PLoS ONE 15(7): e0236015. https://doi.org/10.1371/journal.pone.0236015

Editor: Jun Ma, Lanzhou University of Technology, CHINA

Received: April 22, 2020

Accepted: June 27, 2020

Published: July 15, 2020

Data Availability Statement: All relevant data are within the manuscript.

Funding: This research is supported by the National Natural Science Foundation of China (No: 61672124), the Password Theory Project of the 13th FiveYear Plan National Cryptography Development Fund (No: MMJJ20170203), Liaoning Province Science and Technology Innovation Leading Talents Program Project (No: XLYC1802013), Key R&D Projects of Liaoning Province (No: 2019020105-JH2/103), and Jinan

Abstract

This paper proposes a new chaotic image encryption algorithm. Firstly, an original phased composite chaotic map is used. The comparative study shows that the map cryptographic characteristics are better than the Logistic map, and the map is used as the controller of Fisher-Yates scrambling. Secondly, with the higher complexity of the fractional-order five-dimensional cellular neural network system, it is used as a diffusion controller in the encryption process. And mix the secret key, mapping and plaintext, we can obtain the final ciphertext. Finally, the comparative experiments prove that the proposed algorithm improves the encryption efficiency, has good security performance, and can resist common attack methods.

1 Instruction

With the rapid development of the computer industry, more and more multimedia information needs to ensure its encryption status during transmission to prevent others from gaining privacy and conduct improper behavior. Digital images, because of their large data volume and high data correlation, combined with information image and vividness, have become one of the important means for people to express information. A good encryption algorithm for images is very necessary. Double random phase coding (DRPE) [1] technology provides a theoretical basis for many subsequent optical encryption systems, but it is vulnerable to attack [2]. Therefore many experts have proposed optical image encryption based on Fresnel transform domain [3], gyration transform domain [4], fractional Merlin transform domain [5]. For example, Zhou et al. proposed an image compression encryption algorithm based on compressed sensing and fractional Merlin transform. In order to reduce the problems caused by linear characteristics, chaos is a theoretical system sensitive to initial value conditions, just meets people's expectations of passwords in the encryption process. Especially in recent times, chaotic encryption systems are increasingly used for image encryption [6–10]. For example, Ye et al. used the Logic-tent map for visually meaningful image encryption.

Chaos is a complex nonlinear dynamic system. Chaotic phenomena are a kind of random process in nonlinear deterministic systems. Because chaotic signals have noise-like, initial

City '20 universities' Funding Projects Introducing Innovation Team Program (No: 2019GXRC031) to XW.

Competing interests: The authors have declared that no competing interests exist.

value sensitivity and long-term unpredictability, they are especially suitable for secure communication. technology. Hyperchaotic systems have higher security performance because they can generate more complex dynamic behaviors, have stronger randomness and unpredictability. In recent years, chaos has been used as a research hotspot for people's attention. The color image, by changing the existing order of the image, arranges the pixels according to some operations to form a noise-like image to achieve the encryption effect [11]. So far, some color image encryption algorithms based on chaos theory have been proposed [12–15], while high-dimensional chaotic systems, especially hyperchaotic systems, have large key spaces, complex and unpredictable nonlinear behavior, using hyperchaotic systems to encrypt data will improve the security of the cryptosystem. The research finds that the chaotic characteristics exhibited by CNN make its application in secure communication more and more important. Using the chaotic characteristics of CNN to design the image encryption scheme, the advantages are as follows: Although the dynamic equation of CNN is simple in form, there are chaotic attractors in a large parameter range, and the dynamic behavior is complex; the parameters in CNN dynamic equation are more. The encryption scheme with large key space can be designed; CNN dynamic equation can directly generate a better random matrix, which can design a digital image encryption scheme more conveniently.

Therefore, this paper proposes a color image encryption algorithm based on cellular neural network. The initial key is artificially selected. After the processing of the staged chaotic map, the generated sequence is used as a random number generator to perform Fishery's scrambling, and then the scrambled image is serialized, and the fractional five-dimensional is used. The sequence obtained after the diffusion of the cellular neural network is subjected to secondary diffusion, and finally the ciphertext is obtained. Finally, through simulation experiments, it can be seen that this algorithm has improved security compared with previous algorithms, and is suitable as a way of image encryption.

2 Introduction to chaotic systems

2.1 Fractional 5-dimensional cellular neural network model

The cellular neural network was proposed by Chua and Yang in a combination of cellular automata and Hopfield neural networks. The cellular automatic machine composed of a large number of basic units provides a good model basis for a complex self-organizing structure. The Hopfield neural network constructed by the storage system and the binary neural network can realize the extreme convergence of the system by recursively. They can achieve weight controllable, dual-transmission and local connectivity through improved system networks. Due to its excellent characteristics, cellular neural networks are widely used in prediction, pattern recognition, and control. However, there is not much literature on applying the hyperchaotic characteristics of CNN to image encryption. In many literatures, the chaotic sequences generated by CNN are used for encryption, but due to the defects of its own algorithm, its encryption effect cannot meet the resistance of existing attack methods. Therefore, this paper will use the use of fractional-order 5D neural network to make it better applied to the field of image encryption against existing attacks.

According to its schematic diagram, each neuron cell in CNN can be expressed by Eq (1).

$$\frac{dx_{ij}(t)}{dt} = -\frac{1}{R}x_{ij}(t) + \sum_{C(k,l)\in N_r(i,j)} A(i,j;k,l) + \sum_{C(k,l)\in N_r(i,j)} B(i,j;k,l)u_{kl}(t) + I, \quad (1)$$

where $x_{ij}(t)$ is the state variable of the cell (i,j); I indicates the external output of the network; $u_{kl}(t)$ indicates the corresponding input voltage of the cell (i,j); $y_{ij}(t)$ is the corresponding

output of the cell (*i*,*j*), Its output function $f(x_{ij})$ is a piecewise linear function, whose expression is shown in Eq (2):

$$f(x_{ij}) = \frac{1}{2}(|x_{ij}+1| - |x_{ij}-1|), \tag{2}$$

In the research, we simplified the state equation of CNN for the convenience of research. This paper introduces a simplified version of the CNN model and divides its fractional order into five dimensions, in the form of Eq (3).

$$\frac{d^{q_i}x_i}{d^{q_i}t} = -x_j + a_j p_i + \sum_{\substack{k=1 \\ k\neq j}}^{5} a_{jk}p_k + \sum_{k=1}^{5} s_{jk}x_k + I_j, \tag{3}$$

The CNN parameters of the 5 cells are as follows:

$$a_1 = a_2 = a_3 = a_5 = 0, a_4 = 202, a_{jk} = 0(j,k = 1,2,3,4,5, j \neq k), I_j = 0(j = 1,2,3,4,5)$$

$$S_{jk} = \begin{bmatrix} 1 & 0 & -1 & -1 & -1 \\ 0 & 3 & 1 & 0 & 0 \\ 11 & -12 & 1 & 0 & 0 \\ 92 & 0 & 0 & -94 & -1 \\ 0 & 0 & 15 & 0 & -1 \end{bmatrix}. \tag{4}$$

Then, Eq (3) can be

$$\begin{cases} \frac{d^{q_1}x_1}{dt^{q_1}} = -x_1 + S_{11}x_1 + S_{13}x_3 + S_{14}x_4 \\ \frac{d^{q_2}x_2}{dt^{q_2}} = -x_2 + S_{22}x_2 + S_{23}x_3 \\ \frac{d^{q_3}x_3}{dt^{q_3}} = -x_3 + S_{31}x_1 + S_{32}x_2 + S_{33}x_3 \\ \frac{d^{q_4}x_4}{dt^{q_4}} = -x_4 + S_{41}x_1 + S_{44}x_4 + S_{45}x_5 \\ \frac{d^{q_5}x_5}{dt^{q_5}} = -x_5 + S_{53}x_3 + S_{55}x_5 \end{cases}. \tag{5}$$

Solve Eq (5) using the Runge-Kutta method with a step size of 0.005, set $x_1 = 0.1, x_2 = x_3 = x_4 = x_5 = 0.2$, its Lyapunov exponent diagram is shown in Fig 1. It can be seen that, when $q_1 = q_2 = q_3 = q_4 = q_5 = 0.98$, The Lyapunov index is -0.49121, -0.45898, 0.55644, 0.94533, 2.33257. Therefore, it can be considered that the system is already in a chaotic state at this time, and its chaotic attractor map is shown in Fig 2.

2.2 Staged composite chaotic mapping model

Although one-dimensional chaos can generate pseudo-random sequences, it is often used in image encryption and neural networks [16–18], but due to its low complexity, it is easy to be predicted, which reduces the security of the entire encryption system. We use a phased compound chaotic map composed of two one-dimensional chaotic maps (Logistic map and Tent map) [19]. The specific operations are as follows:

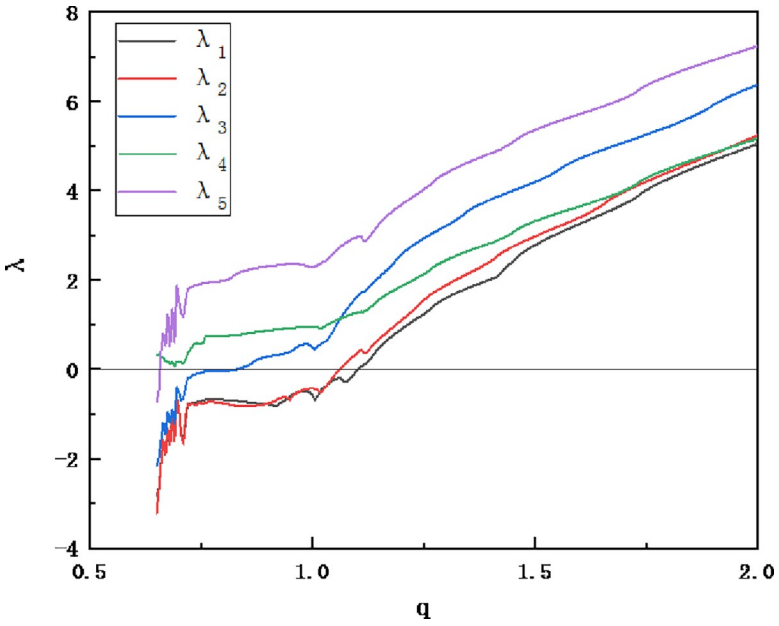


Fig 1. Fractional-order cellular neural network Lyapunov exponential map.

https://doi.org/10.1371/journal.pone.0236015.g001

The Logistic map is divided into two parts and its form is

$$x_{n+1} = \begin{cases} 4\mu x_n(0.5 - x_n), 0 \le x < 0.5 \\ 4\mu x_n(1 - x_n)(x_n - 0.5), 0.5 \le x \le 1 \end{cases}, \quad (6)$$

Divide the Tent map into four parts, the phased compound chaotic map can be obtained by taking the Eq (4)

$$x_{n+1} = \begin{cases} 16\mu x_n(0.5 - \mu x_n), 0 \le x < 0.25 \\ 16\mu(0.5 - x_n)(0.5 - \mu(0.5 - x_n)), 0.25 \le x < 0.5 \\ 16\mu(x_n - 0.5)(0.5 - \mu(x_n - 0.5)), 0.5 \le x < 0.75 \\ 16\mu(1 - x_n)(0.5 - \mu(1 - x_n)), 0.75 \le x \le 1 \end{cases}, \quad (7)$$

where $\mu \in [0,2]$, $x_i \in [0,1]$, its bifurcation diagram is shown in Fig 3, the map has entered a chaotic state at $\mu > 0.33$.

3 Algorithm description

3.1 Scrambling process based on phased composite chaotic map

Fisher-Yates scrambling is generally a random arrangement that produces a finite set. The Fisher-Yates random scrambling algorithm is unbiased, so each permutation is equally possible. The currently used Fisher-Yates random scrambling algorithm is quite effective, and the time required is proportional to the number to be randomly scrambled. The amount of storage space required is required.

Fisher-Yates scrambling is mainly based on a certain rule, starting from the last element of a sequence, and exchanging numbers with a previous position. If the rules for selecting numbers are random, the entire scrambling process is also random. However, the random process does not make the scrambling process reversible, so the use of Fisher-Yates scrambling in this

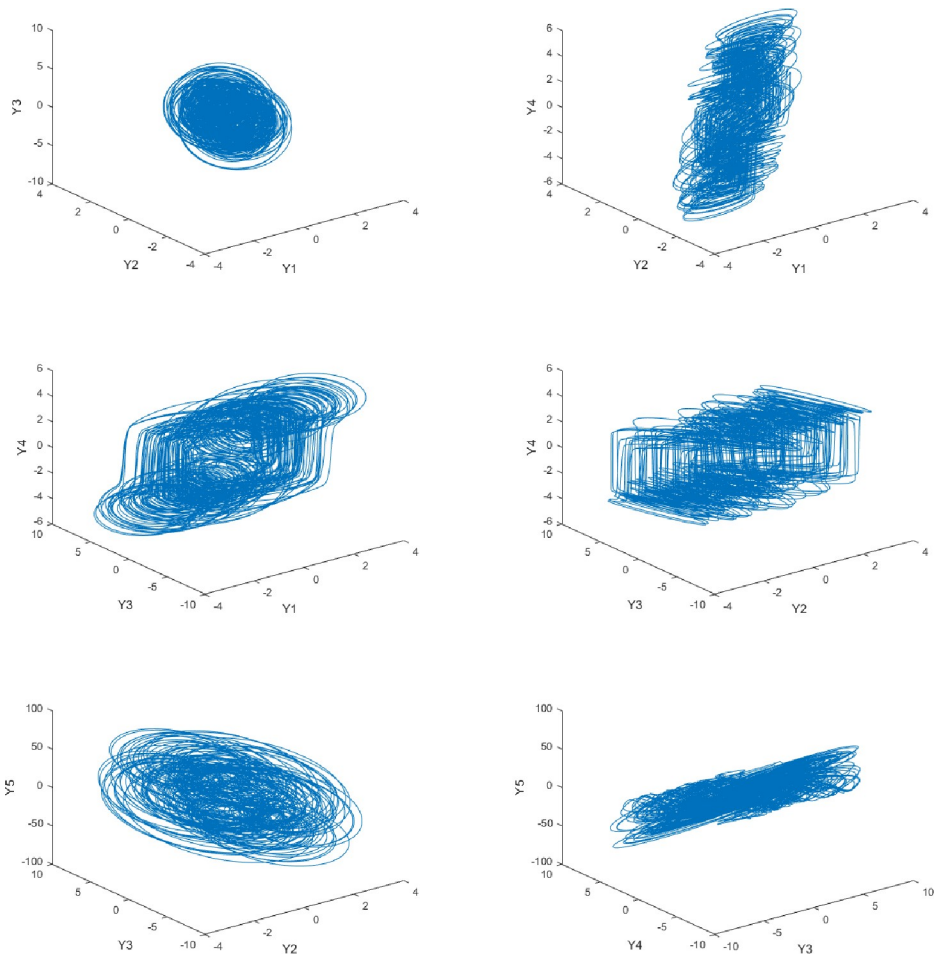


Fig 2. 3-D projection of chaotic attractors for fractional-order cellular neural networks.

https://doi.org/10.1371/journal.pone.0236015.g002

paper is based on the pseudo-randomness of the phased composite chaotic map mentioned above. Because of its good pseudo-randomness, it can undertake the task of random scrambling required, and can complete the restoration of the image with the key.

3.2 Diffusion based on fractional-order 5-dimensional cellular neural networks

In the diffusion phase, this paper uses a fractional-order 5-dimensional cellular neural network as a diffusion method to spread the pixel values of the scrambled image to ensure that the plaintext information can be diffused into each pixel to make it against common attacks. Can have good resistance. In this paper, the diffusion process mainly selects the sequence of the corresponding cellular neural network according to the key, and XORs the ciphertext and the plaintext, and then generates a new ciphertext. The specific process will be described in detail below.

3.3 Encryption steps

We use a grayscale image of size $M \times N$, where M is the width of the image and N is the height of the image. This article uses Matlab to process digital images, so the default is 1 as the beginning of the array instead of 0.

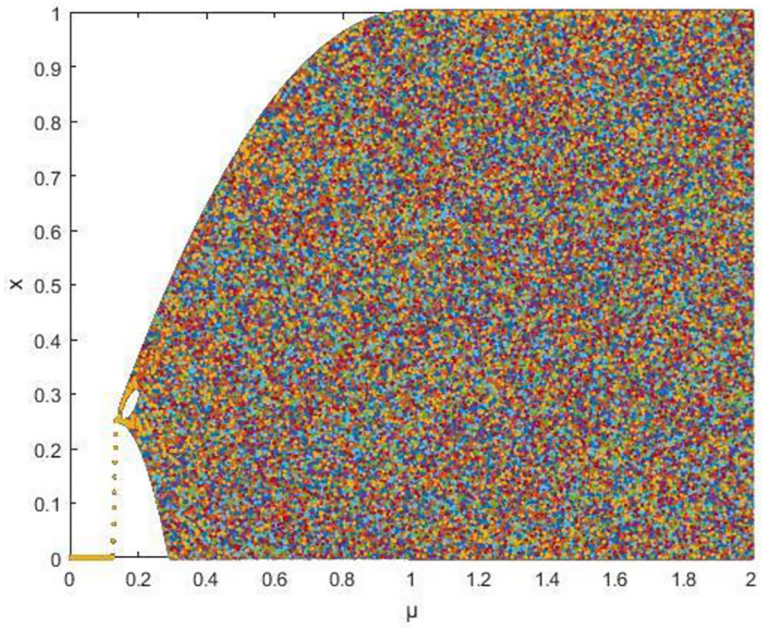


Fig 3. Bifurcation diagram of staged composite chaotic map.

https://doi.org/10.1371/journal.pone.0236015.g003

In the scrambling process, x,μ is input as a key, and then the key is processed according to Eq (7) to obtain a required phased chaotic map sequence L. Then use Fisher-Yates to scramble, use the first scramble, and then scramble to the whole picture. The scrambling process is to first extract the required scrambling rules from the phased composite map, as shown in Eq (8).

$$L' = L(1 + (j-1) \times N : j \times N), \tag{8}$$

where j is the encrypted column, and after the scrambling rule is obtained, the column j is scrambled, and the scrambling method is as shown in Eqs (9)–(12).

$$L_{Final} = floor(L' \times (N - k + 1)) + 1, \tag{9}$$

$$temp = Image_j(L_{Final}(N - k + 1), j), \tag{10}$$

$$Image_j(L_{Final}(N - k + 1), j) = Image_j(N - k + 1, j), \tag{11}$$

$$Image_j(N - k + 1, j) = temp, \tag{12}$$

where Eq (9) is performed by converting L' into integers between [1,N], and Eqs (10)–(12) accomplish the scrambling of the column j, k represents the number of elements that have been scrambled in column j. Repeat this process until each column is scrambled and then finished. After the column is scrambled, the row elements are scrambled with the same rules. At this point, the entire scrambling process is completed.

After the scrambling is completed, a semi-ciphertext $Image_{semi}$ is obtained, and then the semi-ciphertext is diffused. First use the initial key to make it integer, as shown in Eq (13)

$$key = \mathrm{mod}(L(1) \times 10^{14}, 256), \tag{13}$$

Then perform the reconstruction as shown in Eq (14) on the semi-ciphertext $Image_{semi}$,

$$Image'_{semi} = reshape(Image_{semi}, M \times N, 1), \tag{14}$$

after that, the chained conduction diffusion is performed on the reconstructed $Image'_{semi}$, as shown by Eqs (15) and (16).

$$\begin{cases} C_1 = (Image'_{semi}(1) \oplus key) \oplus (\mathrm{mod}(Y(1, \mathrm{mod}(key, 5) + 1) \times 10^5, 256)) \\ C_i = (Image'_{semi}(i) \oplus C_{i-1}) \oplus (\mathrm{mod}(|Y(i, \mathrm{mod}(C_{i-1}, 5) + 1)| \times 10^5, 256))(i \neq 1) \end{cases}, \tag{15}$$

$$C = reshape(C, M, N), \tag{16}$$

where Y is the sequence of the generated fractional-order cellular neural network. There are five groups, and the required parameters are x_1,x_2,x_3,x_4,x_5,q_1,q_2,q_3,q_4,q_5, C is ciphertext. At this point, the encryption process ends, and the process of the encryption process in this paper is shown in Fig 4.

3.4 Image decryption

In the decryption process of this paper, in the case of known keys and ciphertext, the required parameters, such as x,μ and x_1,x_2,x_3,x_4,x_5,q_1,q_2,q_3,q_4,q_5, can be generated to solve the original image.

4 Experimental results and analysis

4.1 Experimental result

This article selects an image of size 256×256 for encryption. Set $x = 0.6$,$\mu = 1.46$,$x_1 = 0.1$,$x_2 = x_3 = x_4 = x_5 = 0.2$, $q_1 = q_2 = q_3 = q_4 = q_5 = 0.98$, Fig 5 shows the results of the encryption and decryption experiments on the images Lena, Bird, Cameraman and the color image Peppers.

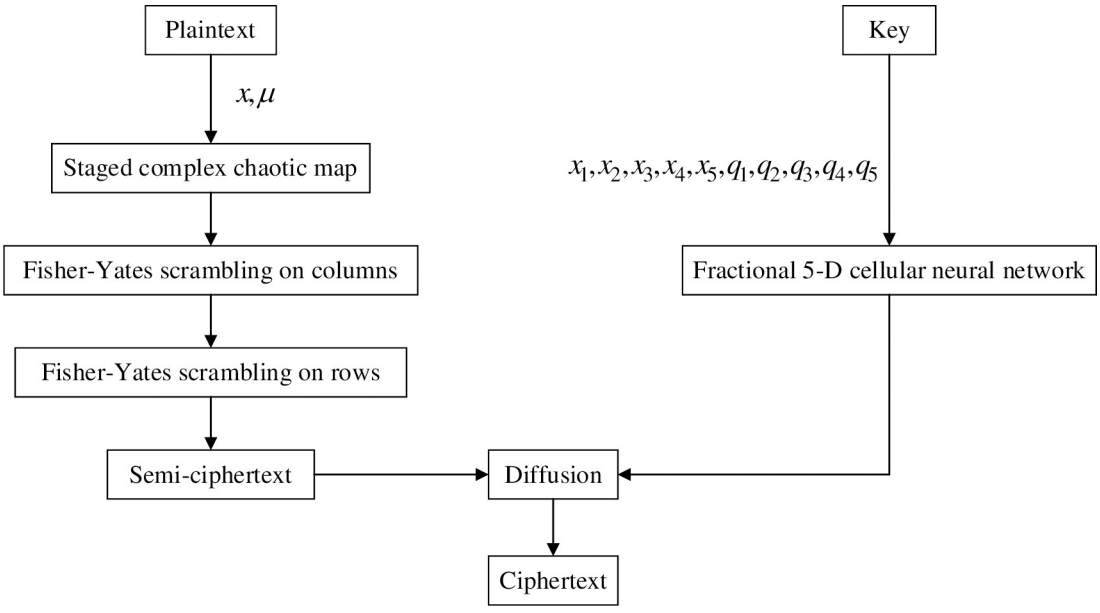
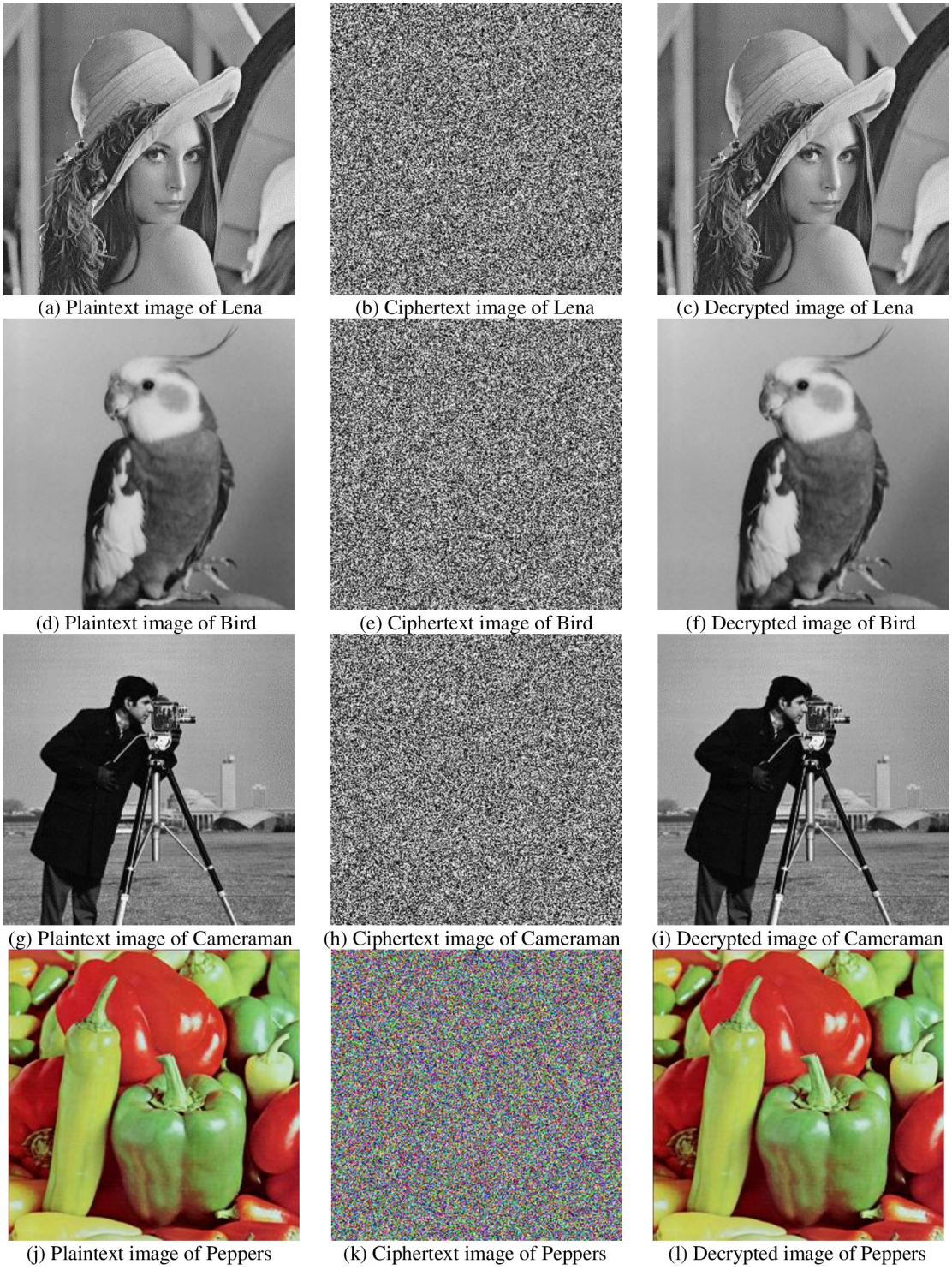


Fig 4. Encryption flow chart.

https://doi.org/10.1371/journal.pone.0236015.g004

4.2 Security analysis

4.2.1 Violent attack. The key in this paper considers that the non-integer key has the precision of 10^{-14}, so its key space should be 2^{128} or more, and the theoretical non-violent cracking has been achieved [20].



(a) Plaintext image of Lena (b) Ciphertext image of Lena (c) Decrypted image of Lena

(d) Plaintext image of Bird (e) Ciphertext image of Bird (f) Decrypted image of Bird

(g) Plaintext image of Cameraman (h) Ciphertext image of Cameraman (i) Decrypted image of Cameraman

(j) Plaintext image of Peppers (k) Ciphertext image of Peppers (l) Decrypted image of Peppers

Fig 5. Plaintext, ciphertext and decrypted image of Lena, bird, cameraman, peppers.

https://doi.org/10.1371/journal.pone.0236015.g005

4.2.2 Key sensitivity analysis. We make a minor change to one key, and the other keys remain unchanged to decrypt the image. The changed values are as follows:

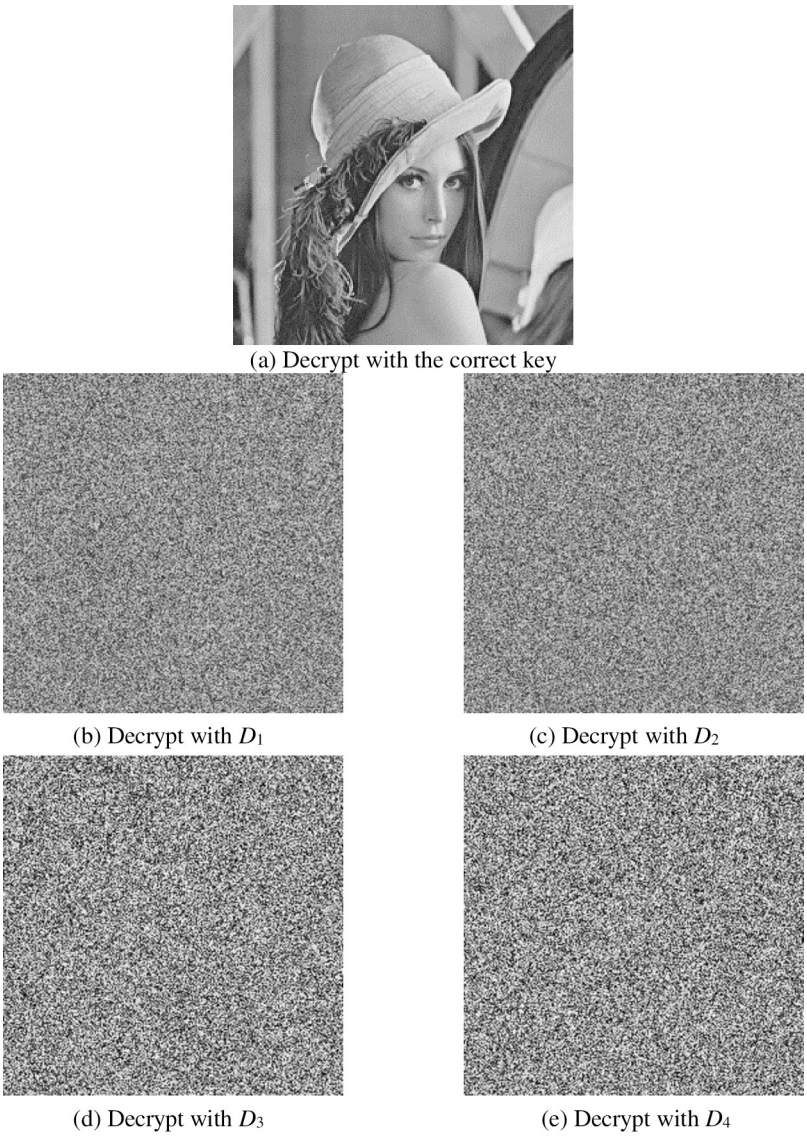
$$D_1 : x = 0.6 + 10^{-14}, \mu_1 = 1.46, x_1 = 0.1, q_1 = 0.98,$$

$$D_2 : x = 0.6, \mu_1 = 1.46 + 10^{-14}, x_1 = 0.1, q_1 = 0.98,$$

$$D_3 : x = 0.6, \mu_1 = 1.46, x_1 = 0.1 + 10^{-14}, q_1 = 0.98,$$

$$D_4 : x = 0.6, \mu_1 = 1.46, x_1 = 0.1, q_1 = 0.98 + 10^{-14},$$

Fig 6 shows the decryption result. It can be seen that when the key is changed in the smallest order, the original image cannot be decrypted, so the algorithm is sensitive to the key.



(a) Decrypt with the correct key

(b) Decrypt with D_1

(c) Decrypt with D_2

(d) Decrypt with D_3

(e) Decrypt with D_4

Fig 6. Decryption with different keys.

https://doi.org/10.1371/journal.pone.0236015.g006

4.2.3 Key statistics analysis. Statistical analysis after image encryption is very important. A good image encryption algorithm should be able to resist any kind of statistical attack. Among them, the histogram analysis of images and the correlation of adjacent pixels are two very important statistical characteristic indicators in image encryption algorithms.

1. Histogram analysis

A histogram is a function graph of the number of pixels of a statistical image having the same attribute value. Generally, the more uniform the pixel values of the ciphertext image processed by the encryption algorithm are, the more uniform the histogram looks [21]. As can be seen from the results of Fig 7, the pixel value distribution of the ciphertext image is obviously more uniform.

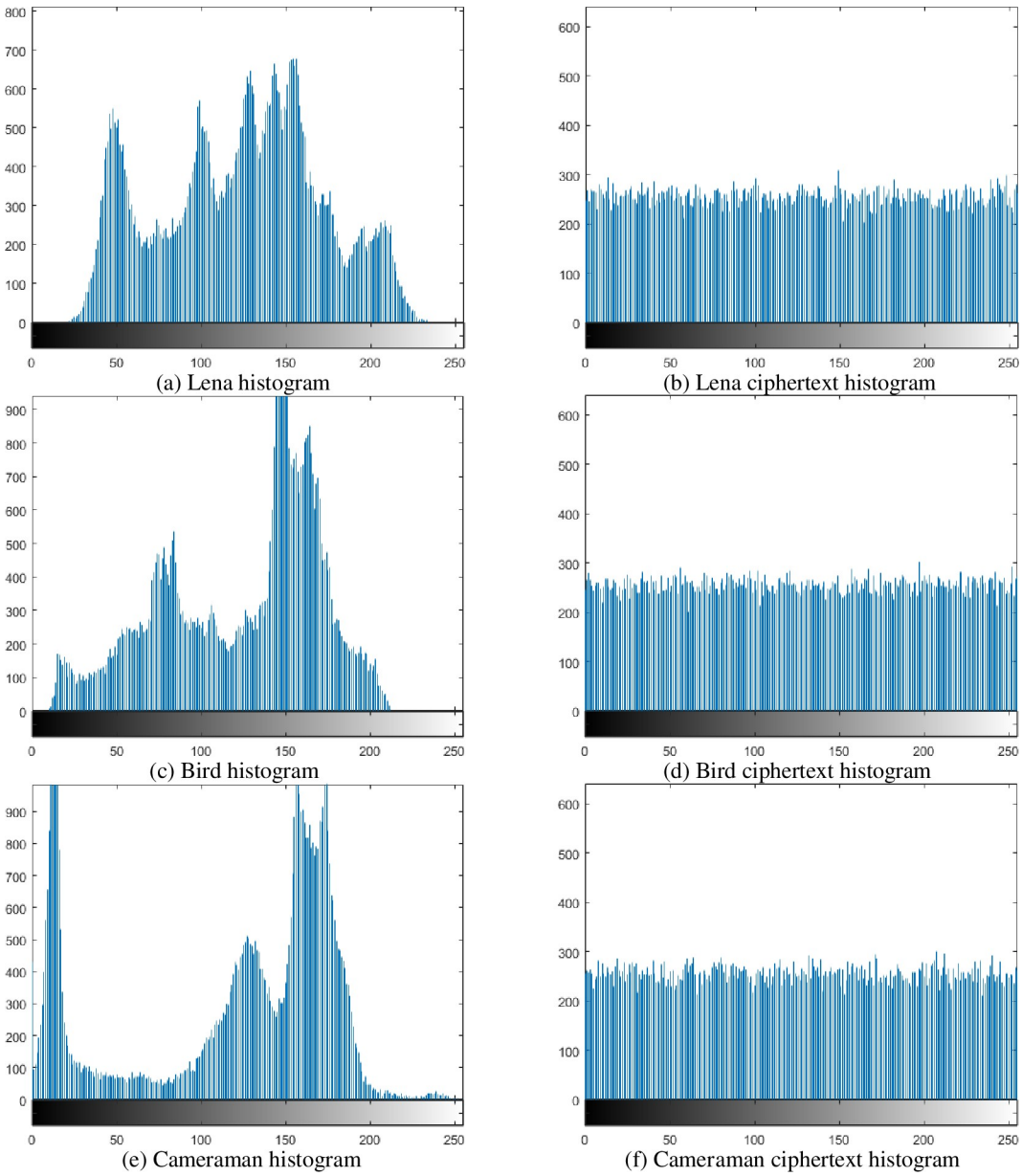


Fig 7. Plaintext and ciphertext histogram.

https://doi.org/10.1371/journal.pone.0236015.g007

2. Adjacent pixel correlation

In the plaintext image, adjacent pixels tend to have strong correlation. In order to avoid others using statistical information attacks, the correlation between adjacent pixels of the ciphertext image must be reduced [22]. The formula for calculating the pixel correlation is

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{17}$$

where

$$\begin{cases} \mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \\ D(x) = \frac{1}{N}\sum_{i+1}^{N}(x_i - E(x))^2 \\ E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \end{cases}. \tag{18}$$

In this paper, the horizontal, vertical and oblique correlations of plaintext and ciphertext are statistically calculated using Eqs (17) and (18). The statistical results are shown in Fig 8. Among them, the Ref. [23] is an algorithm using skewed Tent map and 6th-order CNN, and the literature [24] is an algorithm that uses two hyperchaotic systems for encryption. The Ref. [24, 26] is the current excellent experimental result. The subsequent comparison process goes into the information for the Lena image, and will not be described again. It can be seen from Table 1 that after the encryption of this algorithm, the correlation of the ciphertext is close to 0, and compared with other algorithms, this algorithm has a greater advantage, so it can resist statistical attacks.

3. Information entropy analysis

Information entropy is a way to evaluate the encrypted image. The closer the information entropy value is to 8, the more disordered the encrypted image [26]. The calculation formula of information entropy is as follows:

$$H(s) = \sum_{i=0}^{2^L-1} p(s_i)\log_2\frac{1}{p(s_i)} \tag{19}$$

where $p(s_i)$ is the probability of occurrence of s_i.

Table 2 shows the comparison between this algorithm and other algorithms. It can be seen that the encrypted image is more disordered and can resist statistical attacks.

4.2.4 Differential attack analysis. Differential attacks are a choice of plaintext attacks. That is, by making a slight change to the plaintext, the ciphertext and the modified ciphertext before the encryption algorithm are modified, and the data is analyzed to obtain the key. Therefore, a good image encryption system should be able to make small changes in plaintext can also cause huge changes in ciphertext to be able to withstand differential attacks [27]. The Number Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are respectively

$$NPCR = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\%, \tag{20}$$

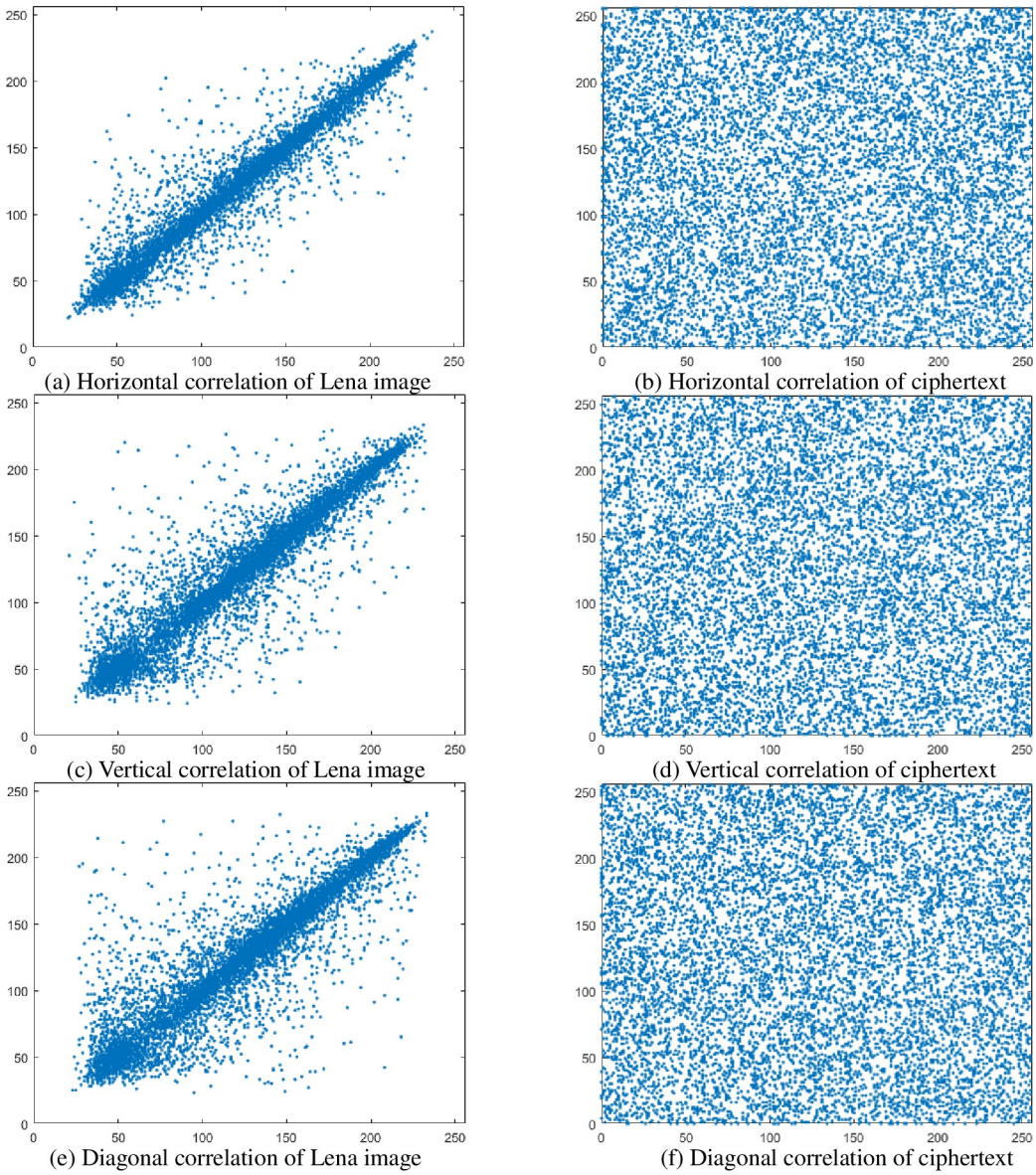


Fig 8. Correlation comparison of plaintext ciphertext.

https://doi.org/10.1371/journal.pone.0236015.g008

Table 1. Correlation between plain image and adjacent pixels of ciphertext image.

Image	Horizontal	Vertical	Diagonal
Lena	0.8951	0.9650	0.9203
Ciphertext of Lena	-0.0002	0.0011	0.0965
Bird	0.9826	0.9810	0.9889
Ciphertext of Bird	-0.0007	0.0024	0.0013
Ref. [23]	-0.0168	0.0445	-0.0022
Ref. [24]	-0.0062	0.0052	0.0043
Ref. [25]	-0.0318	0.0965	0.0362
Ref. [26]	0.0051	-0.0093	-0.0205

https://doi.org/10.1371/journal.pone.0236015.t001

Table 2. Information entropy comparison result.

Image	Information entropy
Lena	7.2775
Ciphertext of Lena	7.9989
Bird	7.2577
Ciphertext of Bird	7.9896
Ref. [23]	7.9744
Ref. [24]	7.9993
Ref. [25]	7.9851
Ref. [26]	7.9991

https://doi.org/10.1371/journal.pone.0236015.t002

and

$$UACI = \frac{1}{W \times H}[\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255}] \times 100\%. \quad (21)$$

Where W and H represents the width and height of the image. C_1 and C_2 are the two ciphertext images after the original plaintext image changes by one pixel value. If $C_1 \neq C_2$, then the corresponding $D(i,j) = 1$, otherwise $D(i,j) = 0$. The larger the value of NPCR, the more sensitive the encryption algorithm is to the changes in the original plaintext image; the larger the value of UACI, the greater the average change intensity [24]. Under ideal conditions, the closer the NPCR is to 99.6049%, the better the UACI is closer to 33.4635%. Table 3 is a comparison between this algorithm and other algorithms. It can be seen from the table that although it is not very close to the ideal value, it can better resist differential attacks.

4.2.5 Cutting and noise attacks. In the process of communication, if signal hijacking is encountered, the transmitted ciphertext may be tampered with. Therefore, in order to prevent malicious hijacking and modify ciphertext, ciphertext should have good performance against scratch attacks. In this paper, the ciphertext is clipped at different positions of 1/16, 1/4, 1/2, and decrypted using the clipped ciphertext. There are not only cutting attacks but also noise attacks. In order to detect the ability to resist noise attacks, this paper uses different strength Gauss noise, salt and pepper noise to attack, as shown in Figs 9 and 10. It can be seen that the encryption algorithm in this paper can resist cutting attacks and noise attacks.

4.2.6 Deviation from uniform histogram. In an ideal encryption model, the encrypted image should have a uniform histogram distribution to hide pixel related information. This means that the encryption algorithm changes the cryptographic pixel values to make the probability of each cryptographic pixel completely uniform. Ref. [28] gives a method for estimating the quality of encryption, uniform histogram deviation (D_H), it is given by Eq (22),

$$D_H = \frac{\sum_{C_i}^{255}|H_{C_i} - H_C|}{M \times N}, \quad (22)$$

Table 3. NPCR and UACI comparison results.

Image	NPCR	UACI
Ciphertext of Lena	99.6302	33.4521
Ciphertext of Bird	99.6218	33.4375
Ref. [22]	99.5643	35.4560
Ref. [23]	99.6002	33.3635
Ref. [24]	99.6140	33.4828
Ref. [25]	99.6239	33.6623

https://doi.org/10.1371/journal.pone.0236015.t003

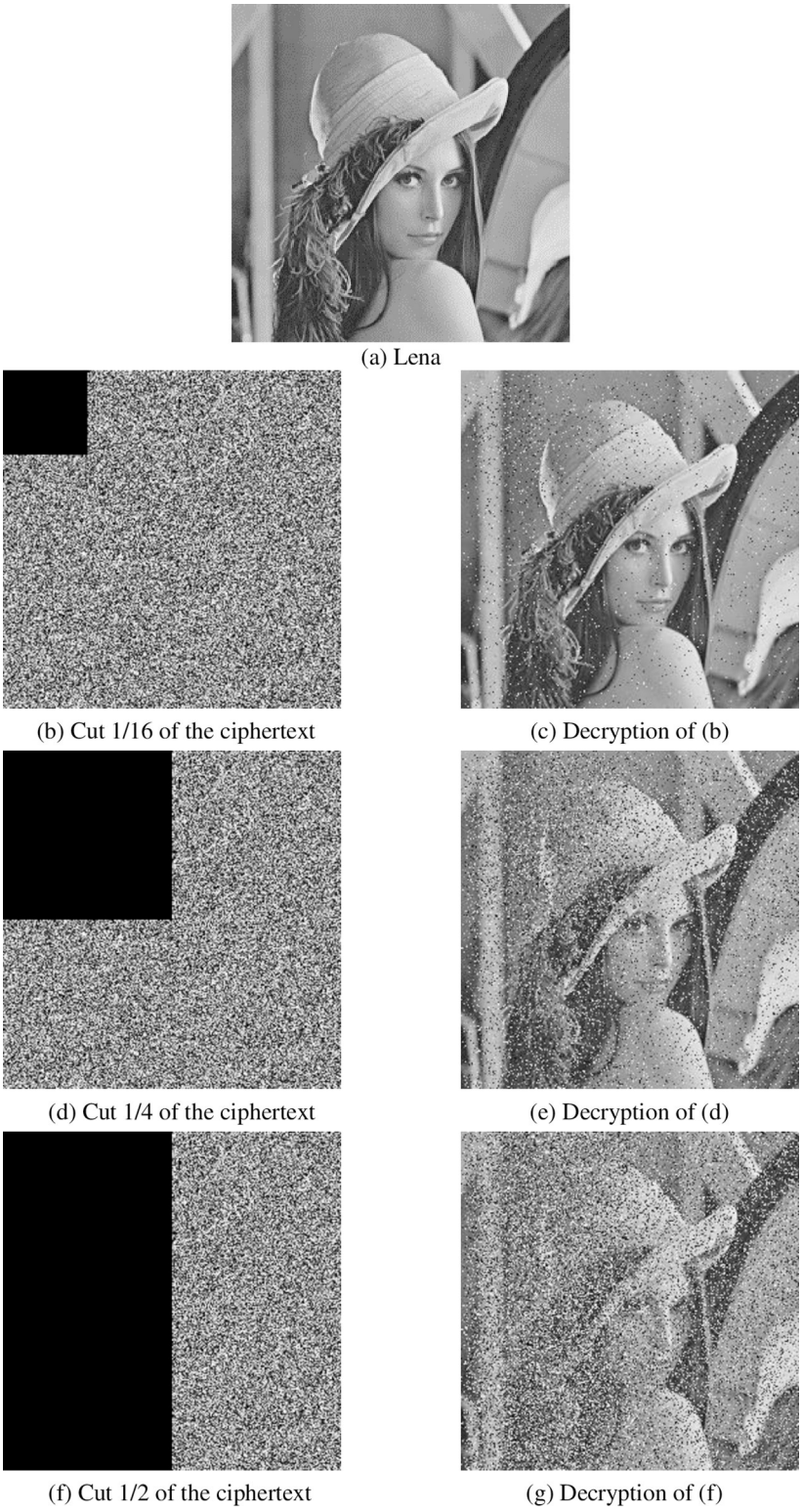


Fig 9. Cutting attack resistance.

https://doi.org/10.1371/journal.pone.0236015.g009

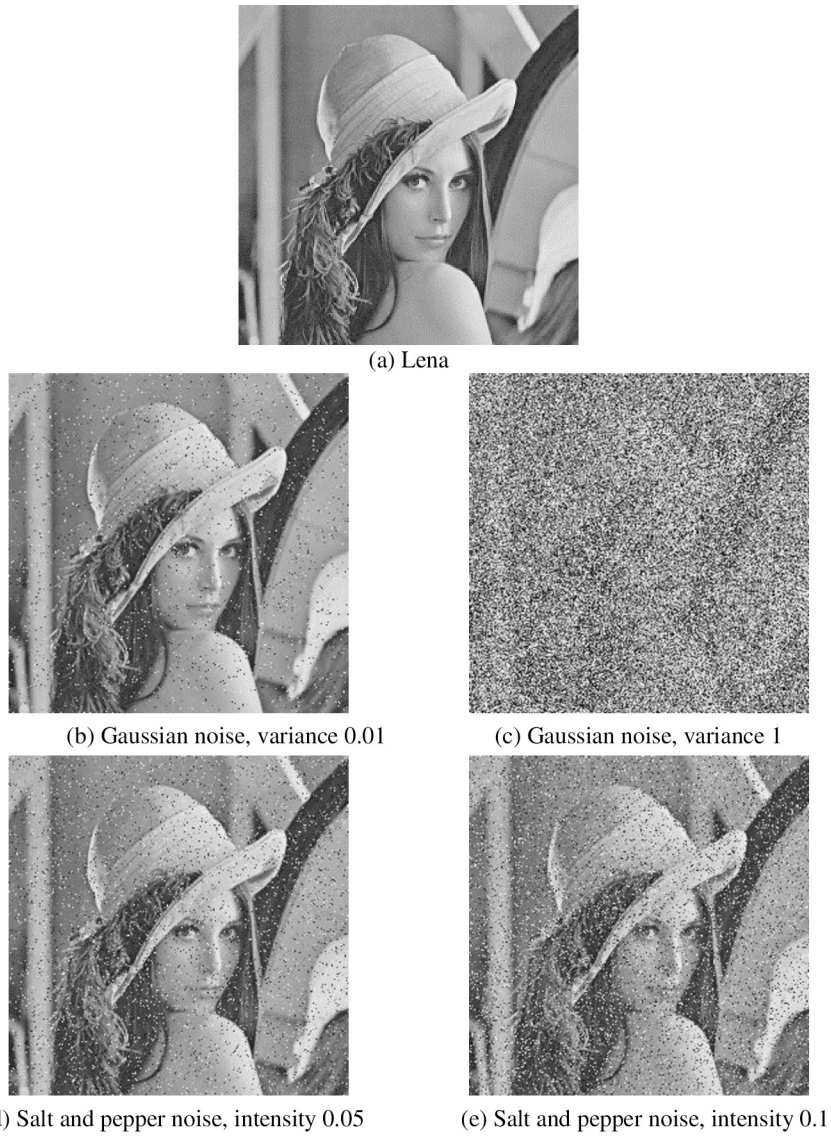


Fig 10. Noise attack resistance.

https://doi.org/10.1371/journal.pone.0236015.g010

where $M \times N$ is the size of the image, H_{C_i} Is the statistic of the ciphertext image at the pixel value of i, H_C is a standard uniform histogram, the statistics of each pixel are $M \times N/256$. It can be seen that when D_H is smaller, it proves that the more uniform the pixel distribution of the ciphertext, the better the encryption effect. We chose some similar chaotic neural networks, as well as some excellent results in some areas for comparison. At the same time, for comparison, this paper also selected the same encrypted images as the comparison references. As shown in Table 4, the D_H value of this algorithm is significantly smaller than other algorithms.

Table 4. Standard histogram deviation comparison result.

Image	Proposed algorithm	Ref. [24]	Ref. [29]	Ref. [30]	Ref. [31]	Ref. [32]
Peppers	0.0531	0.0492	0.0938	0.0979	0.0917	0.0977
Airplane	0.0547	0.0518	0.0969	0.0995	0.0983	0.0943
Boat	0.0503	0.0524	0.0902	0.0995	0.0958	0.0985

https://doi.org/10.1371/journal.pone.0236015.t004

Table 5. Execution time with the same operating environment (unit: s).

Image	Proposed algorithm	Ref. [8]	Ref. [10]
Lena	0.981488	4.230902	1.682497
Cameraman	1.008242	4.330022	1.784329
Peppers	1.007021	4.482100	1.747320

https://doi.org/10.1371/journal.pone.0236015.t005

Table 6. Encryption time and comparisons.

Algorithm	Encryption Time (sec)
Proposed algorithm	0.981488
Ref. [8]	4.230902
Ref. [10]	1.682497
Ref. [20]	1.676400
Ref. [33]	1.205000

https://doi.org/10.1371/journal.pone.0236015.t006

4.2.7 Time analysis. In addition to the security analysis of the algorithm, in practice, the encryption algorithm has a fast encryption speed. In order to test the encryption speed of this algorithm, we tested the encryption speed of three images of size 256×256, run the program 100 times, and obtained the average operation time. As shown in Table 5, we can see that the encryption time of different images is about 1 second, which is more advantageous in time than the literature [8], [10]. Table 6 shows that for the Lena graph, this algorithm is compared with other algorithms. The results show that this algorithm is good in time efficiency.

5 Conclusion

In this paper, two systems are used to encrypt the image. In order to generate a chaotic sequence when using a staged compound chaotic map, the image is randomly scrambled by Fisher-Yates. Using a fractional 5D cellular neural network can increase the complexity of the system, and then serialize the matrix generated by it, and diffuse the image information through XOR processing with the key and the ciphertext to obtain the ciphertext image. Key space analysis, statistical information analysis, differential attack analysis, cropping attack, noise attack, etc., prove the superiority of the algorithm and good resistance to attacks.

Author Contributions

Conceptualization: Chao Luo, Chunpeng Wang.

Writing – original draft: Xingyuan Wang, Yining Su, Chao Luo, Chunpeng Wang.

Writing – review & editing: Xingyuan Wang, Yining Su.

References

1. Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Optics Letters, 1995, 20(7): 767–769 https://doi.org/10.1364/ol.20.000767 PMID: 19859323
2. Peng X, Zhang P, Wei H, Yul B. Known-plaintext attack on optical encryption based on double random phase keys. Optics Letters, 2006, 31(8): 1044–1046 https://doi.org/10.1364/ol.31.001044 PMID: 16625897
3. Liu Z, Guo C, Tan J, Liu W, Wu J J, Wu Q, et al. Securing color image by using phase-only encoding in Fresnel domains. Optics and Lasers in Engineering, 2015, 68: 87–92

4. Sui L S, Zhou B, Ning X J, Tian A L. Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain. Optics Express, 2016, 24 (1): 499–515 https://doi.org/10.1364/OE.24.000499 PMID: 26832280
5. Zhou N R, Li H L, Wang D, Pan S M, Zhou Z H. Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. Optics Communications, 2015, 343: 10–21
6. Ye G D, Pan C, Dong Y X, Shi Y, Huang X L. Image encryption and hiding algorithm based on compressive sensing and random numbers insertion. Signal processing, 2020, 172: 107563
7. Ye G D, Pan C, Huang X L, Mei Q X. An efficient pixel-level chaotic image encryption algorithm. Nonlinear Dynamics, 2018, 94(1): 745–756
8. Luo Y L, Zhou R L, Liu J X, Cao Y, Ding X M. A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. Nonlinear Dynamics, 2018, 93(3): 1165–1181
9. Ye G D, Huang X L. An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing, 2017, 251: 45–53
10. Diab H. An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations. IEEE Access, 2018, 6: 42227–42244
11. Chen S, Han T L. Development Status of Image Encryption Algorithm. China Science and Technology Information, 2012(2): 78–78.
12. Wang L, Song H, Liu P. A novel hybrid color image encryption algorithm using two complex chaotic systems. Optics and Lasers in Engineering, 2016, 77: 118–125
13. Sui L, Liu B, Wang Q, Li Y, Liang J. Color image encryption by using Yang-Gu mixture amplitude-phase retrieval algorithm in gyrator transform domainand two-dimensional Sine logistic modulation map. Optics and Lasers in Engineering 2015, 75: 17–26
14. Liu H, Wang X. Color image encryption based on one-time keys and robust chaotic maps. Computers & Mathematics with Applications, 2010, 59(10): 3320–3327
15. Abuturab M R. An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform. Optics and lasers in engineering, 2015, 69: 49–57
16. Zhang X D, Zhu P, Xie X P, He G G. A dynamic threshold value control method for chaotic neural networks. Acta Physica Sinica, 2013, 62(21): 210506–210506
17. Wang X, Wang S, Zhang Y, Guo K. A novel image encryption algorithm based on chaotic shuffling method. Information Systems Security, 2017, 26(1): 7–16
18. Liu L Z, Zhang J Q, Xu G X, Liang L S, Wang W S. A chaotic secure communication method based on chaos systems partial series parameter estimation. Acta Physica Sinica, 2014, 63(1): 247–254
19. Wang X Y, Li Z M. A color image encryption algorithm based on Hopfield chaotic neural network. Optics and Lasers in Engineering, 2019, 115: 107–118
20. Zhou Y, Cao W, Chen C P. Image encryption using binary bitplane. Signal processing. 2014, 100, 197–207
21. Wang X, Gao S. Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. Information Sciences, 2020, 507: 16–36
22. Behnia S, Akhshania A, MaHmodi H, Akhavan A. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons & Fractals, 2008, 35(2): 408–419
23. Kadir A, Hamdulla A, Guo W Q. Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. Optik—International Journal for Light and Electron Optics, 2014, 125(5): 1671–1675
24. Di X Q, Li J Q, Qi H, Cong L, Yang H. A semi-symmetric image encryption scheme based on the function projective synchronization of two hyperchaotic systems. Plos One, 2017, 12(9): e0184586 https://doi.org/10.1371/journal.pone.0184586 PMID: 28910349
25. Belazi A, El-Latif A A A, Diaconu A V, Rhouma R, Belghitha S. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Optics and Lasers in Engineering, 2017, 88: 37–50
26. Wei X, Guo L, Zhang Q, Zhang G, Lian S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. Journal of Systems and Software, 2012, 85(2): 290–299
27. Wang X Y, Feng L, Zhao H Y. Fast image encryption algorithm based on parallel computing system. Information Sciences, 2019, 486: 340–358
28. Elashry I F, Faragallah O S, Abbas A M, El-Rabaie S, Abd El-Samie F E. A new method for encrypting images with few details using Rijndael and RC6 block ciphers in the electronic code book mode. Information Security Journal A Global Perspective, 2012, 21(4): 193–205

29. Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos. Signal Processing, 2012, 92(4): 1101–1108

30. Wang X, Liu L, Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Optics and Lasers in Engineering, 2015, 66: 10–18

31. Belazi A, Abd Ellatif A A, Belghith S. A novel image encryption scheme based on substitution-permutation network and chaos. Signal Processing, 2016, 128: 155–170

32. Hua Z, Zhou Y, Pun C M, Chen C L P. 2D Sine Logistic modulation map for image encryption. Information Sciences, 2015, 297: 80–94

33. Wang X, Cavusoglu U, Kacar S, Akgul A, Pham V T, Jafari S, et al. S-box based image encryption application using a chaotic system without equilibrium. Applied Sciences-Basel, 2019, 9(4): 781