RESEARCH ARTICLE

# A new secure image encryption algorithm based on a 5D hyperchaotic map

**Dejian Fang**[1,2], **Shuliang Sun**[2]*

**1** College of Computer Science, Chongqing University, Chongqing, China, **2** School of Electronics and Information Engineering, Fuqing Branch of Fujian Normal University, Fuqing, China

* tjussl_07@126.com

## Abstract

Image encryption is an effective method for protecting private images during communication. In this paper, a novel image encryption method is proposed based on a 5D hyperchaotic system. Since a 5D hyperchaotic system can generate more complex dynamic behavior than a low-dimensional system, it is used in this paper to generate pseudorandom number sequences. The generated sequences are processed to obtain new sequences. The randomness of the new sequences is improved by recombination and rearrangement. The experimental results and theoretical analysis show that the method possesses a large key space and can resist differential attacks, statistical analysis, entropy analysis, clipping attacks and noise attacks. Therefore, it is very secure and can be used for secure communication.

**Citation:** Fang D, Sun S (2020) A new secure image encryption algorithm based on a 5D hyperchaotic map. PLoS ONE 15(11): e0242110. https://doi.org/10.1371/journal.pone.0242110

**Editor:** Hua Wang, Victoria University, AUSTRALIA

**Received:** June 11, 2020

**Accepted:** October 26, 2020

**Published:** November 12, 2020

**Data Availability Statement:** All relevant data are within the manuscript and its Supporting Information files.

**Funding:** The authors received no specific funding for this work.

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

## 1 Introduction

With the rapid development of the Internet and communication technologies, researchers have focused increasingly more on information security. Images are known as one of the most important and popular multimedia technologies and are widely transmitted over the Internet. It is important to protect private images from hackers during communication. Image encryption is an effective method for protecting private images during communication, and many image encryption methods have been proposed [1–3]. Chaos is famous for its sensitivity to initial conditions and system parameters, pseudorandomness, ergodicity and reproduction. It is suitable for image encryption. Many chaotic image cryptosystems have been proposed [4–9]. Gao et al. [4] proposed a new nonlinear chaotic algorithm based on a power function and tangent function. The system parameters were obtained by experimental analysis. It is a one-time password system. Wang and Zhang [5] proposed a new color image encryption method based on bit permutations and correlated chaos. Heterogeneous a bit permutation process was adopted to reduce the computational cost and improve the permutation efficiency. An expanded XOR operation was also employed for the red (R), green (G) and blue (B) components of color images. Sun [6] proposed an image encryption scheme based on DNA operations and a chaotic map. A two-dimensional sine iterative chaotic map with an infinite collapse matrix was employed. An extended XOR operation was also applied to improve the security of the system. Liu and Wang [7] proposed a color image encryption scheme based on one-time keys. Image encryption using the DNA complementary rule and chaotic system was proposed in [8]. Wang et al. [9] proposed a chaotic image encryption algorithm based on a perception model. A fast image encryption algorithm based on the perceptron model was proposed in [10]. Wang and Gao proposed an image encryption algorithm based on matrix semi-tensor product theory and a Boolean network [11–12]. However, many image encryption methods employ low-dimensional chaotic systems [13–16]. Low-dimensional chaotic systems have a small key space and parameters. They are not safe enough to use as an image cryptosystem.

A hyperchaotic system is a better image cryptosystem than a low-dimensional chaotic system. A hyperchaotic system has more than one positive Lyapunov exponent. It generates more complex dynamic behavior and higher randomness than low-dimensional chaotic systems [17–21]. Ye and Wong [18] designed an image encryption scheme based on a time delay and a hyperchaotic system. A permutation function and double diffusion operations were executed in both the forward and reverse directions. Sun [19] proposed a novel hyperchaotic image encryption algorithm based on pixel-level scrambling, bit-level scrambling and DNA encoding. A 5-D hyperchaotic system was executed to generate chaotic sequences. Chen [20] proposed a fast chaos-based image encryption scheme with a dynamic state variable selection mechanism. Liu and Kadir [22] proposed color image encryption using bit-level permutations and a high-dimensional chaotic system. Sun et al. [23, 24] proposed a novel hyperchaotic image encryption method. Since a 5-D hyperchaotic system [25] has three positive Lyapunov exponents and generates more complex dynamic behavior than a low-dimensional system, we also adopt a 5-D hyperchaotic system to generate chaotic sequences in this paper. To eliminate the correlations between adjacent elements in chaotic sequences, the generated sequences are pretreated before being used for scrambling and diffusion. Compared with other encryption algorithms, the proposed method has advantages in efficiency and security.

In this paper, we propose a new image encryption method based on a 5D hyperchaotic system. First, a 5D hyperchaotic system is used to generate chaotic sequences. Then, chaotic sequences are preprocessed to obtain new sequences, which are used in the image confusion and diffusion processes.

The rest of this paper is organized as follows. The 5D hyperchaotic system and chaotic sequence generation are introduced in Section 2. The confusion and diffusion methods are described in Section 3. Section 4 discusses the experimental results and safety analysis. The conclusions are given in Section 5.

# 2 5D hyperchaotic system and chaotic sequence generation

## 2.1 5D hyperchaotic system

A 5D hyperchaotic system [25] can be described as follows:

$$\begin{cases} \dot{x}_1 = a_1(x_2 - x_1) + x_4 + a_2x_5 \\ \dot{x}_2 = a_3x_1 - x_2 - x_1x_3 \\ \dot{x}_3 = -a_4x_3 + x_1x_2 \\ \dot{x}_4 = a_5x_4 - x_1x_3 \\ \dot{x}_5 = a_6x_1 + a_7x_2 \end{cases} \tag{1}$$

where $a_1$, $a_2$, $a_3$, $a_4$, $a_5$, $a_6$ and $a_7$ are system parameters. When $a_1 = 10$, $a_2 = 1$, $a_3 = 28$, $a_4 = 8/3$, $a_5 = 2$, $a_6 = -1$ and $a_7 = 1$, the 5D hyperchaotic system is in a chaotic state and can produce five chaotic sequences. The sequence trajectories of system (1) are displayed in Fig 1.

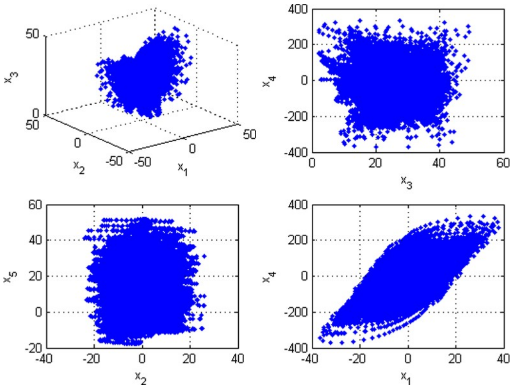

**Fig 1. Sequence trajectories of system (1) with ($a_1$, $a_2$, $a_3$, $a_4$, $a_5$, $a_6$, $a_7$) = (10, 1, 28, 8/3, 2, -1, 1).**

https://doi.org/10.1371/journal.pone.0242110.g001

## 2.2 Preprocessing of chaotic sequences

1. Calculate the initial values of system (1) as follows:

$$\begin{cases} x_1(1) = \mathrm{mod}\left(\sum_{j=1}^{5} x_j^0 + \frac{\sum_{z=1}^{MN} P(z)}{MN}, 1\right) \\ x_i(1) = \mathrm{mod}(x_{i-1}(1) + x_i^0, 1) \quad i = 2, 3, 4, 5, \end{cases} \tag{2}$$

where $x_1^0$, $x_2^0$, $x_3^0$, $x_4^0$ and $x_5^0$ are the initial secret keys, and mod $(x, y)$ represents the residue of $x$ divided by $y$. The row and column of original plain image $P$ are $M$ and $N$.

2. System (1) is iterated $N_0$ times to eliminate the transient response.

$$N_0 = 300 + \mathrm{mod}\left(floor\left(\sum_{i=1}^{5} x_i^0 \times 10^{10}\right), 300\right) \tag{3}$$

where $floor$ $(x)$ returns the nearest integer value less than or equal to $x$.

3. System (1) continues to iterate $MN/4$ times to generate five real-number sequences: $X = [x_1, x_2, \ldots, x_{MN/4}]$, $Y = [y_1, y_2, \ldots, y_{MN/4}]$, $Z = [z_1, z_2, \ldots, z_{MN/4}]$, $U = [u_1, u_2, \ldots, u_{MN/4}]$, and $V = [v_1, v_2, \ldots, v_{MN/4}]$.

4. Four sequences are chosen from the five chaotic sequences, and they are combined to become a new sequence with the length $MN$. There are 120 kinds of arrangement modes according to an arrangement study. For example, $A_1 = \{Y, Z, V, X\}$, $A_2 = \{X, V, Z, U\}$, $A_3 = \{V, X, Z, Y\}$ and $A_4 = \{U, Y, Z, V\}$.

5. Sequences $A_1$, $A_2$ and $A_3$ are rearranged to form new sequences $A_1$', $A_2$' and $A_3$', respectively. The processes of these rearrangements are demonstrated in Eqs 4 and 5.

$$[g, h] = \text{sort } (A_4) \tag{4}$$

$$A_j'(i) = A_j(h(i)), \tag{5}$$

where sort is a sorting function; $i = 1, 2, \ldots, MN$; $j = 1, 2, 3$; $g$ is the new sequence; and $h$ is the index value of $g$.

## 3 Confusion and diffusion methods

### 3.1 Confusion method

1. The sequence of $A_1^{'}$ is modified first as Eq 6.

$$A_1^{'}(i) = \mathrm{mod}\big(floor(abs(A_1^{'}(i) \times 10^{10})), MN\big) \tag{6}$$

where $i = 1, 2, \ldots, MN$, and $abs(x)$ is the absolute value of $x$.

2. Suppose $i$ and $i^{'}$ are the positions of plain image $P$. The corresponding confusion image is denoted as $P^{'}$, and it is calculated as follows:

$$i^{'} = i + \mathrm{mod}\big(A_1^{'}(i) + P^{'}(i-1), MN + 1 - i\big) \tag{7}$$

where $i = 1, 2, \ldots, MN$, and $P^{'}(0)$ is designated as the initial secret key.

3. The scrambling method is executed as

$$P^{'}(i) = P(i^{'}),\ P(i^{'}) = P(i) \tag{8}$$

where $P^{'}(i)$ is the scrambling image positioned at $i$, $P(i')$ and $P(i)$ are the plain images positioned at $i$' and $i$, respectively, for $i = 1, 2, \ldots, MN$.

### 3.2 Diffusion method

1. The sequences $A_2^{'}$ and $A_3^{'}$ are modified as Eqs 9 and 10.

$$A_2^{'}(i) = \mathrm{mod}\big(floor(abs(A_2^{'}(i)) \times 10^{15}), 8\big) \tag{9}$$

$$A_3^{'}(i) = \mathrm{mod}\Big(floor(abs(A_3^{'}(i)) \times 10^{15}), 256\Big) \tag{10}$$

where $A_2^{'}(i)\epsilon[0, 7]$, $A_3^{'}(i)\epsilon[0, 255]$ and $i = 1, 2, \ldots, MN$.

2. Convert decimal sequences P' and $A_2^{'}$ into the corresponding binary sequences.

3. Sequence Q is obtained by Eq 11.

$$Q(r) = \mathrm{CIRSFT}\big[P'(r), LSB(A_2^{'}(r)), A_2^{'}(r)\big] \tag{11}$$

where CIRSFT $[r, s, t]$ represents the $t$-bit cyclic shift on binary sequence $r$. $LSB(t)$ represents the smallest bit of $t$. The left cyclic shift or right cyclic shift will be decided by $s = 0$ or $s = 1$.

4. Convert the binary sequence $Q$ into its decimal sequence.

5. Diffusion sequence $C$ is obtained by Eqs 12–14.

$$sum = floor\left(\left(\sum_{j=1}^{5} x_j^0 + \frac{P^{'}(0)}{256}\right) \times 10^{15}\right) \tag{12}$$

$$C(1) = A_3^{'}(1) \oplus \mathrm{mod}(A_3^{'}(1) + Q(1), 256) \oplus \mathrm{mod}(sum, 256) \tag{13}$$

$$C(i) = A_3^{'}(i) \oplus \mathrm{mod}(A_3^{'}(i) + Q(i), 256) \oplus C(i-1) \tag{14}$$

where $Q(i)$, $A_3^{'}(i)$, $C(i)$ and $C(i\text{-}1)$ represent the decimal sequence value, chaotic sequence value, diffusion sequence value and previous diffusion value, respectively, and $i = 2, 3, \ldots, MN$.

6. Convert $C$ to a gray image $P^{''}$. Finally, encrypted image $P^{''}$ is obtained.

The flowchart of the image encryption procedure is displayed in Fig 2.

The decryption algorithm is the reverse process of the encryption algorithm.

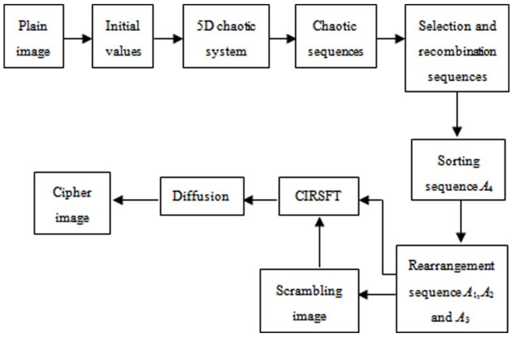

**Fig 2. Flowchart of the image encryption procedure.**

https://doi.org/10.1371/journal.pone.0242110.g002

## 4 Experimental results and safety analysis

In this paper, MATLAB 2010b is applied to execute the algorithm. The experiments are executed on a computer with a Windows 7 operating system, inter(R) Core (TM) i3-3220, 3.3 GHz and 8.00 GB RAM. The initial values of the 5D chaotic system are $x_1^0 = 2.2356$, $x_2^0 = 1.9057$, $x_3^0 = 0.7468$, $x_4^0 = 2.1577$, $x_5^0 = 0.9723$ and $P^{'}(0) = 128$. The 256×256 gray images "Boat", "Tiffany" and "Peppers" are used as the plain images. The plain, cipher and deciphered images are shown in Fig 3.

### 4.1 Key space analysis

In this paper, the key space is determined by the initial values of the 5-D hyperchaotic system $\{x_i^0{}_, i = 1, 2, \ldots, 5\}$. If the precision of the system is $10^{-15}$, the key space is approximately $(10^{15})^5 = 10^{75} \approx 2^{249}$. It is larger than $2^{100}$, so the proposed method could effectively resist a brute-force attack.

Other encryption schemes are compared with the proposed method in Table 1. It can be seen that the key space of the proposed method is much larger than those of Refs [26, 31] but smaller than that of Ref [19]. Although the key space in Ref [19] is larger than that of our scheme, it has more secret keys and is more complex.

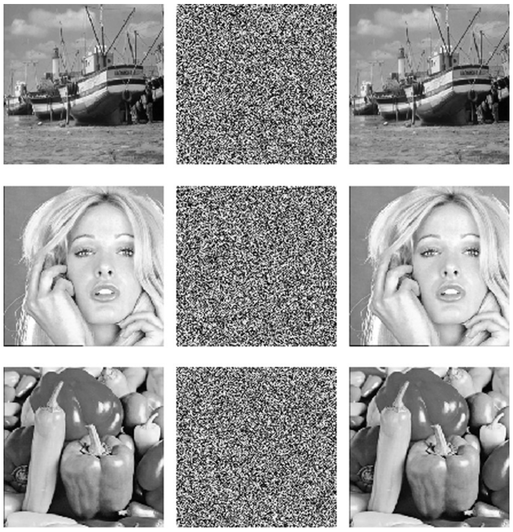

**Fig 3. Encryption and decryption results.** (a) Boat (b) Cipher image, (c) Decoded image, (d) Tiffany, (e) Cipher image, (f) Decoded image, (g) Pepper (h) Cipher image, (i) Decoded image.

https://doi.org/10.1371/journal.pone.0242110.g003

**Table 1. Key space results comparison with other methods.**

| Schemes | Ref [19] | Ref [26] | Ref [31] | proposed |
|---|---|---|---|---|
| Key space | $10^{90}$ | $10^{70}$ | $10^{58}$ | $10^{75}$ |

https://doi.org/10.1371/journal.pone.0242110.t001

## 4.2 Key sensitivity analysis

An excellent cryptosystem should be sensitive to the initial keys. Two completely different cipher images can be produced if a minor change ($10^{-15}$) is made and the other four keys are unchanged. The cipher image also cannot be decrypted correctly if even a slight change ($10^{-15}$) is made between the encryption and decryption keys. The key sensitivity test is shown in Fig 4.

Key $x_1$ is changed to $x_1$+$10^{-15}$, and the cipher image is displayed in Fig 4(A). The value of $x_2$ is modified to $x_2$+$10^{-15}$, and the corresponding cipher image is shown in Fig 4(B). The value of $x_4$ is altered to $x_4$+$10^{-15}$ to decipher Fig 3(H), and the deciphered image is shown in Fig 4(C). Fig 4(D) is the deciphered image when $x_5$ is altered to $x_5$+$10^{-15}$. Table 2 shows the differences between the different cipher and decipher images.

It can be concluded that a small difference in the secret key will generate a completely different cipher image. It also cannot extract the correct deciphered image. If the secret key and plain image have a slight alteration, it is impossible to decrypt the plain image. The pixels differ by approximately 99.6% between the original image and the decrypted image.

## 4.3 Histogram analysis

The histogram of the cipher image should be as uniform as possible. In the proposed method, the histograms of the plain and cipher images of Boat, Tiffany and Pepper are displayed in Fig 5. It is shown that the plain image pixel values are centralized around some values; however, the corresponding cipher image pixel values are very smooth and even. Therefore, it makes a statistical attack ineffective.

The chi-square test [27, 28] is often used to measure the uniformity of the histogram. The chi-square results are listed in Table 3 for different cipher images.

It can be shown from Table 3 that all values generated by the proposed method are smaller than the theoretical value of 293.25 [29, 30]. It can be proven that the distribution of the histogram is flat, and the proposed method could pass the chi-square test.

## 4.4 Correlation analysis

The plain image pixel has a great correlation with its neighboring pixels. An excellent cryptosystem should reduce this correlation to close to zero. The correlation coefficient, $r_{xy}$, between

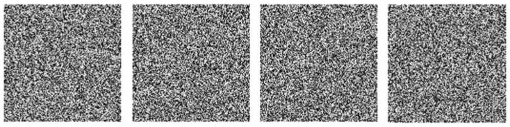

**Fig 4.** The key sensitivity test: (a) cipher image with $x_1$ changed to $x_1$+$10^{-15}$; (b) cipher image with $x_2$ changed to $x_2$+$10^{-15}$; (c) deciphered image with $x_4$ changed to $x_4$+$10^{-15}$; (d) deciphered image with $x_5$ changed to $x_5$+$10^{-15}$.

https://doi.org/10.1371/journal.pone.0242110.g004

**Table 2. Differences between the cipher and decipher images with minor key modifications.**

| Figures | Secret keys | | | | | Comparison with Fig 3(H) |
|---|---|---|---|---|---|---|
| | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | |
| Fig 3(H) | $x_1^0$ | $x_2^0$ | $x_3^0$ | $x_4^0$ | $x_5^0$ | - |
| Fig 4(A) | $x_1^0+10^{-15}$ | $x_2^0$ | $x_3^0$ | $x_4^0$ | $x_5^0$ | 0.9965 |
| Fig 4(B) | $x_1^0$ | $x_2^0+10^{-15}$ | $x_3^0$ | $x_4^0$ | $x_5^0$ | 0.9974 |
| Fig 4(C) | $x_1^0$ | $x_2^0$ | $x_3^0$ | $x_4^0+10^{-15}$ | $x_5^0$ | 0.9963 |
| Fig 4(D) | $x_1^0$ | $x_2^0$ | $x_3^0$ | $x_4^0$ | $x_5^0+10^{-15}$ | 0.9954 |

https://doi.org/10.1371/journal.pone.0242110.t002

two adjacent pixels, $x$ and $y$, is defined as:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,\ D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{15}$$

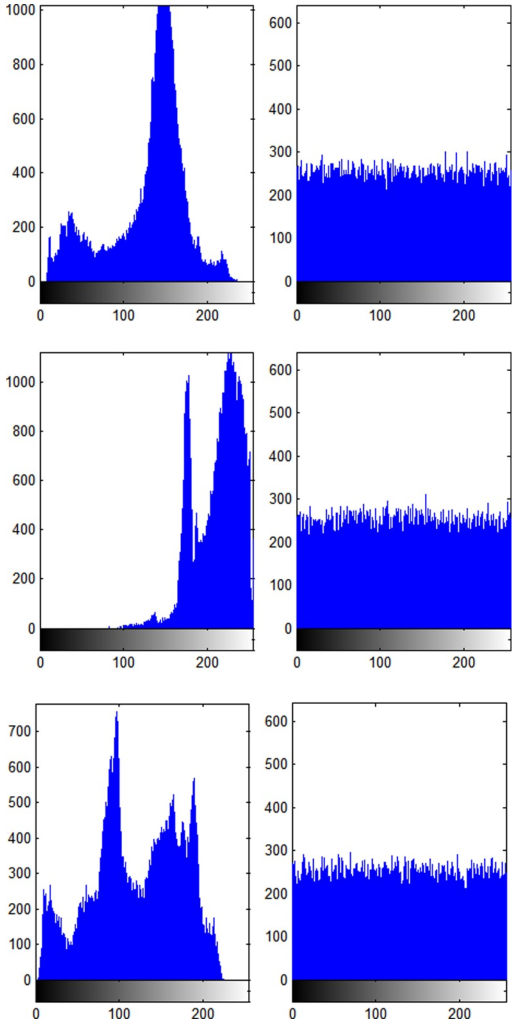

**Fig 5. Histogram of the plain and cipher images.** (a) Boat's histogram (b) Boat's cipher histogram, (c) Tiffany's histogram, (d) Tiffany's cipher histogram, (e) Pepper's histogram, (f) Pepper's cipher histogram.

https://doi.org/10.1371/journal.pone.0242110.g005

**Table 3. Chi-square test of the histograms.**

| Image | Boat | Tiffany | Pepper |
|---|---|---|---|
| $\chi^2_{test}(255)$ | 293.25 293.25 293.25 | | |
| $\chi^2_{test}$ | 245.37 | 265.62 | 256.29 |
| Decision | Pass | Pass | Pass |

https://doi.org/10.1371/journal.pone.0242110.t003

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{16}$$

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

A total of 7225 pairs of adjacent pixels in the "Pepper" plain and cipher images are selected in the horizontal, vertical and diagonal directions. Fig 6 displays the correlation between two adjacent pixels in the plain image Pepper and the corresponding cipher image. It can be concluded that the pixels are highly correlated in the original image, while the correlation is considerably reduced in the cipher image.

Table 4 displays the correlation coefficients of the plain image Pepper and the cipher image.

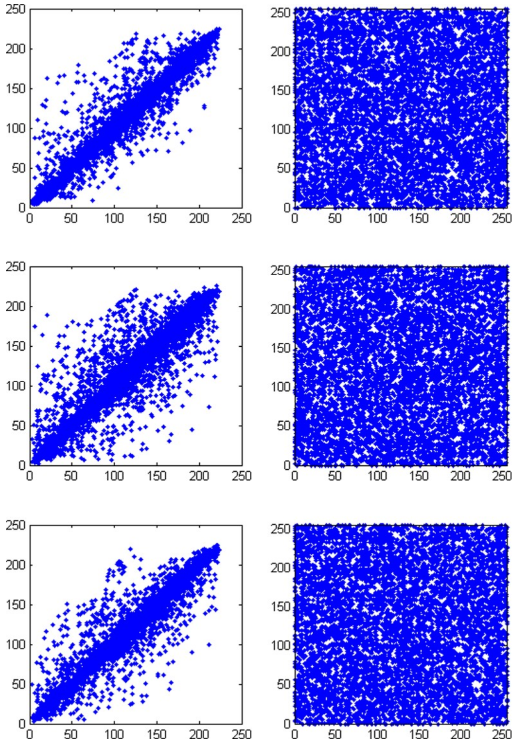

**Fig 6. Correlation between the plain image Pepper and the cipher image in three directions.** (a) Horizontal direction of the plain image, (b) Horizontal direction of the cipher image, (c) Vertical direction of the plain image, (d) Vertical direction of the cipher image, (e) Diagonal direction of the plain image, (f) Diagonal direction of the cipher image.

https://doi.org/10.1371/journal.pone.0242110.g006

**Table 4. Correlation coefficients of the adjacent pixels in the Pepper image.**

| | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| Plain image | 0.9391 | 0.9700 | 0.9146 |
| Cipher image | 0.0068 | -0.0054 | 0.0010 |

https://doi.org/10.1371/journal.pone.0242110.t004

## 4.5 Information entropy analysis

Information entropy is the most important characteristic of randomness. If $m$ is the information source, the information entropy can be defined as follows:

$$H(m) = -\sum_{i=1}^{L} p(m_i)\log_2 p(m_i) \tag{18}$$

where $p(m_i)$ represents the frequency of symbol $m_i$, and $L$ denotes the number of $m_i$. The information entropy data of the cipher image are shown in Table 5.

As displayed in Table 5, the information entropies of the cipher images are close to 8 bits. This also means that the ciphered image with our algorithm is very uniform. This result demonstrates that our method can resist entropy attacks. It can also be found that our algorithm is better than other similar methods.

## 4.6 Differential attack analysis

NPCR and UACI are two important parameters that are often employed to measure the sensitivity to plaintext [26]. These are defined as follows:

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\% \tag{19}$$

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \tag{20}$$

$$D(i,j) = \begin{cases} 0, & if\ C_1(i,j) = C_2(i,j) \\ 1, & else \end{cases} \tag{21}$$

where $M$ and $N$ denote the width and height of the image, respectively, and $C_1$ and $C_2$ represent the ciphered images before and after one pixel of the plain image is modified, respectively.

**Table 5. Information entropy of the cipher image.**

| Image | Boat | Tiffany | Pepper |
|---|---|---|---|
| Proposed | 7.9968 | 7.9972 | 7.9978 |
| Ref. [19] | 7.9967 | 7.9970 | 7.9976 |
| Ref. [26] | 7.9963 | 7.9966 | 7.9971 |
| Ref. [31] | 7.9965 | 7.9969 | 7.9973 |
| Ref. [15] | 7.9967 | 7.9970 | 7.9972 |

https://doi.org/10.1371/journal.pone.0242110.t005

The values of NPCR and UACI are shown in Table 6. It can be concluded that the proposed algorithm can effectively resist differential attacks.

## 4.7 Clipping and noise attack analysis

A good cryptosystem should be designed to resist noise attacks and clipping attacks. The ciphered Pepper image of Fig 2(H) is cropped by 1/8, 1/4 and 1/2, and the decryption results are shown in Fig 7.

Salt and pepper noise and white Gaussian noise are added to the ciphered Pepper image in Fig 2(H), and the deciphered images are shown in Fig 8. When the variance of the white Gaussian noise is increased from 0.001 to 0.01, more noise points appear in the deciphered image, but the deciphered image is still recognizable. Similar results were obtained for the salt and pepper noise.

The results prove that the proposed method effectively resists cropping and noise attacks.

The peak signal-to-noise ratio (*PSNR*) is used to measure the ability of the method to resist noise and data loss [32]. It is adopted to measure the difference between plain image *I* and cipher image *I'*. The PSNR is defined as follows:

$$PSNR = 20\log_{10}\frac{255}{\sqrt{MSE}} \tag{22}$$

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I_{ij} - I'_{ij})^{2} \tag{23}$$

The higher the value of the PSNR is, and the smaller the difference between I and *I'*. The results are shown in Tables 7 and 8.

It can be seen from Tables 7 and 8 that the proposed algorithm obtains higher PSNR values than those in [32–34] when decrypting images under noise and cropping attacks. Therefore, the proposed scheme is superior to the comparative ones.

## 4.8 Classical types of attacks

There are four classical types of attacks: ciphertext only, known plaintext, chosen ciphertext, and chosen plaintext. If a cryptosystem can resist a chosen plaintext attack, then it will be able to resist other attacks [3].

The proposed method is sensitive to initial values $x_i^0$ (i = 1, 2, 3, 4, 5) and the plain image. If one of them is changed, then the generated chaotic sequences will be completely different. The ciphered value not only connects to the confused pixel but also connects to the former confused pixel value and former ciphered value. This means that different ciphered values have different former confused values and different ciphered values. Therefore, the proposed scheme could defend against chosen plaintext attacks.

**Table 6. NPCR and UACI values for cipher images.**

| Image | NPCR (%) | UACI (%) |
|---|---|---|
| proposed | 99.62 | 33.47 |
| Ref. [26] | 99.60 | 33.48 |
| Ref. [19] | 99.61 | 33.46 |
| Ref. [31] | 99.60 | 33.45 |
| Ref. [15] | 99.59 | 33.42 |

https://doi.org/10.1371/journal.pone.0242110.t006

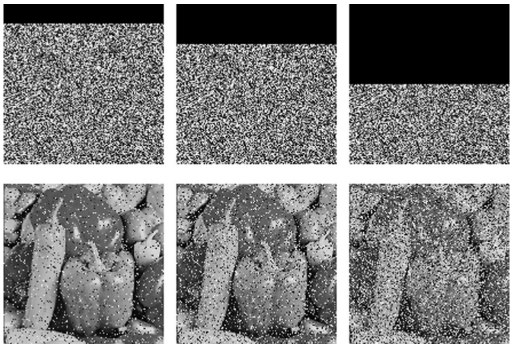

**Fig 7. Recovery after different degrees of cropping attacks.** (a) 1/8 cropped, (b) 1/4 cropped, (c) 1/2 cropped, (d) deciphered of (a), (e) deciphered of (b), (f) deciphered of (c).

https://doi.org/10.1371/journal.pone.0242110.g007

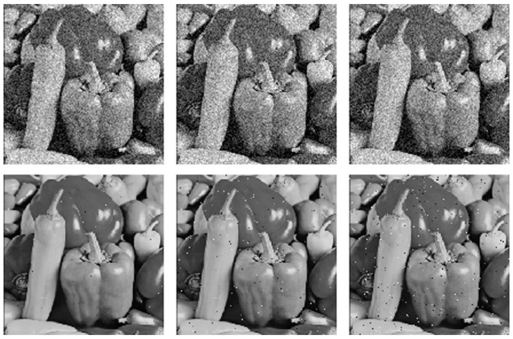

**Fig 8. Decryption results with different noise.** (a) Gaussian v = 0.001, (b) Gaussian v = 0.005, (c) Gaussian v = 0.01, (d) Salt and pepper d = 0.001, (e) Salt and pepper d = 0.005, (f) Salt and pepper d = 0.01.

https://doi.org/10.1371/journal.pone.0242110.g008

**Table 7. PSNR values of different schemes with different percentages of salt and pepper noise.**

| Method | Noise density (%) | | | | | |
|---|---|---|---|---|---|---|
| | 0.01 | 0.05 | 0.1 | 0.5 | 1 | 5 |
| Ref. [32] | 41.40 | 34.17 | 30.93 | 24.03 | 21.18 | 14.32 |
| Ref. [33] | 9.52 | 8.93 | 8.62 | 8.56 | 8.55 | 8.55 |
| Ref. [34] | 42.69 | 36.84 | 31.53 | 28.71 | 9.29 | 18.84 |
| Proposed | 59.69 | 56.79 | 52.46 | 48.51 | 43.59 | 38.16 |

https://doi.org/10.1371/journal.pone.0242110.t007

**Table 8. PSNR values of different schemes with different percentages of data loss.**

| Method | Data loss (%) | | | | |
|---|---|---|---|---|---|
| | 1/32 | 1/16 | 1/8 | 1/4 | 1/2 |
| Ref. [32] | 20.76 | 18.51 | 15.93 | 11.15 | 8.72 |
| Ref. [33] | 8.615 | 8.568 | 8.554 | 8.550 | 8.548 |
| Ref. [34] | 24.37 | 20.63 | 17.64 | 14.61 | 11.61 |
| Proposed | 41.64 | 39.28 | 35.84 | 33.12 | 30.07 |

https://doi.org/10.1371/journal.pone.0242110.t008

**Table 9. Comparison of encryption times (seconds).**

| Image size | Ref [19] | Ref [26] | Ref [31] | Proposed |
|---|---|---|---|---|
| 128×128 | 1.93 | 1.68 | 1.90 | 1.28 |
| 256×256 | 7.72 | 6.72 | 7.59 | 5.14 |
| 512×512 | 31.58 | 26.88 | 30.35 | 20.56 |

https://doi.org/10.1371/journal.pone.0242110.t009

### 4.9 Encryption time analysis

The results of the comparison are shown in Table 9. As shown in Table 9, the proposed method requires the least encryption time compared with the other algorithms. Thus, our proposed method has better performance than other schemes.

## 5 Conclusion

In this paper, a novel image encryption scheme is proposed based on a 5D hyperchaotic system. First, chaotic sequences are produced by a 5D hyperchaotic system based on initial secret keys. Then, the chaotic sequences are preprocessed to obtain new chaotic sequences. They are modified so that they can be used in confusing and diffusing the image. A cycle shift is executed to improve the security of the cryptosystem. The experimental results and theoretical analysis demonstrate that the method has a large key space and resists differential attacks, brute-force attacks, statistical attacks, clipping attacks and noise attacks. Therefore, it is a high-security method that can be used in practical applications.

## Supporting information

**S1 Material.**
(RAR)

## Author Contributions

**Visualization:** Dejian Fang.

**Writing – original draft:** Shuliang Sun.

## References

1. Zhang YQ, Wang XY. A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice. Inform. Sciences, 2014, 273: 329–351.
2. Wang XY, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using DNA sequence operations. Opt. Laser. Eng., 2015, 73:53–61.
3. Wang XY, Teng L, Qin X. A novel colour image encryption algorithm based on chaos. Signal Process., 2012, 92(4):1101–1108.
4. Gao HJ, Zhang YS, Liang SY, Li DQ. A new chaotic algorithm for image encryption. Chaos Soliton. Fract., 2006, 29(2):393–399.
5. Wang XY, Zhang HL. A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt. Commun.,2015, 342:51–60.
6. Sun SL. Chaotic image encryption scheme using two-by-two deoxyribonucleic Acid complementary rules. Opt. Eng., 2017, 56(11):116117.
7. Liu HJ, Wang XY. Color image encryption based on one-time keys and robust chaotic maps. Comput. Math. Appl., 2010, 59(10):3320–3327.
8. Liu HJ, Wang XY, Kadir A. Image encryption using DNA complementary rule and chaotic maps. Appl. Soft Comput., 2012, 12(5):1457–1466.

9. Wang XY, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dynam., 2010, 62(3):615–621.
10. Wang XY, Feng L, Zhao HY. Fast image encryption algorithm based on parallel computing system. Inform. Sciences, 2019, 486:340–358.
11. Wang XY, Gao S. Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. Inform. Sciences, 2020, 507:16–36.
12. Wang XY, Gao S. Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. Inform. Sciences, 2020, 539: 195–214.
13. Zhang YQ, Wang XY. A new image encryption algorithm based on non-adjacent coupled map lattices. Appl. Soft Comput., 2015, 26: 10–20.
14. Wang XY, He GX. Cryptanalysis on a novel image encryption method based on total shuffling scheme. Opt. Commun., 2011, 284(24):5804–5807.
15. Wang XY, Liu LT, Zhang YQ. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt. Laser. Eng., 2015, 66:10–18.
16. Lima J B, Lima E A O, Madeiro F. Image encryption based on the finite field cosine transform. Signal Process., 2013, 28(10):1537–1547.
17. Liu HJ, Wang XY. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt. Commun., 2011, 284(16–17): 3895–3903.
18. Ye GD, Wong K. W. An image encryption scheme based on time-delay and hyperchaotic system. Nonlinear Dynam.,2013, 71(1–2):259–267.
19. Sun SL. A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling. IEEE Photonics J., 2018, 10(2):7201714.
20. Chen JX, Zhu ZL, Fu C, Yu H, Zhang LB. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Commun. Nonlinear Sci., 2015, 20(3): 846–860.
21. Luo YL, Zhou RL, Liu JX, Cao Y, Ding XM. A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. Nonlinear Dynam., 2018, 93(3): 1165–1181.
22. Liu HJ, Kadir A. Asymmetric color image encryption scheme using 2D discrete-time map. Signal Process., 2015, 113:104–112.
23. Sun SL, Guo YN, Wu RK. A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping. IEEE Access, 2019, 7: 28539–28547.
24. Sun SL, Guo YN, Wu RK. A novel plaintext-related image encryption algorithm based on stochastic signal insertion and block swapping. IEEE Access, 2019, 7: 123049–123060.
25. Yang QG, Bai ML. A new 5D hyperchaotic system based on modified generalized Lorenz system. Nonlinear Dynam., 2017, 88(1):189–221.
26. Chai XL, Yang K, Gan ZH. A new chaos-based image encryption algorithm with dynamic key selection mechanisms. Multimed. Tools Appl., 2017, 76(7):9907–9927.
27. Li YP, Wang CH, Chen H. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt. Laser. Eng., 2017, 90:238–246.
28. Chai XL, Chen YR, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations. Opt. Laser. Eng., 2017, 88:197–213.
29. Xu L, Gou X, Li Z, Li J. A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Opt. Laser. Eng., 2017, 91:41–52.
30. Rehman A U, Liao XF, Kulsoom A, Abbas S A. Selective encryption for gray images based on chaos and DNA complementary rules. Multimed. Tools Appl., 2015, 74(13):4655–4677.
31. Chai XL, Han DJ, Lu Y, Chen YR, Gan ZH. A novel image encryption algorithm based on the chaotic system and DNA computing. Int. J. Mod. Phys. C, 2017, 28(5):1750069.
32. Hua ZY, Yi S, Zhou YC. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process., 2018, 144:134–144.
33. Hua ZY, Zhou YC. Design of image cipher using block-based scrambling and image filtering. Inform. Sciences, 2017, 396:97–113.
34. Belazi A, Talha M, Kharbech S, Xiang W. Novel medical image encryption scheme based on chaos and DNA encoding. IEEE Access, 2019, 7:36667–36681.