

Article

A Novel Image Encryption Scheme Based on Self-Synchronous Chaotic Stream Cipher and Wavelet Transform

Chunlei Fan  and Qun Ding *

Electrical Engineering College, Heilongjiang University, Harbin 150080, China; 1172053@s.hlju.edu.cn

* Correspondence: 1984008@hlju.edu.cn; Tel.: +86-0451-8660-8504

Received: 21 May 2018; Accepted: 5 June 2018; Published: 6 June 2018



Abstract: In this paper, a novel image encryption scheme is proposed for the secure transmission of image data. A self-synchronous chaotic stream cipher is designed with the purpose of resisting active attack and ensures the limited error propagation of image data. Two-dimensional discrete wavelet transform and Arnold mapping are used to scramble the pixel value of the original image. A four-dimensional hyperchaotic system with four positive Lyapunov exponents serve as the chaotic sequence generator of the self-synchronous stream cipher in order to enhance the security and complexity of the image encryption system. Finally, the simulation experiment results show that this image encryption scheme is both reliable and secure.

Keywords: hyperchaotic system; self-synchronous stream cipher; permutation entropy; image encryption; wavelet transform

1. Introduction

With the rapid development of social networking, cloud computing, and mobile network communication technology, the problem of secure storage and real-time transmission of image data is increasingly important. Encryption and digital watermarking technology play an important role in guaranteeing the security of multimedia data [1]. However, because of the high correlation and redundancy of adjacent pixels of the digital image, some international standard encryption algorithms are not suitable for image encryption, including 3DES (Triple Data Encryption Algorithm), IDEA (International Data Encryption Algorithm), and AES (Advanced Encryption Standard), etc. On the other hand, the chaotic nonlinear dynamic system has some good characteristics, such as positive Lyapunov exponents, ergodicity, sensitivity to initial conditions, topological transitivity, and unpredictability [2–5], and was widely applied in the field of cryptography and secret communication. In recent years, in order to better solve the security transmission of digital images, some scholars have put forward a series of image security encryption schemes based on the chaotic system and the inherent characteristics of digital images [6–9]. For example, Ping et al. [10] proposed a permutation-substitution image encryption scheme with the Henon map, which can resist a chosen-plaintext attack and known-plaintext attack. Ye et al. [11] put forward an efficient symmetric image encryption algorithm based on an intertwining Logistic map. Haroun [12] came up with a real-time image encryption scheme using a low-complexity discrete 3D dual chaotic cipher.

However, these image encryption schemes generally use low-dimensional chaotic systems or high-dimensional chaotic systems with only one positive Lyapunov exponent such as Logistic, Tent, Henon, and Lorenz, etc. Compared with the high-dimensional hyperchaotic system with more than two positive Lyapunov exponents, the complexity of nonlinear dynamic characteristics of the above chaotic systems are lower. Additionally, because of the influence of the calculation precision and

the quantization method, the chaotic binary sequences generated by the low-dimensional chaotic systems emerge with short periodic phenomena [13,14], which will seriously affect the security of image encryption. Furthermore, the above image encryption schemes usually adopt the synchronous sequence cipher based on the chaotic binary sequences [15,16]. In synchronous stream ciphers, the key stream is independent of plaintext or ciphertext. In the process of communication, the sender and receiver must keep accurate synchronization. If the synchronization mechanism is broken by active attack, the receiver will not be able to decrypt the ciphertext correctly. For instance, if an attacker inserts or removes a certain number of bits ciphertext, it will immediately destroy the synchronization mechanism of the synchronous sequence cipher. Therefore, this encryption method cannot resist active attack [17]. On the basis of the above image encryption problem, we proposed a novel image encryption scheme based on self-synchronous chaotic stream cipher and wavelet transform. Firstly, a two-dimensional discrete wavelet transform is used to convert the original image from the spatial domain to the frequency domain with the purpose of strengthening the difficulty of cracking. Secondly, the pixel value of the image is scrambled by Arnold mapping. Finally, the scrambled image is encrypted by self-synchronous chaotic stream cipher. This algorithm uses a four-dimensional hyperchaotic system with four positive Lyapunov exponents and a self-synchronous stream cipher mechanism. The generation of the key stream of the self-synchronous stream cipher is not independent of the plaintext and ciphertext stream but is related to the seed key and n -bits ciphertext that have been generated before. In the process of ciphertext transmission, the 1-bit ciphertext error will only affect the correct decryption of the n -bits ciphertext in the back. The decryption process returns to normal after this time. Therefore, this scheme cannot only resist active attack but also ensures the limited error propagation of image data. The experimental results show that the encryption scheme has good security.

The rest of this paper is organized as follows: Section 2 introduces a four-dimensional hyperchaotic system and the design scheme of the self-synchronous chaotic stream cipher. Furthermore, the performance of the discrete chaotic sequence was analyzed by multi-scale permutation entropy and NIST-800-22 test. In Section 3, a novel image encryption scheme is proposed and a detailed security analysis is carried out with histogram and information entropy analyses, etc. Section 4 summarizes the conclusion of this paper.

2. Design and Implementation of Self-Synchronous Chaotic Stream Cipher

2.1. The Description of Four-Dimensional Discrete Chaotic System

In this section, a four-dimensional chaotic system is constructed through the Chen–Lai algorithm [18,19]. The discrete dynamic equations of the system can be expressed as the follows:

$$\begin{pmatrix} x_1(k+1) \\ x_2(k+1) \\ x_3(k+1) \\ x_4(k+1) \end{pmatrix} = A \begin{pmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \\ x_4(k) \end{pmatrix} + (\|A\|_2 + e^c) \begin{pmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \\ x_4(k) \end{pmatrix} \pmod{1} \quad (1)$$

where $\|\cdot\|_2$ and e represent Euclidean norm and mathematical constant, respectively. The mod is the module operations, and c is control parameter. Furthermore, matrix A is given as follows:

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ A_{21} & A_{22} & A_{23} & A_{24} \\ A_{31} & A_{32} & A_{33} & A_{34} \\ A_{41} & A_{42} & A_{43} & A_{44} \end{pmatrix} = \begin{pmatrix} 0.7 & 0.4 & 0.1 & 0.2 \\ 0.2 & -0.5 & 0.1 & 0 \\ 0 & -1/3 & 0.1 & 0 \\ 0 & -1/4 & 0.3 & 0.6 \end{pmatrix}. \quad (2)$$

When $c = 3$, the Lyapunov exponents of the system are given by $LE_1 = 3.0128$, $LE_2 = 3.0454$, $LE_3 = 3.0717$, and $LE_4 = 3.0799$. The number of positive Lyapunov exponents are more than two. Thus,

the system is a four-dimensional hyperchaotic system. The chaotic time series of the four-dimensional hyperchaotic system are shown in Figure 1.

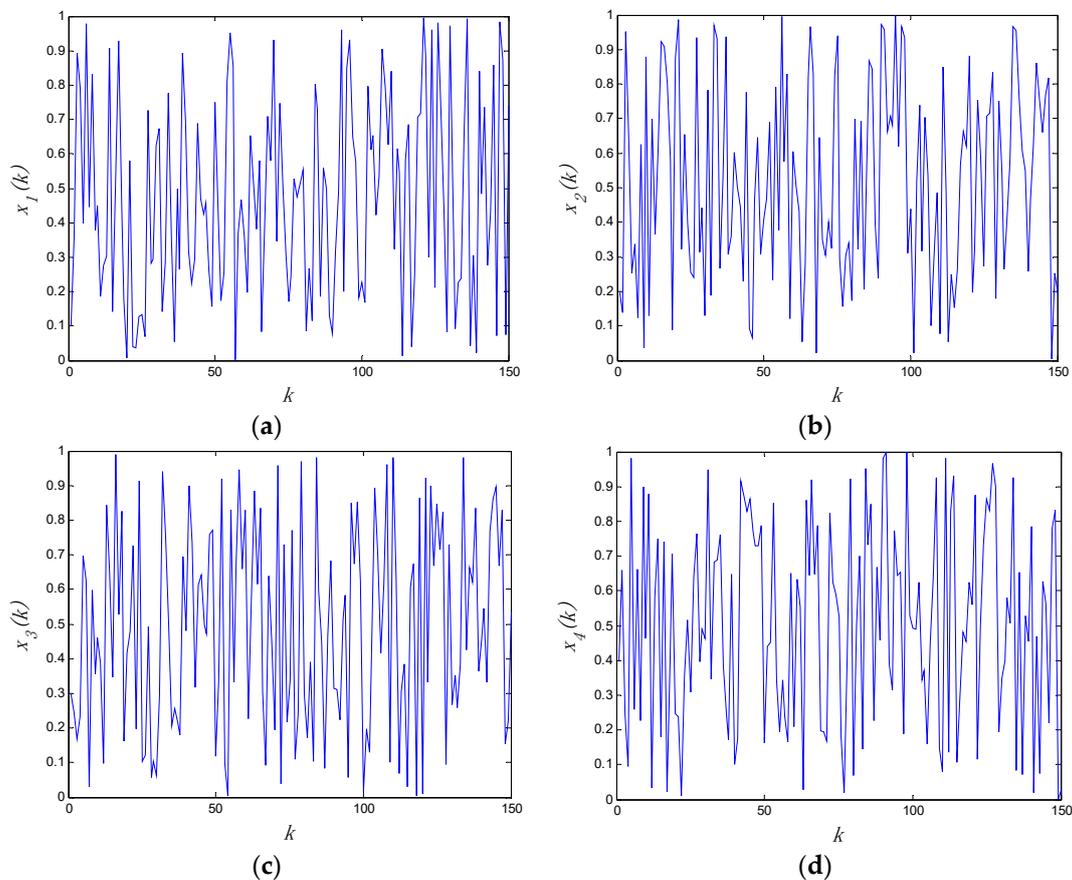


Figure 1. The chaotic time series of the four-dimensional hyperchaotic system with: (a) $x_1(k)$; (b) $x_2(k)$; (c) $x_3(k)$; (d) $x_4(k)$.

2.2. Quantization and Performance Analysis of Discrete Chaotic Sequences

2.2.1. Binary Quantization Method

For the above chaotic system, $x_j(k) \in (0, 1)$ with $j = 1, 2, 3, 4$. In this paper, we adopt the binary quantization method to quantize discrete chaotic real value sequences. The corresponding quantization method is defined as follows:

$$Q_j(k) = \begin{cases} 0 & x_j(k) < t_d \\ 1 & x_j(k) \geq t_d \end{cases} \quad j = 1, 2, 3, 4 \quad (3)$$

where $Q_j(k)$ is the quantized chaotic binary sequence, and t_d represents the quantization threshold with $t_d = 0.5$.

2.2.2. Multi-Scale Permutation Entropy Analysis

Multi-scale permutation entropy (MPE) [20,21] has the advantages of high robustness and fast computational speed. It is widely applied in the measurement of binary sequence complexity and nonlinear system analysis. In this section, we perform a multi-scale permutation entropy analysis for the above chaotic binary sequence. The parameters of MPE have embedding dimension m , delay factor τ , and scale factor s . For the choice of the parameter values of the multi-scale permutation

entropy with the purpose of calculating the complexity of chaotic binary sequences, Sun et al. [22] and Xu et al. [23] give the recommended parameter range in order to obtain more accurate entropy values. On the basis of the theoretical research of the above references, in this experiment, we set $m = 3$, $\tau = 2$, and $s \in [3, 7]$, respectively. The experimental results are shown in Table 1. As can be seen from Table 1, all MPE values of chaotic binary sequences are more than 0.9 and display good sequence complexity.

Table 1. The multi-scale permutation entropy (MPE) value of chaotic binary sequences with $Q_1(k)$, $Q_2(k)$, $Q_3(k)$, and $Q_4(k)$.

Scale Factor S	$Q_1(k)$	$Q_2(k)$	$Q_3(k)$	$Q_4(k)$
3	0.9201	0.9260	0.9177	0.9132
4	0.9366	0.9382	0.9449	0.9410
5	0.9548	0.9488	0.9567	0.9377
6	0.9590	0.9572	0.9585	0.9526
7	0.9552	0.9533	0.9704	0.9553

2.2.3. NIST-800-22 Test

NIST-800-22 is a statistical test suite for random and pseudorandom number generators for cryptographic applications. This test standard was enacted by the National Institute of Standards and Technology (NIST). The test statistic is used to calculate a p -value that summarizes the strength of the evidence against the null hypothesis. On the basis of the results of NIST test, we can judge whether or not this chaotic binary sequence is suitable for a cryptographic algorithm. NIST-800-22 is made up of 16 test methods, including the longest run test, cumulative sums, and the linear complexity test, etc. For these tests, each p -value is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of non-randomness assessed by the test. A significance level (α) can be chosen for the tests. If p -value $\geq \alpha$, then the null hypothesis is accepted; i.e., the sequence appears to be random. If p -value $< \alpha$, then the null hypothesis is rejected; i.e., the sequence appears to be non-random. Typically, α is chosen in the range [0.001, 0.01]. Common values of α in cryptography are about 0.01 based on the NIST-800-22 test standard [24]. The experimental results of NIST-800-22 test are shown in Table 2. Table 2 shows that the chaotic binary sequences $Q_1(k)$, $Q_2(k)$, $Q_3(k)$, and $Q_4(k)$ passed all the tests. These sequences show good randomness and meet the requirements of the stream cipher.

Table 2. NIST-800-22 test of chaotic binary sequences.

Test Item	$Q_1(k)$	$Q_2(k)$	$Q_3(k)$	$Q_4(k)$	Result
	p -Value	p -Value	p -Value	p -Value	
Approximate Entropy	0.026853	0.013829	0.068205	0.034937	Success
Block Frequency	0.058378	0.870831	0.724584	0.297646	Success
Cumulative Sums	0.459642	0.069717	0.963210	0.328997	Success
FFT	0.358795	0.919848	0.081236	0.713570	Success
Frequency	0.435391	0.447255	0.888660	0.193601	Success
Linear Complexity	0.186537	0.203633	0.569565	0.232544	Success
Longest Run	0.359643	0.087189	0.789913	0.250387	Success
Non-Overlapping Template	0.348045	0.680967	0.106169	0.068529	Success
Overlapping Template	0.512834	0.063236	0.020689	0.490518	Success
Random Excursions	0.319514	0.181174	0.524622	0.304589	Success
Random Excursions Variant	0.579380	0.177934	0.108254	0.659874	Success
Rank	0.949536	0.648387	0.862457	0.648387	Success
Runs	0.340097	0.086469	0.041369	0.027231	Success
Serial Test-1	0.407933	0.213432	0.648688	0.814738	Success
Serial Test-2	0.462490	0.880617	0.584615	0.512974	Success
Maurer's Universal	0.026152	0.538143	0.142680	0.600293	Success

2.3. The Design of Self-Synchronous Chaotic Stream Cipher

The self-synchronous stream cipher is also known as the asynchronous stream cipher. The generation of the key stream of self-synchronous stream cipher is not independent of the plaintext and ciphertext stream but is related to the seed key and some ciphertext that has been generated before.

It has the advantages of limited error propagation, self-synchronous and ciphertext statistical diffusion. In this section, the encryption and decryption block diagram of the self-synchronous stream cipher based on the four-dimensional hyperchaotic system is shown in Figure 2.

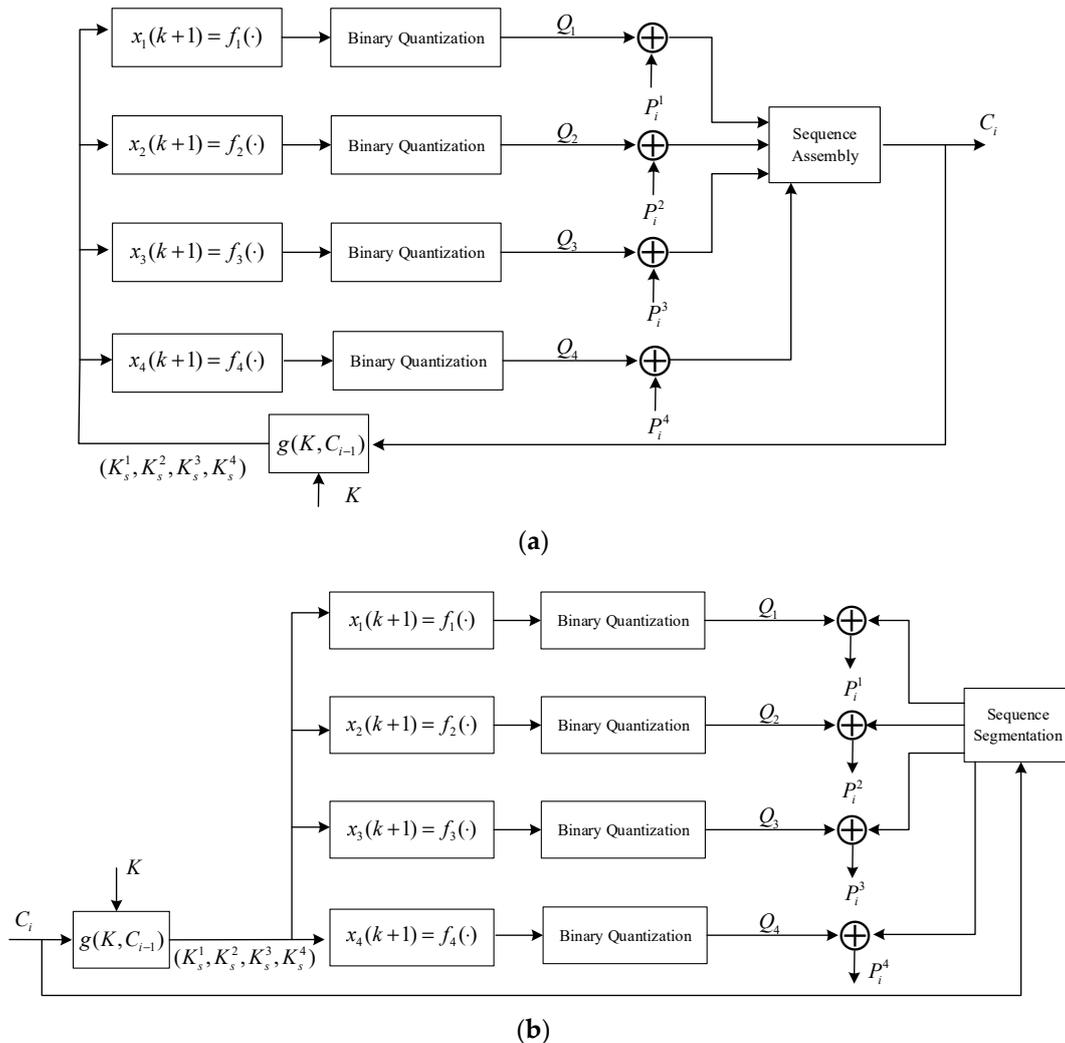


Figure 2. The self-synchronous chaotic stream cipher with: (a) encryption block diagram; (b) decryption block diagram.

Where $K, (K_s^1, K_s^2, K_s^3, K_s^4), \oplus$ and function $g(\cdot)$ represent the seed key, subkey, exclusive OR (XOR) operational character and subkey generation function, respectively. C_{i-1} and C_i are the ciphertext stream generated at two adjacent moments. $Q_1, Q_2, Q_3,$ and Q_4 are the quantized chaotic binary sequence. $P_i^1, P_i^2, P_i^3,$ and P_i^4 are the adjacent plaintext stream with the purpose of parallel encryption. According to Equations (1) and (2), $f_1(\cdot), f_2(\cdot), f_3(\cdot),$ and $f_4(\cdot)$ can be given as Equation (4).

$$\begin{cases} x_1(k+1) = f_1(\cdot) = A_{11}x_1(k) + A_{12}x_2(k) + A_{13}x_3(k) + A_{14}x_4(k) + (\|A\|_2 + e^c)x_1(k) \pmod{1} \\ x_2(k+1) = f_2(\cdot) = A_{21}x_1(k) + A_{22}x_2(k) + A_{23}x_3(k) + A_{24}x_4(k) + (\|A\|_2 + e^c)x_2(k) \pmod{1} \\ x_3(k+1) = f_3(\cdot) = A_{31}x_1(k) + A_{32}x_2(k) + A_{33}x_3(k) + A_{34}x_4(k) + (\|A\|_2 + e^c)x_3(k) \pmod{1} \\ x_4(k+1) = f_4(\cdot) = A_{41}x_1(k) + A_{42}x_2(k) + A_{43}x_3(k) + A_{44}x_4(k) + (\|A\|_2 + e^c)x_4(k) \pmod{1} \end{cases} \quad (4)$$

The encryption process of the self-synchronous chaotic stream cipher can be described as follows:

1. The subkey $(K_s^1, K_s^2, K_s^3, K_s^4)$ is generated by function $g(\cdot)$ and $K_s^j \in (0, 1)$ with $j = 1, 2, 3, 4$. Where K and C_{i-1} are the 0-1 binary sequence with length of 32 bits. The function $g(\cdot)$ is given as follows:

$$\left\{ \begin{array}{l} K = (k_1, k_2, \dots, k_{32}) \\ C_{i-1} = (c_{i-1}^1, c_{i-1}^2, \dots, c_{i-1}^{32}) \\ K_s^1 = g(K, C_{i-1}) = \sum_{v=1}^8 (k_{4v-3} \oplus c_{i-1}^{4v-3})2^{-v} \\ K_s^2 = g(K, C_{i-1}) = \sum_{v=1}^8 (k_{4v-2} \oplus c_{i-1}^{4v-2})2^{-v} \\ K_s^3 = g(K, C_{i-1}) = \sum_{v=1}^8 (k_{4v-1} \oplus c_{i-1}^{4v-1})2^{-v} \\ K_s^4 = g(K, C_{i-1}) = \sum_{v=1}^8 (k_{4v} \oplus c_{i-1}^{4v})2^{-v} \end{array} \right. \quad (5)$$

2. The generated subkey $(K_s^1, K_s^2, K_s^3, K_s^4)$ is used as the state variable $(x_1(k), x_2(k), x_3(k), x_4(k))$ of the four-dimensional hyperchaotic system. The key stream Q_1, Q_2, Q_3 and, Q_4 with length of 8 bits are generated by hyperchaotic Equation (4) and a binary quantization operation with the purpose of parallel encryption.
3. Ciphertext C_i is generated by the Equation (6). At the same time, the C_i will feedback to the function $g(\cdot)$ with the purpose of generating the next round subkey $(K_s^1, K_s^2, K_s^3, K_s^4)$. Where $||$ is sequence assembly operation.

$$\left\{ \begin{array}{l} Q_1 \oplus P_i^1 = c_i^1, c_i^2, \dots, c_i^8 \\ Q_2 \oplus P_i^2 = c_i^9, c_i^{10}, \dots, c_i^{16} \\ Q_3 \oplus P_i^3 = c_i^{17}, c_i^{18}, \dots, c_i^{24} \\ Q_4 \oplus P_i^4 = c_i^{25}, c_i^{26}, \dots, c_i^{32} \\ C_i = (Q_1 \oplus P_i^1) || (Q_2 \oplus P_i^2) || (Q_3 \oplus P_i^3) || (Q_4 \oplus P_i^4) = c_i^1, c_i^2, \dots, c_i^{32} \end{array} \right. \quad (6)$$

The decryption process of the self-synchronous chaotic stream cipher is similar to the encryption process, which is not repeated here.

3. A Novel Image Encryption Scheme Based on Self-Synchronous Chaotic Stream Cipher

3.1. The Description of the Image Encryption Scheme

In this section, a novel image encryption scheme is proposed based on self-synchronous chaotic stream cipher, Arnold mapping, and two-dimensional discrete wavelet transform (DWT). The encryption process of the proposed scheme is shown in Figure 3. Firstly, the spatial domain of the image is transformed into the frequency domain by two-layer DWT. Secondly, Arnold mapping is implemented with the purpose of obtaining good diffusion effectiveness. Finally, on the basis of self-synchronous chaotic stream cipher, the scrambled image is encrypted to ensure its security.

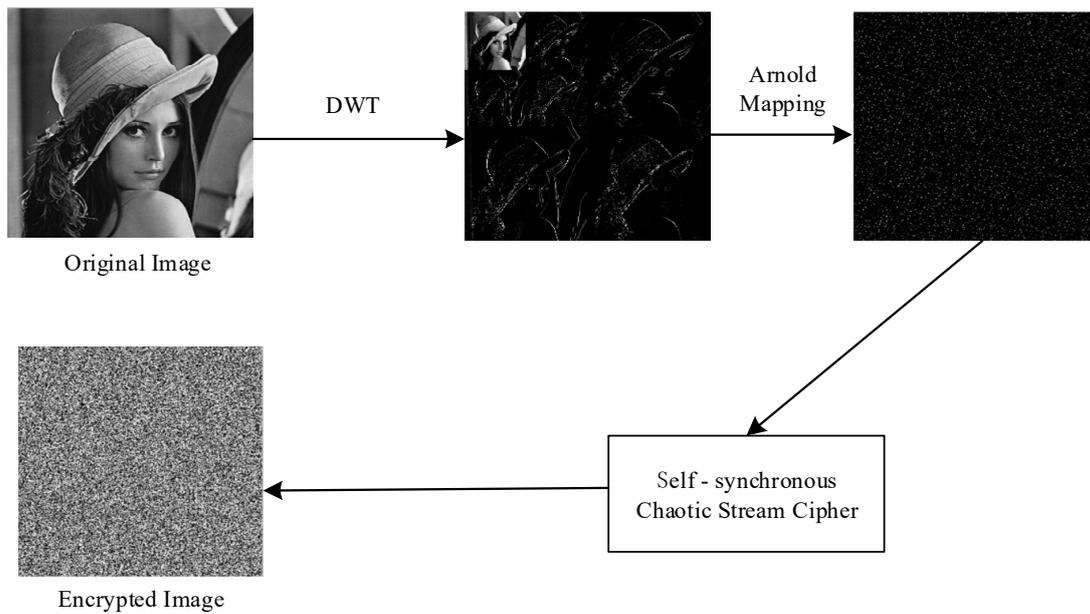


Figure 3. The encryption process of the proposed scheme.

3.1.1. Discrete Wavelet Transform

The DWT plays an important role in image compression and image information processing. The decomposition process of signal S_o by the two-dimensional DWT is shown in Figure 4. A two-dimensional matrix S_o can be decomposed into four groups of coefficients $[cA, cD^{(h)}, cD^{(v)}, cD^{(d)}]$. Where cA , $cD^{(h)}$, $cD^{(v)}$, and $cD^{(d)}$ represent approximate coefficient (low frequency component), horizontal detail coefficient, vertical detail coefficient, and diagonal detail coefficients, respectively. Furthermore, the approximate coefficient cA can continue to be decomposed by the same method. On the basis of the above image encryption scheme, in order to obtain the transformation coefficient, the pixel value of the grayscale image is processed by two-dimensional discrete wavelet transform. Thereafter, the spatial domain of the digital image is transformed into the frequency domain with the purpose of enhancing the pixel scrambling effect.

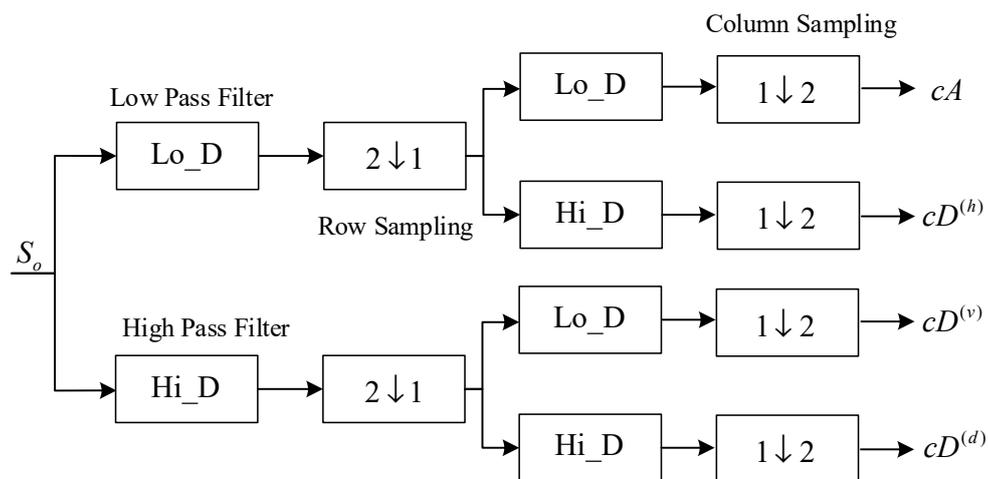


Figure 4. The principle block diagram of the two-dimensional discrete wavelet transform.

3.1.2. Arnold Mapping

Arnold mapping [25], also known as cat mapping, is a chaotic mapping method for repeated folding and stretching transformation in a limited area. It is widely applied to pixel scrambling of images. The mathematical equation of Arnold mapping is given as follows:

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \pmod{M} \quad (7)$$

where (X_n, Y_n) and (X_{n+1}, Y_{n+1}) represent the pixel coordinates of the original image and the pixel coordinates of transformed image, respectively. In addition, $X_n, Y_n, X_{n+1}, Y_{n+1} \in \{0, 1, \dots, N-1\}$, and $a = 1, b = 1$. The variable M is the size of the image.

3.2. Security Analysis of Image Encryption Scheme

In this section, the Lena, fruits, and airplane gray images with a size of 256×256 are encrypted using the above image encryption scheme based on self-synchronous chaotic stream cipher. The security analysis results of image encryption are shown below.

3.2.1. Histogram Analysis

The histogram of the image is an important statistical feature of the image. It can be considered as the gray density function of the image. One of the evaluation criteria of image encryption effect is whether the gray histogram of the ciphertext image has the characteristics of uniform distribution. The results of the grayscale histogram are shown in Figure 5, and the horizontal and vertical coordinates of the gray histogram represent the pixel values and number of pixel values, respectively. As can be seen from the Figure 5g–i, the pixel values of the ciphertext images are so evenly distributed that it is difficult for the attacker to extract the plaintext pixel statistical characteristics from the ciphertext. Therefore, this image encryption scheme can resist statistical attacks well.

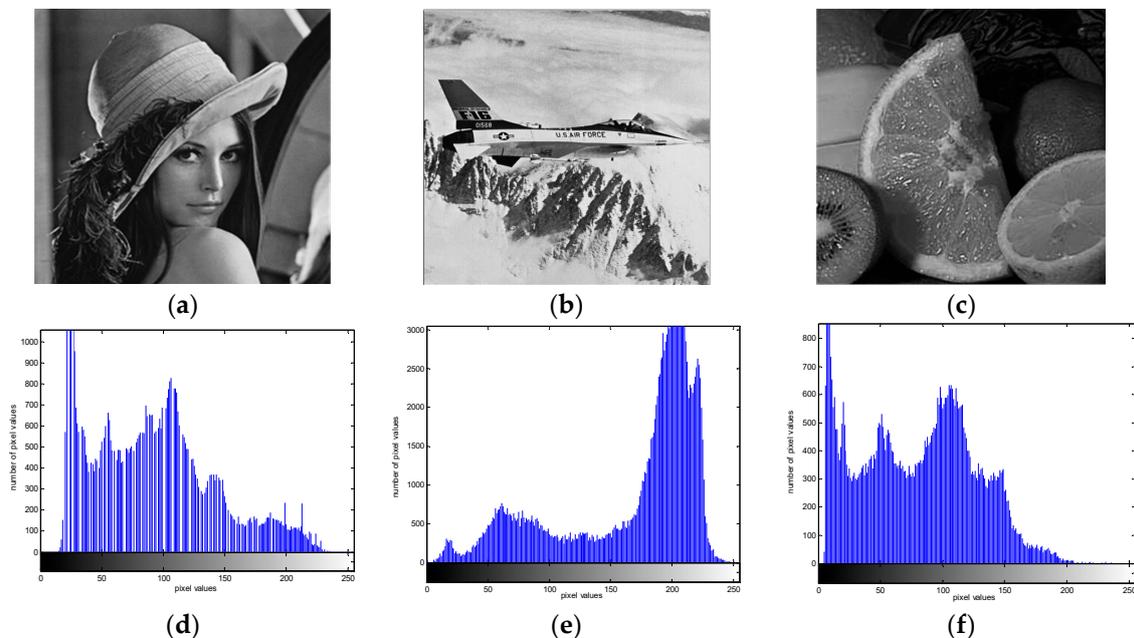


Figure 5. Cont.

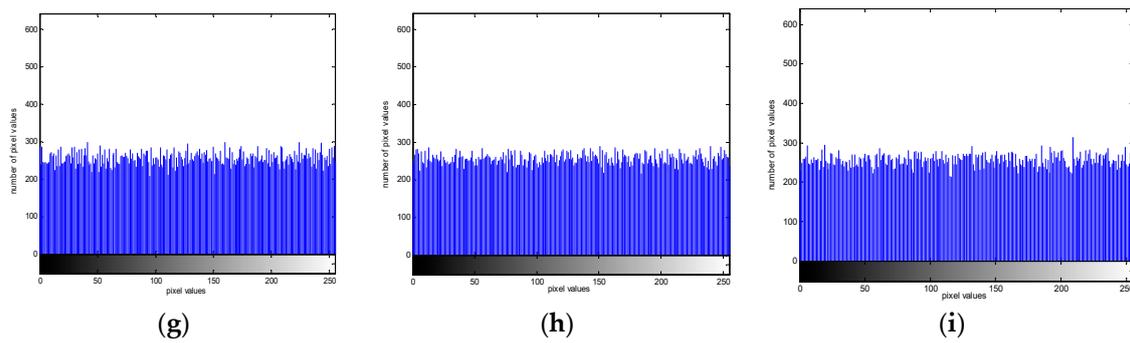


Figure 5. Histogram test with: (a) plain-image of Lena; (b) plain-image of airplane; (c) plain-image of fruits; (d) histogram of plain-image of Lena; (e) histogram of plain-image of airplane; (f) histogram of plain-image of fruits; (g) histogram of encrypted image of Lena; (h) histogram of encrypted image of airplane; (i) histogram of encrypted image of fruits.

3.2.2. Correlation Analysis of Adjacent Pixels

Correlation analysis refers to the analysis of two variables with correlation so as to measure the correlation degree of two variables. The correlation of adjacent pixels can reflect the scrambling effect of image pixels. The mathematical equation for the correlation of adjacent pixels is shown as follows [26]:

$$E(x) = \frac{1}{N} \sum_{k=1}^N x_k \quad (8)$$

$$D(x) = \frac{1}{N} \sum_{k=1}^N (x_k - E(x))^2 \quad (9)$$

$$\text{cov}(x, y) = \frac{1}{N} \sum_{k=1}^N (x_k - E(x))(y_k - E(y)) \quad (10)$$

$$\rho_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (11)$$

where x_k and y_k represent the grey values of two adjacent pixels, and N is the number of randomly selected adjacent pixels from the original or encrypted image. The ρ_{xy} , $E(x)$, $D(x)$ and $\text{cov}(x, y)$ represent the correlation coefficient, mean value, variance, and covariance, respectively.

For the correlation analysis experiment, we randomly selected 2000 pairs of adjacent pixels in horizontal, vertical, and diagonal directions from the plain and encrypted images of Lena. The experimental results are shown in Figure 6. Where (i, j) represents the position coordinates of this pixel in the image. As can be seen from the figure, the correlation of cipher-images is much lower than that of plain-images. Furthermore, Table 3 shows the correlation analysis of the adjacent pixels with the Lena, airplane, and fruits image. Obviously, the correlation coefficient of the plain-image is close to 1. On the contrary, the correlation coefficient of the cipher-image is close to 0, which indicates a good performance.

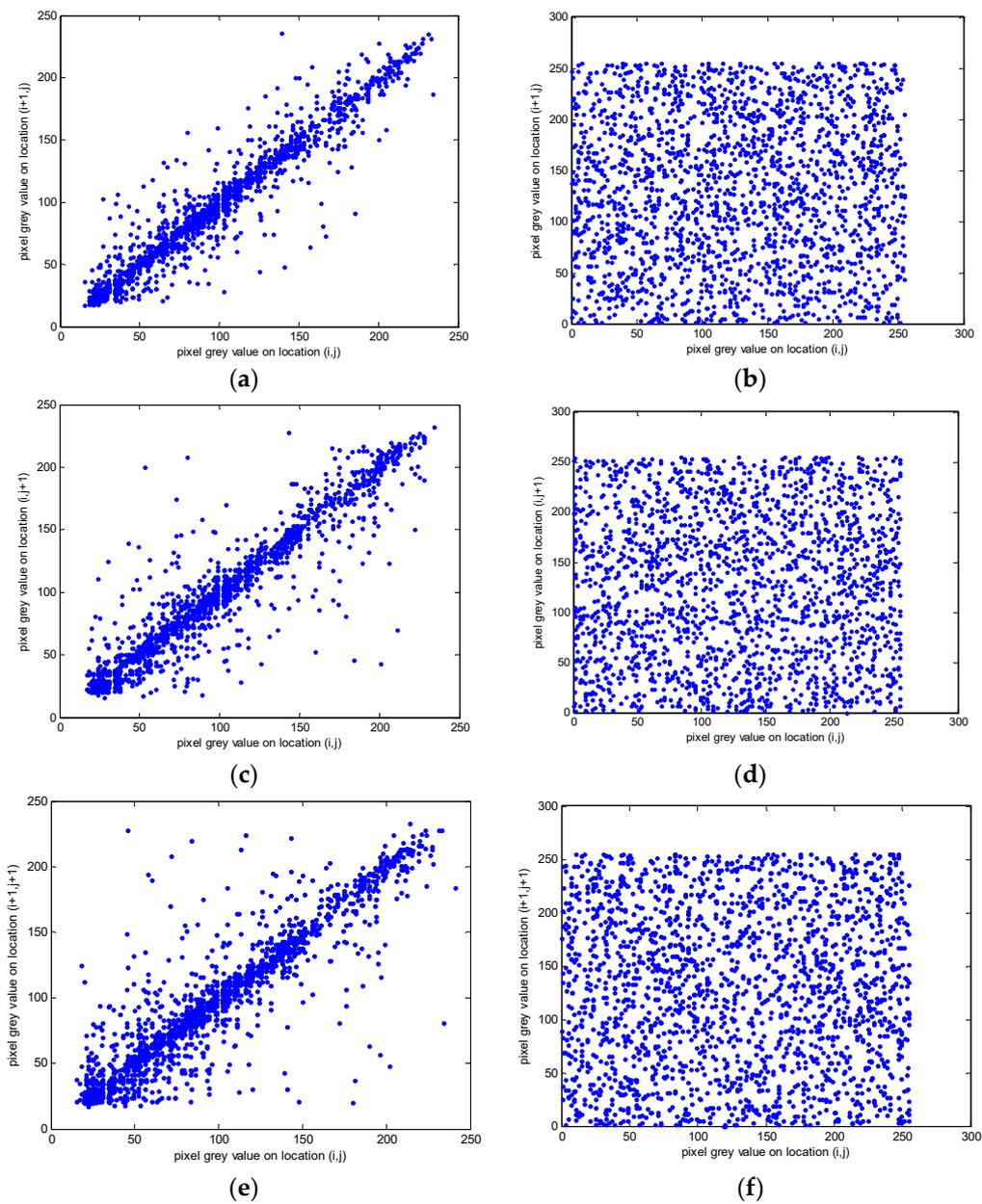


Figure 6. The correlation plots of two adjacent pixels for the plain and encrypted images of Lena with: (a) horizontal correlation of plain-image of Lena; (b) horizontal correlation of cipher-image of Lena; (c) vertical correlation of plain-image of Lena; (d) vertical correlation of cipher-image of Lena; (e) diagonal correlation of plain-image of Lena; (f) diagonal correlation of cipher-image of Lena.

Table 3. Correlation analysis of adjacent pixels for the Lena, airplane, and fruits images.

Direction	Horizontal	Vertical	Diagonal
Plain-image of Lena	0.9577	0.9440	0.9126
Cipher-image of Lena	−0.0082	0.0027	0.0030
Plain-image of Airplane	0.9147	0.9225	0.9109
Cipher-image of Airplane	0.0334	−0.0285	−0.0073
Plain-image of Fruits	0.9540	0.9497	0.9459
Cipher-image of Fruits	−0.0273	−0.0176	−0.0026

3.2.3. Peak Signal-To-Noise Ratio (PSNR) Analysis

The peak signal-to-noise ratio is an objective criterion for evaluating images, and its mathematical equation is given as follows:

$$\text{PSNR} = 10 \log_{10}(L^2/\text{MSE}) \quad (12)$$

$$\text{MSE} = \frac{1}{M^2} \sum_{i=1}^M \sum_{j=1}^M (I'(i,j) - I(i,j))^2 \quad (13)$$

where $M \times M$ is the size of image, $I'(i,j)$, and $I(i,j)$ represent the pixel value of encrypted and original images, respectively. MSE is mean squared error, and L is the range of gray values in the image. Generally speaking, the better the encryption effect is, the smaller the PSNR of the image becomes. The results of the PSNR test is shown in Table 4. For the test result of our scheme, it is the average PSNR of the Lena, airplane, and fruits images. Similarly, for the image encryption method of Yin et al. [27] and Zhu [28], this PSNR represents the average value of multiple images. As can be seen from the table, our scheme has a smaller PSNR value, which shows a good encryption effect.

Table 4. Peak signal-to-noise ratio (PSNR) test with different methods.

Methods	PSNR Value
Our scheme	8.1543
Yin et al. [27]	8.4100
Zhu [28]	9.2322

3.2.4. Information Entropy Analysis

Information entropy can measure the distribution of gray values in images. The more random the gray value distribution, the greater the information entropy of the image. According to the information theory of Shannon, the information entropy can be defined as follows:

$$H(s) = - \sum_{i=0}^{2^n-1} P(s_i) \log_2(P(s_i)) \quad (14)$$

where $P(s_i)$ represents the probability of symbol s_i , n is the number of bits required to store each pixel value, 2^n is the total states of the information source s . When $n = 8$, the theoretical value of information entropy is 8. The information entropy test was performed for the encrypted images of Lena, airplane, and fruits. Table 5 shows the experimental results of the entropy test. The test result of our scheme is the average entropy value of the Lena, airplane, and fruits images. For the scheme of Liu et al. [29], Liu et al. [30], and Niyat [31], these entropy values represent the average value of multiple images. As can be seen from the table, the entropy value of encrypted image of our scheme is closer to the theoretical value 8. Therefore, this scheme can effectively resist the information entropy attack.

Table 5. Information entropy test with different methods.

Methods	Entropy Value
Our scheme	7.9971
Liu et al. [29]	7.9914
Liu et al. [30]	7.9851
Niyat et al. [31]	7.9877

4. Discussion

In this paper, we proposed a novel image encryption scheme with the purpose of ensuring secure transmission of image data. A four-dimensional hyperchaotic system is constructed to act as the chaotic

sequence generator. Moreover, the performance of chaotic binary sequences is analyzed by multi-scale permutation entropy and the NIST-800-22 test. The test results show that the binary sequence has good randomness and security. On the basis of the chaotic sequence generator, a self-synchronous stream cipher is designed to encrypt the image data. The generation of the key stream of the chaotic stream cipher is related to the seed key and a certain number of bits ciphertext that has been generated previously. It has the advantages of limited error propagation, self-synchronous and ciphertext statistical diffusion, which can satisfy the security and stability of image encryption system. Finally, a novel image encryption scheme is designed based on the self-synchronous stream cipher. Arnold mapping and wavelet transform are used to obtain a good scrambling effect for the digital image. Some simulation results show that the proposed scheme is both reliable and secure.

Author Contributions: C.F. conceived and wrote the paper, which devoted to the simulation experiments. Q.D. gave some theoretical guidance. All authors have read and approved the final manuscript.

Acknowledgments: This work was supported by Natural Science Foundation of China (No. 61471158) and “modern sensing technology” innovation team project of Heilongjiang province (No. 2012TD007).

Conflicts of Interest: The authors declare no conflict of interest.

References

- Asikuzzaman, M.; Pickering, M.R. An overview of digital video watermarking. *IEEE Trans. Circuit Syst. Video Technol.* **2017**, *27*, 1–23. [[CrossRef](#)]
- Kengne, J. Coexistence of chaos with hyperchaos, period-3 doubling bifurcation, and transient chaos in the hyperchaotic oscillator with gyrators. *Int. J. Bifurc. Chaos* **2015**, *25*, 1550052. [[CrossRef](#)]
- Mahmoud, E.E.; Abood, F.S. A new nonlinear chaotic complex model and its complex antilag synchronization. *Complexity* **2017**, *25*, 3848953. [[CrossRef](#)]
- Wang, Q.X.; Yu, S.M.; Li, C.Q.; Lu, J.H.; Fang, X.L.; Guyeux, C.; Bahi, J.M. Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems. *IEEE Trans. Circuit Syst. I* **2016**, *63*, 401–412. [[CrossRef](#)]
- Yang, Q.G.; Chen, G.R. A chaotic system with one saddle and two stable node-foci. *Int. J. Bifurc. Chaos* **2008**, *18*, 1393–1414. [[CrossRef](#)]
- Li, C.H.; Luo, G.C.; Qin, K.; Li, C.B. An image encryption scheme based on chaotic tent map. *Nonlinear Dyn.* **2017**, *87*, 127–133. [[CrossRef](#)]
- Cao, L.C.; Luo, Y.L.; Qiu, S.H.; Liu, J.X. A perturbation method to the tent map based on Lyapunov exponent and its application. *Chin. Phys. B* **2015**, *24*, 326–337. [[CrossRef](#)]
- Usama, M.; Khan, M.K.; Alghathbar, K.; Lee, C. Chaos-based secure satellite imagery cryptosystem. *Comput. Math. Appl.* **2010**, *60*, 326–337. [[CrossRef](#)]
- Zheng, Y.F.; Jin, J.X. A novel image encryption scheme based on Henon map and compound spatiotemporal chaos. *Multimed. Tools Appl.* **2015**, *74*, 7803–7820. [[CrossRef](#)]
- Ping, P.; Xu, F.; Mao, Y.C.; Wang, Z.J. Designing permutation-substitution image encryption networks with Henon map. *Neurocomputing* **2018**, *283*, 53–63. [[CrossRef](#)]
- Ye, G.D.; Huang, X.L. An efficient symmetric image encryption algorithm based on an intertwining logistic map. *Neurocomputing* **2017**, *251*, 45–53. [[CrossRef](#)]
- Haroun, M.F.; Gulliver, T.A. Real-time image encryption using a low-complexity discrete 3D dual chaotic cipher. *Nonlinear Dyn.* **2015**, *82*, 1523–1535. [[CrossRef](#)]
- Persohn, K.J.; Pavinelli, R.J. Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation. *Chaos Soliton Fract.* **2012**, *45*, 238–245. [[CrossRef](#)]
- Zheng, Y.B.; Song, Y.; Du, B.X.; Pan, J.; Ding, Q. A novel detection of periodic phenomena of binary chaotic sequences. *Acta. Phys. Sin. Chin. Ed.* **2012**, *61*, 230501.
- Khelifi, F. On the security of a stream cipher in reversible data hiding schemes operating in the encrypted domain. *Signal Process.* **2018**, *143*, 336–345. [[CrossRef](#)]
- Ullagaddi, V.; Hassan, F.; Devabhaktuni, V. Symmetric synchronous stream encryption using images. *Signal Image Video Process.* **2015**, *9*, 1–8. [[CrossRef](#)]

17. Bucerzan, D.; Craciun, M.; Chis, V.; Ratiu, C. Stream ciphers analysis methods. *Int. J. Comput. Commun.* **2010**, *5*, 483–489. [[CrossRef](#)]
18. Chen, G.R.; Lai, D.J. Making a dynamical system chaotic: Feedback control of Lyapunov exponents for discrete-time dynamical systems. *IEEE Trans. Circuit Syst. I Fundam. Theory Appl.* **2002**, *44*, 250–253. [[CrossRef](#)]
19. Chen, G.R.; Lai, D.J. Feedback control of lyapunov exponents for discrete-time dynamical systems. *Int. J. Bifurc. Chaos* **1996**, *6*, 1341–1349. [[CrossRef](#)]
20. Zhang, X.Y.; Liang, Y.T.; Zhou, J.Z.; Zang, Y. A novel bearing fault diagnosis model integrated permutation entropy, ensemble empirical mode decomposition and optimized SVM. *Measurement* **2015**, *69*, 164–179. [[CrossRef](#)]
21. Bandt, C.; Pompe, B. Permutation entropy: A natural complexity measure for time series. *Phys. Rev. Lett.* **2002**, *88*, 174102. [[CrossRef](#)] [[PubMed](#)]
22. Sun, K.H.; He, S.B.; Yin, L.Z.; Duo, L.K. Application of FuzzyEn algorithm to the analysis of complexity of chaotic sequence. *Acta Phys. Sin. Chin. Ed.* **2012**, *61*, 130507.
23. Xu, W.; Ding, Q.; Zhang, X.G. Improving the complexity of chaotic sequence based on the PCA algorithm. *J. Appl. Anal. Comput.* **2015**, *5*, 262–272.
24. Rukhin, A.; Soto, J.; Nechvatal, J.; Miles, S.; Barker, E. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *Appl. Phys. Lett.* **2015**, *22*, 1645–1776.
25. Soleymani, A.; Nordin, M.J.; Sundararajan, E. A chaotic cryptosystem for images based on Henon and Arnold cat map. *Sci. World J.* **2014**, *2014*, 536930. [[CrossRef](#)] [[PubMed](#)]
26. Li, T.Y.; Yang, M.G.; Wu, J.; Jing, X. A novel image encryption algorithm based on a fractional-order hyperchaotic system and DNA computing. *Complexity* **2017**, *2017*, 9010251. [[CrossRef](#)]
27. Yin, Q.; Wang, C.H. A new chaotic image encryption scheme using breadth-first search and dynamic diffusion. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850047. [[CrossRef](#)]
28. Zhu, C.X. A novel image encryption scheme based on improved hyperchaotic sequences. *Opt. Commun.* **2012**, *285*, 29–37. [[CrossRef](#)]
29. Liu, H.J.; Kadir, A.; Sun, X.B. Chaos-based fast colour image encryption scheme with true random number keys from environmental noise. *IET Image Process.* **2017**, *11*, 324–332. [[CrossRef](#)]
30. Liu, H.J.; Wang, X.Y. Color image encryption based on one-time keys and robust chaotic maps. *Comput. Math. Appl.* **2010**, *59*, 3320–3327. [[CrossRef](#)]
31. Niyat, A.Y.; Moattar, M.H.; Torshiz, M.N. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt. Laser Eng.* **2017**, *90*, 225–237. [[CrossRef](#)]



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).