

Article

The Establishment and Dynamic Properties of a New 4D Hyperchaotic System with Its Application and Statistical Tests in Gray Images

Lina Ding ^{1,2} and Qun Ding ^{1,*}

- ¹ Electronic Engineering College, Heilongjiang University, Harbin 150080, China; 1141738@s.hlju.edu.cn
- ² Electrical Engineering College, Suihua University, Suihua 152061, China
- * Correspondence: 1984008@hlju.edu.cn; Tel.: +86-0451-8660-8504

Received: 22 January 2020; Accepted: 6 March 2020; Published: 10 March 2020



Abstract: In this paper, a new 4D hyperchaotic system is generated. The dynamic properties of attractor phase space, local stability, poincare section, periodic attractor, quasi-periodic attractor, chaotic attractor, bifurcation diagram, and Lyapunov index are analyzed. The hyperchaotic system is normalized and binary serialized, and the binary hyperchaotic stream generated by the system is statistically tested and entropy analyzed. Finally, the hyperchaotic binary stream is applied to the gray image encryption. The histogram, correlation coefficient, entropy test, and security analysis show that the hyperchaotic system has good random characteristics and can be applied to the gray image encryption.

Keywords: hyperchaotic system; image encryption; entropy test; statistical tests

1. Introduction

Since Lorenz [1] discovered the first three-dimensional chaos model, chaos theory has grown with the development of computer science. Chaos is an unpredictable and random motion in deterministic dynamical systems due to its sensitivity to initial values. The certainty of a dynamic system is a concept defined in mathematics, which means that the state of the system at any time can be determined by the initial state of the system. Although the motion state of the deterministic dynamic system at any time can be calculated according to the initial state and motion law, the measurement of the initial state and data cannot be completely accurate. Even a slight difference will lead to a very large error in the predicted results, to an unpredictable degree. In recent years, as chaotic systems have many advantages in encryption, such as ergodicity, unpredictability, pseudo-randomicity, and high sensitivity to parameters and initial values [2], image encryption based on chaos has become a research hotspot. Aside from image encryption based on chaotic systems, there are many representative methods such as: based on one-time keys, bit-level permutation, DNA rule, matrix, and semi-tensor product theory [3,4].

At present, research on 1D chaos, such as Logistic mapping [5–7]; 2D chaos, such as Henon mapping [8–10]; and 3D chaos, such as Rossler chaotic attractor [11–13], Chua [14–16], and Chen [17–19], have been very extensive and mature. With the development of chaos theory, many people began to study high-dimensional chaotic attractors, such as 4D chaotic attractor subsystems [20–23], 5D chaotic attractor subsystems [24–27], and 6D chaotic attractor subsystems [28]. In recent years, fractional-order chaotic systems [29–31], hidden attractors [32–34], and chaotic systems with co-existing attractors [35,36] have also been extensively studied. In ordinary three-dimensional chaotic attractors, linear or nonlinear state feedback controllers can generate different kinds of four-dimensional chaotic systems. The 4D hyperchaotic system has better computational complexity and two or more positive Lyapunov exponents [37,38].



Recently, many scholars have generated many new chaotic systems on the basis of studying the Lorenz chaotic system, which are collectively referred to as Lorenz type hyperchaotic systems [39,40]. These new systems are applied to many aspects, such as chaotic synchronization [41], image encryption [8,12,13,19], stream cryptography [42,43], and so on.

The chaos-based image encryption systems are usually applied to generate chaotic stream ciphers for exchanging the positions or values of the pixels in the original images. A 2D chaotic Arnold cat map was used to generate a 3D cat map, which then was used in image encryption [44]. The results show that the scheme is fast and safe. The authors of [45] applied Henon mapping to the image encryption scheme, and proved that the encryption method could resist selective plaintext attack, etc. The authors of [46] proposed an image encryption scheme based on Logistic mapping, and the authors of [47] proposed an image encryption scheme based on the 3D chaotic system. The above image encryption methods using chaotic systems are based on low-dimensional chaotic systems with at most one positive Lyapunov exponent, which have many advantages, such as simple format, few control parameters, and ease of implementation. However, low-dimensional chaotic systems are vulnerable to attack. If low-dimensional chaotic systems are changed into high-dimensional chaotic systems, the encryption will be more effective. Lyapunov exponent (LE) is an effective method to measure chaotic systems. If a chaotic system has two or more positive LEs, it can be called a hyperchaotic system, which usually has a larger key space and much higher security in encryption schemes [37,38]. As the chaotic systems with four dimensions or more have two or more Lyapunov exponents and better dynamic characteristics, the application to image encryption will have better practical effects [37,38]. The authors of [48] presented a novel approach that uses a hyperchaotic system, Pixel-level, and DNA-level diffusion. The authors of [49] proposed a new image encryption method based on matrix semi-tensor product theory and hyperchaotic Lorenz. The research above shows that the application of hyperchaotic system encryption has become an important trend.

The main contributions of this paper are shown as follows: (1) A new 4D hyperchaotic system is generated, and the dynamic properties of the attractor such as phase space, local stability, poincare section, periodic attractor, quasi-periodic attractor, chaotic attractor, bifurcation diagram, and Lyapunov index are analyzed; (2) Then the new hyperchaotic system is normalized and binary serialized, and the binary hyperchaotic stream generated by the system is statistically tested and entropy analyzed; (3) The hyperchaotic binary stream is applied to the gray image encryption; (4) The histogram, correlation coefficient, entropy test, and security analysis show that the hyperchaotic system has good random characteristics and can be applied to the gray image encryption.

The main advantages of this paper are shown as follows: (1) A new 4D hyperchaotic system based on Lorenz is proposed and analyzed; (2) The hyperchaotic system with two positive LEs is much more random, which is then used to generate sequences for the encryption operations; (3) The new hyperchaotic system in this paper is obtained by adding a new variable, w, and a feedback controller, $-dx^3$, to the classical Lorenz chaotic attractor system. In this way, an equilibrium point curve exists in the system which is a new phenomenon in the system.

In this paper, a new 4D hyperchaotic system is proposed by studying Lorenz-type hyperchaotic system, and the corresponding dynamic properties, such as Lyapunov exponent, phase space diagram, poincare section diagram, and local stability are studied. The method of normalization and binarization is applied to the encryption of gray image. Finally, the entropy test and security analysis of image encryption are carried out.

The rest of this paper is organized as follows: Section 2 introduces a new 4D hyperchaotic system based on Lorenz system with two positive LEs. In Section 3, analyses of the dynamic properties are done, such as judgment of local stability, Poincare section diagram, periodic attractor, etc. In Section 4, normalization and quantization are done. Furthermore, NIST tests, permutation entropy, and approximate entropy are completed to test the time series of the hyperchaotic system. In Section 5, the hyperchaotic system is used in image encryption. Then, the encryption effect and security are

tested by correlation coefficient analysis, information entropy, differential attack, etc. Finally, the paper is summarized in Section 6.

2. A New Hyperchaotic System

In 1963, a representative Lorenz equation in chaotic attractors was proposed [1]. The differential expression of this equation is shown as follows Equation (1):

$$\dot{x} = \sigma(y - x),$$

$$\dot{y} = \alpha x - y - xz,$$

$$\dot{z} = xy - \beta z.$$
(1)

The equation set is a third-order system of ordinary differential equations, and each variable in the equations does not obviously contain time *t*, so the equation set is called an autonomous system. Its parameters, σ , α , and β , are all constants greater than zero. When the parameters of this equation are taken as $\sigma = 10$, $\alpha = 28$, and $\beta = 8/3$, the system presents chaotic attractor state, namely the classical Lorenz attractor, and its phase space is shown in Figure 1. The numeric computation method used to compute the chaotic system or hyperchaotic system is the 4th order Runge–Kutta method.



Figure 1. Chaotic Lorenz attractor and its phase diagrams with $\sigma = 10$, $\alpha = 28$, and $\beta = 8/3$: (a) Lorenz attractor; (b) Lorenz attractor on y–z plane; (c) Lorenz attractor on x–z plane; and (d) Lorenz attractor on x–y plane.

The new hyperchaotic system in this paper is obtained by adding a new variable, w, and a feedback controller, $-dx^3$, to the classical Lorenz chaotic attractor system. The new hyperchaotic system is expressed as follows in Equation (2):

$$\dot{x} = a(y - x),$$

$$\dot{y} = bx - y - xz + w,$$

$$\dot{z} = x^2 - cz,$$

$$\dot{w} = w - dx^3.$$
(2)

Where *a*, *b*, *c*, and *d* are all constants greater than zero. Let $a \in [20, 30]$. There are two positive LEs over a wide range of parameters, which implies that the system here is hyperchaotic, as shown in Figure 9b. Fix the parameter a = 24, then set the parameters of the system with a = 24, b = 25, c = 3, d = 0.5, and initial condition (1, 1, 1, 1). The system can present the state of a hyperchaotic system, as shown in Figure 2. The Lyapunov exponent corresponding to the hyperchaotic system is shown as follows:

$$\lambda_1 = 0, \lambda_2 = 2.5274, \lambda_3 = 2.1036, \lambda_4 = -16.3014$$

The divergence of the hyperchaotic system can be expressed as Equation (3):

$$\nabla V = \frac{\partial \dot{x}}{x} + \frac{\partial \dot{y}}{y} + \frac{\partial \dot{z}}{z} + \frac{\partial \dot{w}}{w} = -(a+c) < 0, \tag{3}$$

According to Equation (3), when a + c > 0, the hyperchaotic system is a dissipative system.



Figure 2. Hyperchaotic attractors and the phase diagrams with parameters a = 24, b = 25, c = 3, and d = 0.5: (a) hyperchaotic attractor; (b) hyperchaotic attractor on y–w plane; (c) hyperchaotic attractor on x–y plane; and (d) hyperchaotic attractor on y–z plane.

Figure 2 shows the new hyperchaotic attractors and the phase diagrams with parameters a = 24, b = 25, c = 3, and d = 0.5. (a) shows the hyperchaotic attractor, (b) shows the hyperchaotic attractor on y–w plane, (c) shows the hyperchaotic attractor on x–y plane, (c) shows the hyperchaotic attractor on y–z plane. The time series diagrams of the phases x, y, z, and w of the hyperchaotic system is shown in Figure 3 shows the time series diagrams of the hyperchaotic system, and it can be seen that the sequences have good randomness.



Figure 3. Time series diagrams of a hyperchaotic system with parameters a = 24, b = 25, c = 3, and d = 0.5: (a) time series x; (b) time series y; (c) time series z; and (d) time series w.

3. Analysis of Dynamic Properties

3.1. Subsection Equilibrium Curve

Obviously, according to system (2), an equilibrium point curve exists in the system, and the equation of the equilibrium point curve can be expressed as Equation (4):

$$\left\{ (x, y, z, w) \in \mathbb{R}^4 \middle| y = x, z = \frac{1}{c} x^2, w = dx^3 \right\},\tag{4}$$

The position relationship between this curve and system (1) is shown in Figure 4, which shows the hyperchaotic system attractor and its equilibrium curve in red.



Figure 4. Hyperchaotic attractor and its equilibrium curve with parameters a = 24, b = 25, c = 3, and d = 0.5.

3.2. Judgment of Local Stability

It is easy to know from Equation (2) that when $\frac{c(1-b)}{dc-1} < 0$ there is only one equilibrium point, O(0,0,0,0), for the system. When $\frac{c(1-b)}{dc-1} \ge 0$, the system has three balance points: O(0,0,0,0) and $O_{1,2}(\pm \frac{c(1-b)}{dc-1}, \pm \frac{c(1-b)}{dc-1}, c(\frac{1-b}{dc-1})^2, \pm dc^2(\frac{1-b}{dc-1})^3)$.

Let $k \in R$, according to Equation (2), the point $A = (k, k, k^2/3, 0.2k^3)$ is on the equilibrium point curve. Therefore, the Jacobian matrix at the equilibrium point, A, of the hyperchaotic system can be obtained as follows:

$$J = \begin{pmatrix} -a & a & 0 & 0 \\ b - k^2 / 3 & -1 & -k & 1 \\ 2k & 0 & -c & 0 \\ -3dk^2 & 0 & 0 & 1 \end{pmatrix},$$
(5)

Then the characteristic equation can be obtained:

$$\lambda^4 + g_1 \lambda^3 + g_2 \lambda^2 + g_3 \lambda^1 + g_4 = 0, (6)$$

The coefficients in the equation are:

$$g_{1} = a + c,$$

$$g_{2} = ac - ab + ak^{3}/3 - 1$$

$$g_{3} = -a - c + ab - abc + \frac{5}{3}ak^{2} + \frac{1}{3}ack^{2} + 3adk^{2}$$

$$g_{4} = -ac + abc + 3acdk^{2} - \frac{1}{3}ack^{2} - 2ak^{2}$$
(7)

According to the Routh–Hurwitz criterion, if the coefficients of the first column in the Routh array table are all positive, the system is stable. That is, all the roots of the characteristic equation are located in the left half plane of the root plane and have negative real parts. From the criterion, it can be known that the four coefficients g_1 , g_2 , g_3 , and g_4 should be positive, and $g_1g_2 - g_3 > 0$ and $g_1g_2g_3 - g_3^2 - g_4g_1^2 > 0$.

3.3. Poincare Section Diagram

The complex motion of a chaotic system is described by the Poincare section method proposed in the 19th century. It can be known from the section diagram that if only one fixed point or relatively few discrete points are shown on the section, the motion can be judged as periodic motion. When the Poincare section shows a closed curve, the motion can be judged as quasi-periodic motion. When there are dense points in the section, the motion can be judged as complex chaotic motion. For this hyperchaotic system, the Poincare section is also used to observe its motion, which is shown in Figure 5. Figure 5 shows the Poincare section of the hyperchaotic system. It can be seen that the Poincare section presents dense spots in patches, which means the system is chaotic.



Figure 5. Poincare section of hyperchaotic system attractors with parameters a = 24, b = 25, c = 3, and d = 0.5: (a) Poincare section on z–y plane; (b) Poincare section on x–y plane; and (c) Poincare section on z–x plane.

3.4. Periodic Attractor

When the hyperchaotic system (2) has the parameters a = 4, b = 5, c = 3, and d = 0.5, and its initial conditions are defined as (1, 1, 1, 1), the periodic attractor appears in the phase space of the system. Its 3D phase space projection diagram and the corresponding Poincare section diagram are shown in Figure 6. Figure 6 shows the Poincare section of the hyperchaotic system. It can be seen that the Poincare section presents a few discrete points, which means the system is periodic.



Figure 6. Poincare section of periodic attractor for hyperchaotic systems with a = 4, b = 5, c = 3, and d = 0.5: (a) Periodic attractor, and (b) Poincare section.

3.5. Quasi-Periodic Attractors

When the hyperchaotic system (2) selects parameters a = 7, b = 25, c = 3, and d = 0.5, and its initial conditions are defined as (1, 1, 1, 1), the quasi-periodic attractor appears in the phase space of the system, and its 3D phase space projection diagram and the corresponding Poincare section diagram are shown in Figure 7. Figure 7 shows the Poincare section of the hyperchaotic system. It can be seen that the Poincare section presents closed circles, which means the system is quasi-periodic.



Figure 7. Poincare section of quasi-periodic attractor for hyperchaotic systems with a = 7, b = 25, c = 3, and d = 0.5: (a) Quasi-periodic attractor, and (b) Poincare section.

3.6. Chaotic Attractor

When system (2) selects parameters a = 14, b = 25, c = 3, d = 0.5 and its initial conditions are defined as (1, 1, 1, 1), then the chaotic attractor appears in the phase space of the system. Its 3D phase space projection diagram and the corresponding Poincare section diagram are shown in Figure 8. The Lyapunov exponents corresponding to the chaotic attractor are shown below. Figure 8 shows the Poincare section of the chaotic state of the new hyperchaotic system.



Figure 8. Poincare section of chaotic attractor for hyperchaotic systems with a = 14, b = 25, c = 3 and d = 0.5: (a) Chaotic attractor, and (b) Poincare section.

3.7. Bifurcation and Lyapunov Exponent

When $a \in [20, 30]$, the change of the bifurcation diagram and Lyapunov exponent spectrum of the system with changes of parameter *a* are shown in Figure 9. Figure 9 shows the bifurcation diagram and Lyapunov exponent spectrum of the hyperchaotic system. It can be seen that bifurcation diagram is in a chaotic state in $a \in [20, 30]$, and there are two positive LEs, which means that it is a hyperchaotic system.



Figure 9. Bifurcation diagram and Lyapunov exponent spectrum of hyperchaotic system with $a \in [20, 30]$, b = 25, c = 3, and d = 0.5: (a) Bifurcation diagram, and (b) Lyapunov exponent spectrum.

4. Normalization and Quantization

In order to put the hyperchaotic system into use, normalization and quantization are done. The time series after normalization and quantization are tested.

4.1. Normalization Treatment

In order to facilitate the data processing of the hyperchaotic system, the normalization is carried out first. In this paper, the time series data of four output signals, x, y, z, and w, are mapped to the interval [-1, 1] and then quantified. The stream of the normalized hyperchaotic system is shown in Figure 10 shows the time series are normalized into the interval [-1, 1].



Figure 10. Streams of the normalized hyperchaotic system: (**a**) time series *x*; (**b**) time series *y*; (**c**) time series *z*; and (**d**) time series w.

4.2. Quantization

For the above hyperchaotic system, it must be converted into binary stream. Here, the quantization function expression is set as Q[x, y, z, w], and the definition is shown as follows:

$$Q[x, y, z, w] = \begin{cases} 0 & x, y, z, w < Tv \\ 1 & x, y, z, w \ge Tv \end{cases}$$
(8)

Here Tv = 0, $Q[\cdot]$ is the quantized binary stream. The conversion value falls within the corresponding interval of the quantization function and gets 0 or 1, respectively. As chaotic signals [x, y, z, w] have good random statistical properties, the quantized stream ($Q[\cdot]$) should have excellent statistical properties of equilibrium 0-1 ratio in theory. The streams after quantization of the time series x, y, z, and w are shown in Figure 11. Figure 11 shows the time series of the hyperchaotic system are quantized into 0-1 sequences.



Figure 11. Quantized hyperchaotic time series: (**a**) quantized time series x; (**b**) quantized time series y; (**c**) quantized time series z; and (**d**) quantized time series w.

4.3. NIST Test

The NIST SP 800-22 [50] random test package for stream cryptography (NIST random test) was provided by the National Institute of Standards and Technology. In order to verify the statistical performance of the quantized streams of the hyperchaotic system, NIST tests are carried out by using the test programs. The test package includes frequency test within a block, binary matrix rank test, non-overlapping template matching test, etc. These tests can be used to test binary sequences of an arbitrary length, generated by the pseudo-random number generator, which can be used to determine the non-randomness hidden in the stream. All of the test results are determined by P - value. If P < 0.01, then the stream is not random. If $P \ge 0.01$, then the stream is considered random. In order to make the system get better randomness, this paper carries out NIST tests to prove that the random streams generated by the system can be used in the encryption application. Table 1 shows the test results. It can be seen that the quantized streams have good statistical characteristics and have passed the tests. Table 1 shows that the sequences generated by the new hypersystem have passed all the tests in statistical NIST tests.

Test Frequency Test Frequency Test within a Block Runs Test Test for the Longest Run of Ones in a

> Block Binary Matrix Rank Test

Discrete Fourier Transform Test

Non-Overlapping Template Matching

Test

Overlapping Template Matching Test

Maurer's "Universal Statistical" Test

Linear Complexity Test

Serial Test

Approximation Entropy Test

Cumulative Sums Test

Random Excursions Test

Random Excursions Variant Test

ble 1. NIST statistical tests.					
P–Valuex	P–Valuey	P–Valuez	P–Valuew	Result	
0.110561 0.835247 0.759814	0.251486 0.142578 0.521473	0.528546 0.512879 0.715854	0.228145 0.627428 0.452842	Success Success Success	
0.214189	0.204144	0.158728	0.157569	Success	

0.428745

0.284784

0.157525

0.527865

0.285954

0.528765

0.078458

0.025481

0.627854

0.458745

0.257841

0.638175

0.258741

0.784452

0.518653

0.287695

0.318528

0.052145

0.011285

0.458654

0.514865

0.258145

Та

0.521632

0.472575

0.418622

0.514832

0.147258

0.625411

0.052148

0.021458

0.565281

0.442389

0.328489

0.352471

0.644782

0.652417

0.524718

0.195748

0.652149

0.058472

0.024187

0.421863

0.524862

0.352874

4.4. Permutation Entropy

The permutation entropy can be used to measure the complexity of time series. Permutation entropy is obtained by adding the permutation idea into the calculation of the complexity of sub-sequences. The algorithm is described as follows:

- 1. Define a time series $x(1), x(2), \ldots, x(N), m$ is the embedded dimension, τ is time delay.
- 2. Reconstruct the time series as $X(i) = x(i), x(i + \tau), \dots, x(i + (m 1)\tau)$.

3. Increase and rearrange X(i). When $x(i + (j_1 - 1)\tau) \le x(i + (j_2 - 1)\tau) \le ... \le x(i + (j_m - 1)\tau)$, if the two values are equal, rearrange by subscript.

- 4. X(i) is redefined to $(j_1, j_2, ..., j_m)$. Therefore, there will be *m*! permutations.
- 5. Define the probability distribution of all symbols as $p_1, p_2, \ldots, p_k, k \le m!$.
- 6. The permutation entropy of the time series can be calculated by the following formula:

$$H(m) = -\sum_{j=1}^{k} p_j \ln p_j,$$
(9)

 $p_k = 1/m!$, that is to say that when the probability of each symbol is equal, then the stream has the maximum permutation entropy. To facilitate data analysis, H(m) will be normalized.

$$0 \le H(m) / \ln(m!) \le 1,$$
 (10)

The results of the permutation entropy test are shown in Table 2.

Table 2. Permutation entropy valu	e
-----------------------------------	---

Time Series	т	τ	PE
x	3	1	0.6201
у	3	1	0.6548
\overline{z}	3	1	0.5724
w	3	1	0.6017

4.5. Approximate Entropy

Approximate entropy (ApEn) is used to measure the law of motion and unpredictability of a quantized time series, which is often used in nonlinear dynamics. It is characterized by the use of a

Success

non-negative number to represent the complexity of a time stream, which can reflect the possibility of new information in the stream. Therefore, the higher the approximate entropy is, the higher the complexity of the time series is. The algorithm description is shown as follows:

1. Define a time series U(1), U(2), ..., U(N).

2. *m* is the length of the comparison vector.

3. *r* is the measure of similarity.

4. Reconstruct the *m* dimension vector Y(1), Y(2), ..., Y(N - m + 1), and Y(i) = [U(i), U(i + 1), ..., U(i + m - 1)].

5. When $1 \le i \le N - m + 1$, calculate the number of vectors satisfying the following conditions:

$$C_{i}^{m}(r) = \frac{1}{N - m + 1} SUM[d(i, j) \le r],$$
(11)

6. The function is defined as:

$$\Phi^{m}(r) = \frac{1}{N-m+1} \sum_{i=1}^{N-m+1} \log(C_{i}^{m}(r)),$$
(12)

Here, $d(i, j) = \max_{a} |U(a) - U^*(a)|$. |U(a)| represents the element of the vector *Y*; *d* represents the distance between *Y*(*i*) and *Y*(*j*), whose value is determined by the maximum difference value of the corresponding element; $j \in [1, N - m + 1]$, *j* and *i* is allowed to exist in the case of equality.

From the above, the definition of Approximate Entropy (ApEn) can be obtained. In general, the value of the parameter m = 2 or m = 3 and r are determined by the actual application. Here r = 0.2 * std, and std represents the standard deviation of the original time series. Normally, $d(i, j) \le r$. The more complex the time series is, the greater the corresponding approximate entropy is. The ApEn here is shown in Table 3, which means that the time series are of good unpredictability and can be used in nonlinear dynamics.

Table 3. Approximate entropy value.

Time Series	т	r=0.2std	N	ApEn
x	2	0.1172	2048	0.7824
у	2	0.1036	2048	0.7653
z	2	0.1284	2048	0.7906
w	2	0.1165	2048	0.7819

5. Application in Image Encryption

5.1. Image Encryption Scheme

A digital image is represented by a two-dimensional matrix. Each element of the two-dimensional matrix represents the pixel value, and the coordinates of each element represent the location of the pixel. Permutation refers to taking the row and column of each element in the two-dimensional matrix of the image as the coordinate value of the pixel value, then using the encryption function to change the coordinate value of the pixel, thus changing the position of the individual pixel so that the original plaintext image cannot be recognized. Diffusion is to change the value of the pixels in the image, so as to change the statistical characteristics of the original image. Based on the principle of permutation and diffusion, the image encryption scheme here uses a low-dimensional chaotic system to obtain permutation, and high-dimensional hyperchaotic system to obtain diffusion, and generally achieves the effect of a two-step chaotic image encryption. Firstly, the sequence generated by the 1D Logistic chaotic system is used to construct the replacement table to transform the position of the original image to complete the permutation operation. Secondly, the stream cipher generated by the 4D hyperchaotic system proposed in this paper is used for diffusion operation to further ensure the security of image encryption.

Here, the hyperchaotic system stream is used to encrypt 256×256 Lena image, Cameraman image, Cake image, and Seaside image, respectively. The results of image encryption and security analysis are shown in Figure 12. Variance analysis can be used for testing the uniformity of the ciphered images. Through calculation, the histogram variance of the original Lena image is 6.2993×10^4 , and the histogram variance of the ciphered Lena image is 771.7529; the histogram variance of original Cameraman image is 1.1141×10^5 , and the histogram variance of the ciphered Cameraman image is 825.4153. It can be concluded that the histogram variances of the ciphered images are much smaller than those of the original images.



Figure 12. Comparison before and after image encryption of hyperchaotic stream: (a) original four images; (b) histograms of the four images; (c) encrypted four images; and (d) histograms of the encrypted four images.

It can be seen that the histograms of the plain images in Figure 12 are very different. The different histograms mean that the distributions of the plain images are totally different. From the cipher images, it can be found that they are all random-like. The histograms of all the encrypted images are relatively flat and are very close to uniform distributions.

5.2. Correlation Coefficient Analysis

The correlation coefficient can be used to measure the degree of the correlation between two variables, with a value between -1 and 1. The Pearson correlation coefficient between two variables is defined as the quotient of covariance and standard deviation between two variables. The correlation coefficient, r_{xy} , is defined as follows:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x) \cdot D(y)}},\tag{13}$$

Here

$$\operatorname{cov}(x,y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \tag{14}$$

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

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2,$$
(16)

where *x* and *y* are two different image pixel values, *N* represents the number of all pixels, cov(x, y) represents the covariance, D(x) represents the variance of variable *x*, and E(x) represents the mean. The more observed variables are, the less the correlation coefficient is affected by the sampling error, and the more reliable the results are. The value range of the correlation coefficient is $r_{xy} \in [-1, 1]$, and the closer $|r_{xy}|$ is to 1, the higher the correlation between the two variables is, and the closer the relationship between them is. $r_{xy} > 0$ stands for positive correlation, $r_{xy} < 0$ stands for negative correlation, and $r_{xy} = 0$ stands for zero correlation for no correlation.

In this paper, the Lena image and its encrypted image are selected as the observation data, and a total of 5000 pairs of sampling points are used. The experimental results of correlation coefficients are shown in the Figures 13 and 14. The comparison and analysis of the two groups of data are listed in Table 4.



Figure 13. The Lena image correlation coefficient diagram before encryption: (**a**) horizontal correlation; (**b**) vertical correlation; and (**c**) diagonal correlation.



Figure 14. The Lena image correlation coefficient diagram after encryption: (**a**) horizontal correlation; (**b**) vertical correlation; and (**c**) diagonal correlation.

Horizontal	Vertical	Diagonal
0.9842	0.6160	0.1969
0.0043	-0.0230	-0.0027
0.9144	0.9545	0.9562
-0.0014	0.0028	0.0080
0.9254	0.9438	0.9325
0.0045	0.0012	0.0001
0.9577	0.9440	0.9126
-0.0082	0.0027	0.0030
0.9249	0.9593	0.9026
-0.0042	-0.0011	0.0029
	Horizontal 0.9842 0.0043 0.9144 -0.0014 0.9254 0.0045 0.9577 -0.0082 0.9249 -0.0042	HorizontalVertical0.98420.61600.0043-0.02300.91440.9545-0.00140.00280.92540.94380.00450.00120.95770.9440-0.00820.00270.92490.9593-0.0042-0.0011

Table 4. Correlation coefficient analysis of Lena Image and photographer image.

As can be seen from Figures 13 and 14, the correlation coefficient diagrams before and after encryption are quite different. The correlation coefficient diagrams before encryption are of great correlation, and the diagrams after encryption are almost of no correlation.

In Table 4, the correlation coefficient of the Lena image before encryption is close to 1, which has a high correlation. The correlation coefficient of the encrypted graph is close to 0, indicating that there is almost no correlation, so it can well resist the corresponding statistical attack.

5.3. The Information Entropy

Information entropy can be used to measure the uncertainty of the randomly distributed gray value in an image. The definition of information entropy is shown as follows:

$$H(m) = \sum_{i=1}^{N} p(m_i) * \log \frac{1}{p(m_i)},$$
(17)

where $p(m_i)$ represents the probability of the sign m_i occurring, and N represents the total number of m_i . Since the state of 256 grayscale images can reach 2^8 , the maximum value of information entropy, H(m), can be 8. In this paper, the information entropy of the Lena image and the photographer image is calculated and compared. The results can be seen in Table 5, which found that the entropy value of the encrypted image here is closer to the theoretical value 8. Therefore, the encryption scheme can effectively resist an information entropy attack.

Table 5. Information entropy value.

Image	InEn
Lena image	7.9978
[38]	7.9971
[52]	7.9965
[53]	7.9971
[54]	7.9851

5.4. Analysis of Differential Attack

The attacker adds a small change to the system by changing some pixels in the image, so that the association between plaintext and ciphertext can be detected by observing the changes in the pre-encrypted and post-encrypted images. In general, to test the above, you can use the following two metrics to evaluate the encryption effect. One is pixel change rate (NPCR) [55], and the other is normalized mean change intensity (UACI) [55]. The two indicators are defined as follows:

$$NPCR = \frac{\sum_{i,j} M(i,j)}{L_1 \times L_2} \times 100\%,$$
(18)

$$UACI = \frac{1}{L_1 \times L_2} \sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \times 100\%,$$
(19)

where, C_1 and C_2 are the values before and after the change of the pixel in the same position, and $C_1(i, j)$ and $C_2(i, j)$ represents the pixel intensity of the image (i, j) before and after the change. M(i, j) is a binary matrix of the same size as C_1 and C_2 . If $C_1(i, j) \neq C_2(i, j)$, then M(i, j) = 1, otherwise M(i, j) = 0. In this paper, only one pixel value is changed, and the simulation results are shown in Table 6. The results showed that the NPCR value was close to 1, and the UACI value was close to 33.5% [38]. It shows that the encryption effect can resist some differential attacks. The test results are shown as follows:

Table 6. NPCR and UACI.

Image	NPCR	UACI%
Lena image	0.9961	33.42

5.5. Analysis of Plaintext Attack and Ciphertext Attack

There are four typical types of attacks in an image encryption system, namely ciphertext only attack, chosen ciphertext attack, known plaintext attack, and chosen plaintext attack. The chosen plaintext attack is regarded as the most powerful attack among these attacks. If an image encryption system can resist chosen plaintext attack, it can be regarded to have the ability to resist the other three attacks [55]. From the differential attack analysis above, it is known that any small changes in the plain image will lead to a totally different cipher image. It means that the encryption system in this paper can resist differential attack, which is a typically chosen plaintext attack. The new hyperchaotic system has four parameters and presents different chaotic states and output sequences, with different initial values. The ciphered images are noise-like, and the corresponding histograms are close to uniform distributions. Therefore, the proposed image encryption scheme can resist against plaintext attacks.

5.6. Analysis of Noise Attack

The ciphered image is often changed by noise attack during the transmission process of the channel, making the receiver unable to decrypt correctly. Therefore, the anti-noise attack capability of an image encryption system is one of the criteria for measuring the anti-interference capability of the system. In order to test the anti-noise attack capability of the system, before decrypting the ciphered image, pepper and salt noises of different intensities were added to the ciphered image, and then the ciphered image with the noise was decrypted with the correct key. The ciphered image with pepper and salt noise and the decrypted image were respectively shown in Figure 15. Through comparative analysis, it can be seen that the encryption algorithm in this paper has better ability to resist anti-noise attacks.



Figure 15. The ciphered images with different levels of noises and corresponding decrypted images: (a) Ciphered image with noise intensity 0.1; (b) ciphered image with noise intensity 0.2; (c) ciphered image with noise intensity 0.3; (d) decrypted image with noise intensity 0.1; (e) decrypted image with noise intensity 0.2; and (f) decrypted image with noise intensity 0.3.

5.7. Analysis of Exhaustive Attack

In the analysis of exhaustive attack, the key space and key sensitivity can be analyzed, respectively. Firstly, the analysis of anti-exhaustive attack from the perspective of key space is discussed. The encryption key in this paper consists of two parts, one is the four system parameters of the hyperchaotic system *a*, *b*, *c*, and *d*; the other part is the four initial values of the hyperchaotic system x_0 , y_0 , z_0 , and w_0 . For the above four parameters and four initial values, if the calculation accuracy is 10^{-15} , the total key space of the image encryption system is not less than 10^{120} , so the encryption algorithm has enough key space to resist exhaustive attacks. Secondly, it discusses the analysis of anti-exhaustive attack from the perspective of key sensitivity. In order to test the key sensitivity of the image encryption system for the hyperchaotic system, four initial values of x_0 , y_0 , z_0 , and w_0 were increased respectively, and the corresponding decrypted images were shown in Figure 16, under the condition that other keys do not change. It can be seen from the figure that the original image cannot be decrypted correctly even if the key is changed very slightly, so the image encryption algorithm has strong key sensitivity. In conclusion, the image encryption system has a good ability to resist exhaustive attacks.



Figure 16. The decrypted images with minor key changes: (a) decrypted image with secret key $x_0 + 10^{-15}$; (b) decrypted image with secret key $y_0 + 10^{-15}$; (c) decrypted image with secret key $z_0 + 10^{-15}$; and (d) decrypted image with secret key $w_0 + 10^{-15}$.

6. Conclusions

In this paper, a new 4D hyperchaotic system was generated based on the Lorenz chaotic system. Through numerical calculation and computer simulation, the equilibrium point, local stability, and Poincare section of the hyperchaotic system were studied. It was found that there were periodic attractors, quasi-periodic attractors, and low-dimensional chaotic attractors in the hyperchaotic system. Then, the hyperchaotic system was normalized and discretized into binary random stream ciphers. Through NIST statistical test, permutation entropy, and approximate entropy analysis, it was found that this binary stream has good statistical performance. Finally, the binary stream generated by the hyperchaotic system was applied to the grayscale image encryption. It was concluded that the encryption scheme can resist statistical attack by the correlation coefficient and the information entropy analysis. From the analysis of differential attack, plaintext attack, ciphertext attack, noise attack, and exhaustive attack, it can be concluded that the encryption scheme can resist those attacks, which shows that the image encryption scheme in this paper can achieve a better encryption effect and resist most typical attacks.

Author Contributions: L.D. conceived and wrote the paper. Q.D. gave some theoretical guidance. All authors have read and agreed to the published version of the manuscript.

Funding: The Natural Science Foundation of China: No. 61471158.

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

References

- 1. Lorenz, E.N. Deterministic non-periodic flow. J. Atmos. Sci. 1963, 20, 130–141. [CrossRef]
- 2. Li, X.; Xie, Z.; Wu, J.; Li, T. Image Encryption Based on Dynamic Filtering and Bit Cuboid Operations. *Complexity* **2019**, 2019, 7485621. [CrossRef]
- 3. Wang, X.; Gao, S. Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. *Inf. Sci.* **2020**, *507*, 16–36. [CrossRef]
- Wang, X.; Feng, L.; Zhao, H. Fast image encryption algorithm based on parallel computing system. *Inf. Sci.* 2019, 486, 340–358. [CrossRef]
- 5. Ai, B.-Q.; Wang, X.-J.; Liu, G.-T.; Liu, L.-G. Correlated noise in a logistic growth model. *Phys. Rev. E* 2003, 67, 022903. [CrossRef]
- Wang, L.Y.; Cheng, H. Pseudo-Random Number Generator Based on Logistic Chaotic System. *Entropy* 2019, 21, 960. [CrossRef]
- 7. Rubens, R. Quantum-chaotic key distribution in optical networks: From secrecy to implementation with logistic map. *Quantum Inf. Process.* **2018**, *17*, 329.
- 8. Sheela, S.J. Image encryption based on modified Henon map using hybrid chaotic shift transform. *Multimed. Tools. Appl.* **2018**, *77*, 25223–25251. [CrossRef]
- 9. Roy, A. Audio signal encryption using chaotic Henon map and lifting wavelet transforms. *Eur. Phys. J.* 2017, 132, 524. [CrossRef]
- 10. Balibrea-Iniesta, F.; Lopesino, C.; Wiggins, S.; Mancho, A.M. Chaotic Dynamics in Nonautonomous Maps: Application to the Nonautonomous Henon Map. *Int. J. Bifurcat. Chaos* **2015**, *25*, 1550172. [CrossRef]
- 11. Jamal, R.K. Secure Communication Coupled Laser Based on Chaotic Rossler Circuits, Nonlinear Optics. *Quantum Optics* **2019**, *51*, 79–91.
- Girdhar, A. A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences. *Multimed Tools Appl.* 2018, 77, 27017–27039. [CrossRef]
- 13. Mandal, M.K. Symmetric key image encryption using chaotic Rossler system. *Secur. Commun. Netw.* **2014**, *7*, 2145–2152. [CrossRef]
- 14. Mishra, J. Modified Chua chaotic attractor with differential operators with non-singular kernels. *Chaos Solitons Fractals* **2019**, *125*, 64–72. [CrossRef]
- 15. Freud, S. On the Influence of the Coupling Strength among Chua's Circuits on the Structure of Their Hyper-Chaotic Attractors. *Int. J. Bifurcat. Chaos* **2016**, *26*, 1650115. [CrossRef]

- 16. Korneta, W.; Garcia-Moreno, E.; Sena, A.L. Noise activated dc signal sensor based on chaotic Chua circuit. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *24*, 145–152. [CrossRef]
- 17. Sathiyamurthi, P.; Ramakrishnan, S. Testing and Analysis of Chen Chaotic Mapping for Speech Cryptography. *J. Test. Eval.* **2019**, *47*, 3028–3040. [CrossRef]
- 18. Huang, X.; Liu, L.F.; Li, X.J.; Yu, M.R.; Wu, Z.J. A New Pseudorandom Bit Generator Based on Mixing Three-Dimensional Chen Chaotic System with a Chaotic Tactics. *Complexity* **2019**, 2019, 6567198. [CrossRef]
- 19. Ozkaynak, F.; Celik, V.; Ozer, A.B. A new S-box construction method based on the fractional-order chaotic Chen system. *Signal Image Video P* **2017**, *11*, 659–664. [CrossRef]
- 20. Liu, L.C.; Du, C.H.; Zhang, X.F.; Li, J.; Shi, S.S. Dynamics and Entropy Analysis for a New 4-D Hyperchaotic System with Coexisting Hidden Attractors. *Entropy* **2019**, *21*, 287. [CrossRef]
- 21. Ma, J.; Chen, Z.; Wang, Z.; Zhang, Q. A four-wing hyper-chaotic attractor generated from a 4-D memristive system with a line equilibrium. *Nonlinear Dyn.* **2015**, *81*, 1275–1288. [CrossRef]
- 22. Singh, J.P.; Roy, B.K.; Jafari, S. New family of 4-D hyperchaotic and chaotic systems with quadric surfaces of equilibria. *Chaos Solitons Fractals* **2018**, *106*, 243–257. [CrossRef]
- 23. Vaidyanathan, S. Analysis, adaptive control and synchronization of a novel 4-D hyperchaotic hyperjerk system via backstepping control method. *Arch. Control.Sci.* **2016**, *26*, 311–338. [CrossRef]
- 24. Koyuncu, I.; Alcin, M.; Tuna, M.; Pehlivan, I.; Varan, M.; Vaidyanathan, S. Real-time high-speed 5-D hyperchaotic Lorenz system on FPGA. *Int. J. Comput. Appl. Technol.* **2019**, *61*, 152–165.
- 25. Bonyah, E. Chaos in a 5-D hyperchaotic system with four wings in the light of non-local and non-singular fractional derivatives. *Chaos Solitons Fractals* **2018**, *116*, 316–331. [CrossRef]
- 26. Zhang, L.M.; Sun, K.H.; He, S.B.; Wang, H.H.; Xu, Y.X. Solution and dynamics of a fractional-order 5-D hyperchaotic system with four wings. *Eur. Phys. J. Plus* **2017**, *132*, 31. [CrossRef]
- 27. Vaidyanathan, S.; Volos, C.; Pham, V.T. Hyperchaos, adaptive control and synchronization of a novel 5-D hyperchaotic system with three positive Lyapunov exponents and its SPICE implementation. *Arch. Control Sci.* **2014**, *24*, 409–446. [CrossRef]
- 28. Hu, Z.Y.; Chan, C.K. A 7-D Hyperchaotic System-Based Encryption Scheme for Secure Fast-OFDM-PON. *J. Lightwave. Technol.* **2018**, *36*, 3373–3381. [CrossRef]
- 29. Liu, J.; Tong, X.J.; Wang, Z.; Ma, J.; Yi, L.T. An Improved Rao-Nam Cryptosystem Based on Fractional Order Hyperchaotic System and EDF-QC-LDPC. *Int. J. Bifurcat. Chaos* **2019**, *29*, 1950122. [CrossRef]
- 30. Lassoued, A.; Boubaker, O. Dynamic Analysis and Circuit Design of a Novel Hyperchaotic System with Fractional-Order Terms. *Complexity* **2019**, 1564573. [CrossRef]
- 31. Boraha, M.; Roy, B.K. Design of fractional-order hyperchaotic systems with maximum number of positive Lyapunov exponents and their antisynchronisation using adaptive control. *Int. J. Control* **2018**, *91*, 2615–2630. [CrossRef]
- 32. Goufo, E.F.D. On chaotic models with hidden attractors in fractional calculus above power law. *Chaos Solitons Fractals* **2019**, 127, 24–30. [CrossRef]
- Bayani, A.; Rajagopal, K.; Khalaf, A.J.M.; Jafari, S.; Leutcho, G.D.; Kengne, J. Dynamical analysis of a new multistable chaotic system with hidden attractor: Antimonotonicity, coexisting multiple attractors, and offset boosting. *Phys. Lett. A* 2019, 383, 1450–1456. [CrossRef]
- 34. Pham, V.T.; Volos, C.; Jafari, S.; Kapitaniak, T. A Novel Cubic-Equilibrium Chaotic System with Coexisting Hidden Attractors: Analysis, and Circuit Implementation. *J. Circuit Syst. Comp.* **2018**, 27, 1850066. [CrossRef]
- 35. Wang, N.; Zhang, G.S.; Bao, H. Bursting oscillations and coexisting attractors in a simple memristor-capacitorbased chaotic circuit. *Nonlinear Dyn.* **2019**, *97*, 1477–1494. [CrossRef]
- 36. Lai, Q.; Nestor, T.; Kengne, J.; Zhao, X.W. Coexisting attractors and circuit implementation of a new 4D chaotic system with two equilibria. *Chaos Solitons Fractals* **2018**, *107*, 92–102. [CrossRef]
- 37. Li, T.; Yang, M.; Wu, J.; Jing, X. A Novel Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System and DNA Computing. *Complexity* **2017**, 2017, 9010251. [CrossRef]
- 38. Li, T.; Shi, J.; Li, X.; Wu, J.; Pan, F. Image Encryption Based on Pixel-Level Diffusion with Dynamic Filtering and DNA-Level Permutation with 3D Latin Cubes. *Entropy* **2019**, *21*, 319. [CrossRef]
- 39. Molteni, F.; Kucharski, F. A heuristic dynamical model of the North Atlantic Oscillation with a Lorenz-type chaotic attractor. *Clim. Dyn.* **2019**, *52*, 6173–6193. [CrossRef]
- 40. Mallory, K.; van Gorder, R.A. Competitive Modes for the Detection of Chaotic Parameter Regimes in the General Chaotic Bilinear System of Lorenz Type. *Int. J. Bifurcat. Chaos* **2015**, *25*, 1530012. [CrossRef]

- 41. Yan, W.H.; Ding, Q. A New Matrix Projective Synchronization and Its Application in Secure Communication. *IEEE Access* **2019**, *7*, 112977–112984. [CrossRef]
- 42. Ding, L.N.; Liu, C.Y.; Zhang, Y.P. A New Lightweight Stream Cipher Based on Chaos. *Symmetry* **2019**, *11*, 853. [CrossRef]
- 43. Garcia-Bosque, M.; Diez-Senorans, G.; Perez-Resa, A. A 1 Gbps Chaos-Based Stream Cipher Implemented in 0.18 mu m CMOS Technology. *Electronics* **2019**, *8*, 623. [CrossRef]
- 44. Li, X.; Li, T.; Wu, J.; Xie, Z.; Shi, J. Joint image compression and encryption based on sparse Bayesian learning and bit-level 3D Arnold cat maps. *PLoS ONE* **2019**, *14*, e0224382. [CrossRef] [PubMed]
- 45. 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]
- 46. Ye, G.D.; Huang, X.L. An efficient symmetric image encryption algorithm based on an intertwining logistic map. *Neurocomputing* **2017**, 251, 45–53. [CrossRef]
- 47. 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]
- 48. Wu, J.; Shi, J.; Li, T. A Novel Image Encryption Approach Based on a Hyperchaotic System, Pixel-Level Filtering with Variable Kernels, and DNA-Level Diffusion. *Entropy* **2020**, *22*, 5. [CrossRef]
- 49. Wang, X.; Gao, S. Application of matrix semi-tensor product in chaotic image encryption. *J. Frankin. Inst.* **2019**, *18*, 11638–11667. [CrossRef]
- 50. 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.
- 51. Zhu, C.; Hu, Y.; Sun, K. New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern. *J. Electron. Inf. Technol.* **2012**, *34*, 1735–1743. [CrossRef]
- 52. Fan, C.L.; Ding, Q. A Novel Image Encryption Scheme Based on Self-Synchronous Chaotic Stream Cipher and Wavelet Transform. *Entropy* **2018**, *20*, 445. [CrossRef]
- 53. Li, P.; Xu, J.; Mou, J.; Yang, F.F. Fractional-order 4D hyperchaotic memristive system and application in color image encryption. *EURASIP J. Image* 2019, 2019, 22. [CrossRef]
- 54. Chai, X.; Gan, Z.; Lu, Y.; Chen, Y.; Han, D. A novel image encryption algorithm based on the chaotic system and DNA computing. *Int. J. Mod. Phys. C* 2017, *28*, 1750069. [CrossRef]
- 55. Zhan, K.; Wei, D.; Shi, J.; Yu, J. Cross-utilizing hyperchaotic and DNA sequences for image encryption. *J. Electron. Imaging* **2017**, *26*, 013021. [CrossRef]



© 2020 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/).