electronics

MDPI

Article

A Novel Image Encryption Scheme Based on 2D Fractional Chaotic Map, DWT and 4D Hyper-chaos

Lina Ding [1,2] and Qun Ding [1,*]

[1] Electronic Engineering College, Heilongjiang University, Harbin 150080, China; dinglina@aliyun.com
[2] Electrical Engineering College, Suihua University, Suihua 152061, China
* Correspondence: qunding@aliyun.com; Tel.: +86-0451-8660-8504

Received: 16 July 2020; Accepted: 6 August 2020; Published: 9 August 2020

Abstract: In this paper, a novel image encryption scheme based on a fractional-order Henon chaotic map, a two-dimensional (2D) Discrete Wavelet Transform (DWT) and a four-dimensional (4D) hyperchaotic system is proposed. Firstly, the original image is transformed and scrambled by the 2D DWT, and then the image is shuffled with the fractional-order Henon chaotic time series. Finally, the shuffled image is diffused and encrypted by the 4D hyperchaos system. Through the application of DWT and high-low dimensional chaotic systems, the encryption effect of this algorithm is better than those done by single or ordinary chaotic encryption algorithm, and it has a larger key space and higher security. The experimental tests show that the system has good statistical characteristics, such as histogram analysis, correlation coefficient analysis, key space and key sensitivity, information entropy analysis and so on. The encryption algorithm also passes the relevant security attack tests with good security.

Keywords: fractional-order Henon chaotic map; hyper-chaos system; image encryption

1. Introduction

Due to inherent initial value sensitivity, ergodicity and unpredictability, chaotic system is very suitable for information security and secure communication [1,2]. With the development of network technology, an image is used as a very important carrier, and how to prevent it from being illegally copied and transmitted in the transmission process, namely the image information security and encryption, has become an important research topic. Therefore, image encryption schemes based on chaotic systems have been widely used in recent years, and many new methods have emerged in the image encryption processes, such as DNA rules, bit-level arrangement, one-time key, matrix and semi-tensor product theory [3–5].

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. The original low-dimensional chaotic systems were applied in image encryption schemes by some researchers because of their simple forms and being easily realized by coding. The authors of [6] applied Logistic, a one-dimensional (1D) chaotic map, to image encryption and two 1D Logistic chaotic maps were used to obtain good encryption effects. The authors of [7] generated a new 1D chaotic system and applied it to real-time image encryption. However, since the one-dimensional system has only one variable, few parameters and relatively simple structure, the encryption effect and security were relatively low. Therefore, some researchers applied a two-dimensional (2D) chaotic systems to image encryption schemes. A 2D chaotic Arnold cat map was used to generate a three-dimensional (3D) cat map, which then was used for image encryption [8]. The results show that the scheme was fast and safe. The authors of [9] applied the Henon mapping to their image encryption scheme, and proved that the encryption method could resist selective plaintext attack, etc. The authors of [10] applied the 2D

Henon chaotic map to the image encryption method of mixed shift transformation. The authors of [11] applied the symmetric cipher generated by a 2D chaotic map to image encryption and obtained a good diffusion effect. With the application of the 2D chaotic systems in the image encryption schemes, the 3D chaotic systems are widely used in image encryption. The authors of [12] applied a 3D Rossler chaotic system to a symmetric key image encryption. The authors of [13] combined a 3D Lorenz chaotic system and a 3D Rossler chaotic system to generate deoxyribonucleic acid (DNA) sequences and applied them to a red-green-blue (RGB) image encryption. With the research and development of chaotic systems, hyperchaotic systems with more than four dimensions have been studied and applied [14–18]. Such hyperchaotic systems have two or more positive Lyapunov exponents, with better chaotic characteristics and more random chaotic time series. Therefore, the applications of hyperchaotic systems in image encryption are increasing. The authors of [19] applied a hyperchaos system to generate a random key and applied it to the image diffusion process to obtain a good encryption effect. The authors of [20] applied a five-dimensional (5D) hyperchaos system in the process of parallel image encryption and showed a good encryption effect. The authors of [21] proposed an image encryption algorithm based on a seven-dimensional (7D) hyper-chaotic system and simultaneous row-column swapping. In this paper, a hash function was applied to generate the system parameters and initial values of the 7D hyper-chaotic system. Then seven real numbers were transformed in order to form three new sequences, which were used for the scrambling and diffusion operations. A scrambling matrix was formed, and a plain image was subjected to the permutation process. Finally, the diffusion method was performed on the scrambled image, and the cipher image was ultimately obtained.

So far, based on the above 1D chaotic maps, such as the Logistic map and the Tent map [22–24], and 2D chaotic systems, such as the Henon map [25–28], and 3D chaotic systems such as the Rossler chaotic attractor [29,30], the Chua chaotic system [31,32] and the Chen chaotic system [33–35], the applications of chaotic systems in image encryption schemes have been relatively mature in chaos researches and developments. However, the fractional-order chaotic systems have more complex dynamic behaviors and mathematical explanations than the above integer order chaotic systems, so they have higher degrees of non-linearity [36]. In recent years, the applications of the fractional-order chaotic systems in image encryption schemes have become the research hotspots [37,38]. The authors of [39] combined a fractional discrete chaotic system and a SPIHT (Set partitioning in Hierarchical Trees) coding algorithm, and then proposed an image compression and encryption algorithm based on the above algorithms. The authors of [40] constructed a new image encryption algorithm, which was based on a fractional-order hyper-chaotic system and the DNA computing. Firstly, the authors used a fractional-order hyper-chaotic Lorenz system to generate a pseudo-random sequence that utilized during the whole encryption process; secondly, a diffusion scheme was used to spread the little change in one pixel to all the other pixels; thirdly, DNA rules were used to encode the plain image and the corresponding DNA operations were performed; finally, the global permutation and 2D and 3D permutations were performed on pixels, bits, and acid bases.

Wavelet transform is a time-frequency analysis tool, which can not only investigate the time-domain characteristics of the local frequency-domain processes, but also investigate the frequency-domain characteristics of the local time-domain processes. Wavelet transform can transform the image into a series of wavelet coefficients, which contain the low frequency coefficients and the high frequency coefficients of the image data. The wavelet coefficients can be efficient compressed and stored, the rough edges of the wavelet can better show the image, so the wavelet transform is often applied in the process of image encryption [41]. Digital image is characterized by large amount of data with high degree of data redundancy and strong correlation among pixels. Through wavelet transform, the entire frequency domain cannot be encrypted, but a small number of low-frequency coefficients can be encrypted, so the redundancy can be reduced, and the important part of the image can be encrypted, then the rest of the secondary part is not encrypted and compressed [42]. The authors of [43] proposed a color image lossless encryption algorithm based on a hyperchaotic system and the 2D DWT.

Based on the above analysis, this paper proposes an image encryption scheme based on a second-order fractional-order chaotic map and the 2D DWT and a hyperchaotic system.

The main contributions of this paper are shown as follows: (1) the original image is obtained and transformed by using the time-frequency transform characteristics of the DWT, which greatly scrambles the pixel values of the image; (2) then the fractional-order 2D Henon chaotic map is applied in the image confusion stage to achieve a better image confusion effect; (3) the stream cipher generated by the four-dimensional (4D) hyper-chaos is applied to the gray image encryption with sufficient confusion in the above two steps, and the encryption process is completed; (4) the system has experienced a DWT scrambling, a fractional-order 2D chaotic map confusion operations and finally a 4D hyper-chaotic system encryption processes. There are sufficient confusion operations, transformation operations and diffusion operations, which shows that it is a proper idea and method.

The main innovation points of this paper are shown as follows: (1) the DWT is used to scramble the pixel value of the image greatly from the time domain to the frequency domain; (2) the application of the fractional-order chaotic system in image encryption is different from those of previous chaotic systems. In this paper, the fractional-order Henon chaotic system is applied in the confusion stage of image encryption to obtain a better confusion effect; (3) the 4D hyperchaotic system adopted here has large Lyapunov exponents, which makes the generated chaotic stream cipher more random, and the experiments prove that the image encryption effect is good; (4) in the confusion and diffusion stages of the image encryption algorithm, there are mixed applications of high and low dimensional chaotic systems, mixed applications of fractional order and integer order chaotic systems, and image transformation both in time domain and frequency domain.

The structure of this paper is shown as follows: in Section 2, the fractional calculus, the fractional-order 2D Henon chaotic map, the DWT and the theoretical basis of the 4D hyperchaotic system are introduced; in Section 3, the image encryption algorithm is introduced, and the experimental results of the image encryption effect are given, including statistical analysis, comparisons, attacks and other security tests; in Section 4, the paper is summarized.

2. The Basic Theory

2.1. The Definition of Fractional Calculus

The fractional-order differential operator D^{α} and the fractional-order integral operator I^{α} are the basis of studying the fractional-order calculus (FOC), here α is a real number. The discrete fractional calculus is often applied to the study of the fractional discrete chaotic systems. In general, the nth order difference equation can be defined as:

$$\Delta^{m} g(t) = \Delta^{m-1} g(t+1) - \Delta^{m-1} g(t) = \sum_{j=0}^{m} \binom{m}{j} (-1)^{j} g(t+m-j), \tag{1}$$

Definition 1 (See [44]). *For $g: N_i \to R$ and $\alpha > 0$, the fractional order sum of order α is defined as:*

$$\Delta_{i}^{-\alpha} g(t) = \frac{1}{\Gamma(\alpha)} \sum_{s=i}^{t-\alpha} (t - \sigma(s))^{(\alpha-1)} g(s), \tag{2}$$

Here, each variable is defined as: $t \in N_{i+\alpha}$, i is the starting point, $i \in R$, $\sigma(s) = s + 1$, $\Delta_{i}^{-\alpha}$ is a mapping which is from functions defined on N_i to functions defined on $N_{i+\alpha}$, $\Gamma(\alpha)$ is a Gamma function and is defined as $\Gamma(\alpha) = \int_{0}^{+\infty} t^{\alpha-1} e^{-t} dt$, then the generalized falling factorial $t^{(\alpha)}$ is defined as $t^{(\alpha)} = \frac{\Gamma(t+1)}{\Gamma(t+1-\alpha)}$.

It is the Caputo's definition of the fractional difference, which is derived from the continuous time definition of the fractional calculus given by Caputo.

Definition 2 (See [45]). *The Caputo like delta fractional difference of $g(t)$ on N_i is defined as:*

$$\Delta_C^{\alpha} g(t) = \frac{1}{\Gamma(m-\alpha)} \sum_{s=i}^{t-(n-\alpha)} (t-\sigma(s))^{(m-\alpha-1)} \Delta_s^n g(s), \tag{3}$$

Here, each variable is defined as: α is the difference order, i is a real number, $N_i = \{i, i+1, i+2, \ldots\}$ and $m = [\alpha] + 1$.

2.2. The Basic Definition of Fractional Difference Equation

The fractional order nonlinear difference equation can be defined as [46]:

$$\Delta_i^{\alpha} u(t) = g(t+\alpha-1, u(t+\alpha-1)), \tag{4}$$

Here, each variable is defined as: $\Delta^k u(i) = u_k$, $n = [\alpha] + 1$, $k = 0, 1, \ldots, n-1$, k is a real number and is the order of the fractional difference.

The solution of the above equation can be obtained as follows:

$$u(t) = u_0(t) + \frac{1}{\Gamma(\alpha)} \sum_{s=i+n-\alpha}^{t-\alpha} (t-\sigma(s))^{(\alpha-1)} g(s+\alpha-1, u(s+\alpha-1)), \tag{5}$$

Here, $u_0(t)$ is the initial state, $u_0(t) = \sum_{k=0}^{n-1} \frac{(t-i)^k}{k!} \Delta^k u(i)$.

By extending $(t-\sigma(s))^{(\alpha-1)} = \frac{\Gamma(t-s)}{\Gamma(t-s-\alpha+1)}$, the fractional difference equation can be obtained as [44]:

$$u(t) = u_0(t) + \frac{1}{\Gamma(\alpha)} \sum_{j=1}^{t} \frac{\Gamma(t-j+\alpha)}{\Gamma(t-j+1)} g(j-1, u(j-1)), \tag{6}$$

2.3. The Fractional Henon Map

The 2D Henon chaotic map equation is shown as follows:

$$\begin{cases} x_{n+1} = 1 + y_n - a x_n^2 \\ y_{n+1} = b x_n \end{cases}, \tag{7}$$

Here a and b are both parameters and are positive real numbers. By rewriting and modifying the 2D Henon chaotic map equation and exchanging the integral form to the fractional form through the methods above, the paper by [47] gives the fractional form of the Henon map, which can be expressed as:

$$\begin{cases} x_{n+1} = x_0 + \frac{1}{\Gamma(\alpha)} \sum_{i=1}^{m} \frac{\Gamma(m-i+\alpha)}{\Gamma(m-i+1)} (1 + y_n - a x_n^2 - x_n) \\ y_{n+1} = y_0 + \frac{1}{\Gamma(\alpha)} \sum_{i=1}^{m} \frac{\Gamma(m-i+\alpha)}{\Gamma(m-i+1)} (b x_n - y_n) \end{cases}, \tag{8}$$

Here, x_0 and y_0 are the initial values, the parameters α, a and b can be adjusted to produce the fractional order Henon map, and $\Delta\alpha = 0.001$. The phase space diagrams of the fractional-order Henon map is shown in Figure 1, and the bifurcation diagram and time series diagram are shown in Figures 2 and 3.

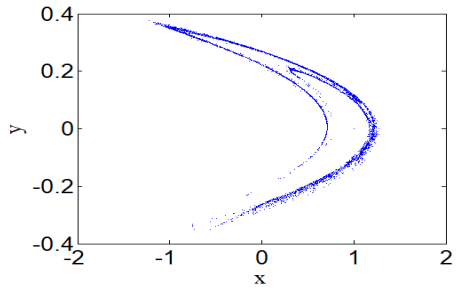


Figure 1. The phase space diagram of the fractional-order Henon map with $x_0 = 0$, $y_0 = 0$, $\alpha = 0.99$, $a = 1.4$ and $b = 0.3$.

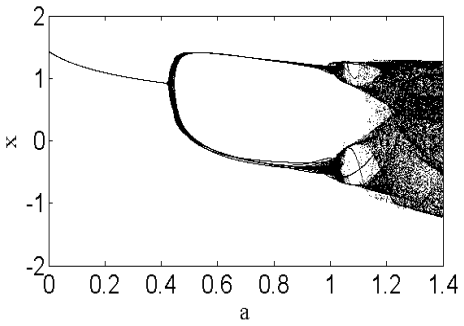


Figure 2. The bifurcation diagram of the fractional-order Henon map with $x_0 = 0$, $y_0 = 0$, $\alpha = 0.99$ and $b = 0.3$.

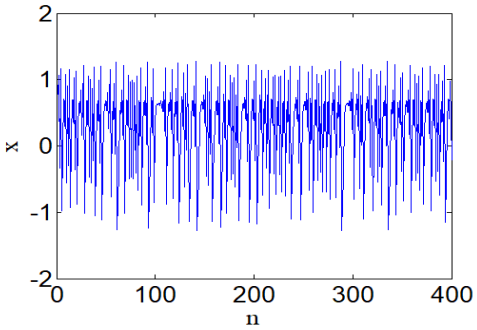


Figure 3. The time series diagram of the fractional-order Henon map with $\alpha = 0.99$ and $b = 0.3$.

2.4. Discrete Wavelet Transform

Wavelet transform is a new theory and method developed on the basis of Fourier transform. Wavelet transform can carry out localized time-frequency analysis and show the characteristics of the signal simultaneously both in the frequency domain and the time domain. It can also independently analyze any frequency band and the time period of a signal. Figure 4 shows the DWT decomposition and reconstruction processes. The cA_{i-1} is the approximated coefficient at level 1, the cA_i is the approximated coefficient at level 2, the $cD(h)_i$ is the horizontal detail coefficient at level 2, the $cD(v)_i$ is the vertical detail coefficient at level 2 and the $cD(d)_i$ is the diagonal detail coefficient at level 2.

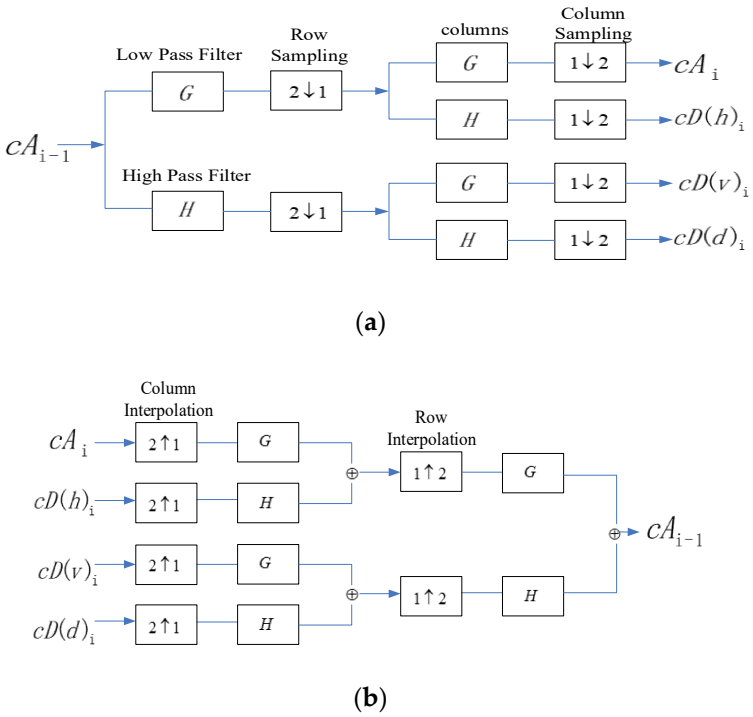


Figure 4. The DWT image decomposition and reconstruction processes: (**a**) the decomposition process; (**b**) the reconstruction process.

Wavelet transform has been widely used in digital image processing in recent years. Since the form of a digital image is a 2D matrix, so you can apply the 2D DWT multi-resolution decomposition to the image. The 2D DWT decomposed image consistent four parts, namely the LH1 (horizontal details), HL1 (vertical details), HH1 (diagonal details) and LL1 (approximate figure, the low frequency part). Each decomposition is conducted on the basis of decomposition of LL1 part. The basic information of the digital image is mostly covered in its approximate part, namely the LL1 low frequency part. The LL1 sub-band can be further decomposed into four sub-diagrams of LL2, HL2, LH2 and HH2, namely the two-level decomposition, which are shown in Figure 5.

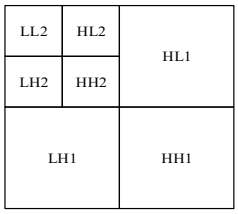


Figure 5. The DWT image two-level decomposition.

In order to achieve better digital image encryption accuracy and resolution, the digital image is decomposed through the two-level decomposition, and the image is transformed from time domain to frequency domain with a good effect in enhancing the scrambling effect of the pixel.

2.5. The 4D Hyperchaotic System

The authors of [48] proposed a new 4D hyperchaotic system, which is controlled by six parameters and has two extremely large positive Lyapunov exponents. The orbit of this hyperchaotic system has very strong expansion and contraction, resulting in a more disordered and random system. Moreover, the hyperchaotic system has strong robustness and extremely complex dynamic behavior. It can be seen from the spectrum analysis that the high frequency band is very wide and it has very good

randomness. In this paper, the pseudorandom sequences generated by the system are used for image encryption. The equations of the system [48] are shown as:

$$\begin{aligned} \dot{x_1} &= a(x_2 - x_1) + x_2x_3, \\ \dot{x_2} &= b(x_2 + x_1) - x_1x_3, \\ \dot{x_3} &= -cx_3 - ex_4 + x_1x_2, \\ \dot{x_4} &= -dx_4 + fx_3 + x_1x_2, \end{aligned} \tag{9}$$

Let $b \in [15.425, 27]$, the parameters $a = 50$, $c = 13$, $d = 8$, $e = 33$ and $f = 30$, at this time the system can obtain Lyapunov exponents $l_1 \in [8.3585, 13.4632]$, $l_2 \in [0.1, 3.4781]$, $l_3 \cong 0$ and $l_4 < -60$. Thus, within the above parameter intervals, the hyperchaotic system has two large positive Lyapunov exponents, and the randomness of the system is the best. The phase space diagrams and time series diagrams of the system are shown in Figures 6 and 7.

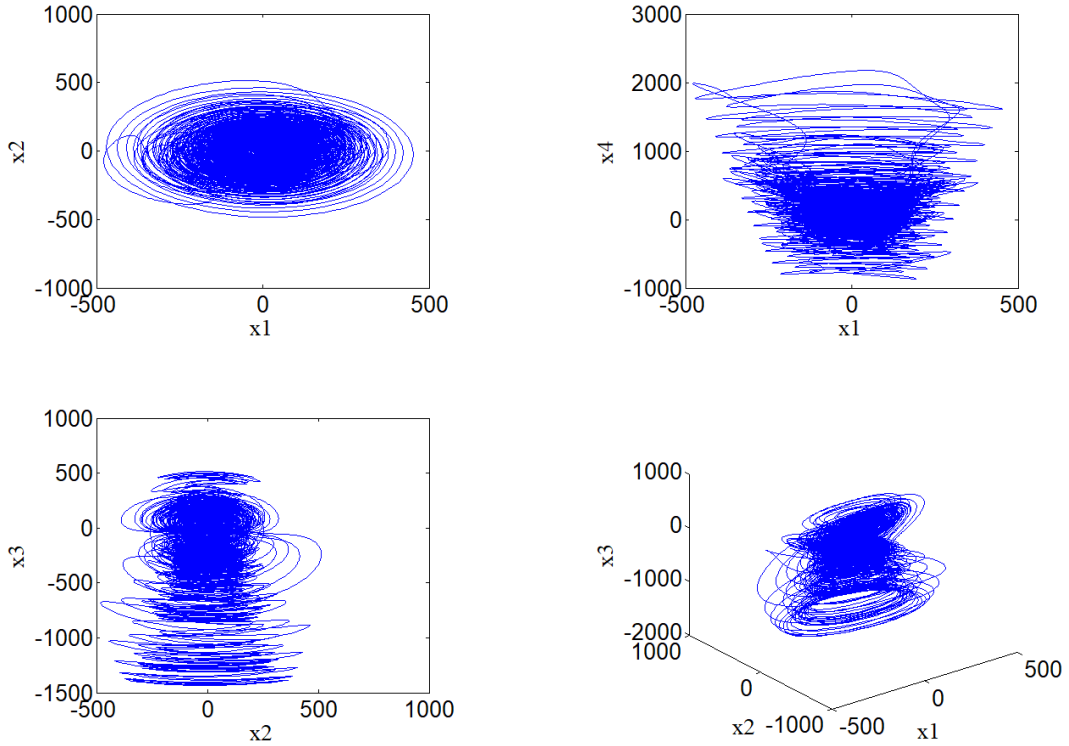


Figure 6. The hyperchaotic system phase space diagrams with parameters $a = 50$, $b = 26$, $c = 13$, $d = 8$, $e = 33$ and $f = 30$.

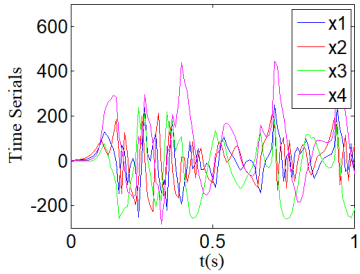


Figure 7. The hyperchaotic system time series diagrams with parameters $a = 50$, $b = 26$, $c = 13$, $d = 8$, $e = 33$ and $f = 30$.

Here, $x_0 = [0.1201\ 1.72\ 2.52\ 3.05]$ and $x_0' = [0.1202\ 1.72\ 2.52\ 3.05]$, it can be seen that there is a tiny difference of the initial values between x_0 and x_0', namely $x_{01} = 0.1201$ and $x_{01}' = 0.1202$. The the initial value sensitivity of the system is shown in Figure 8. It can be seen that the initial value sensitivities of the four time series of the system are very good.

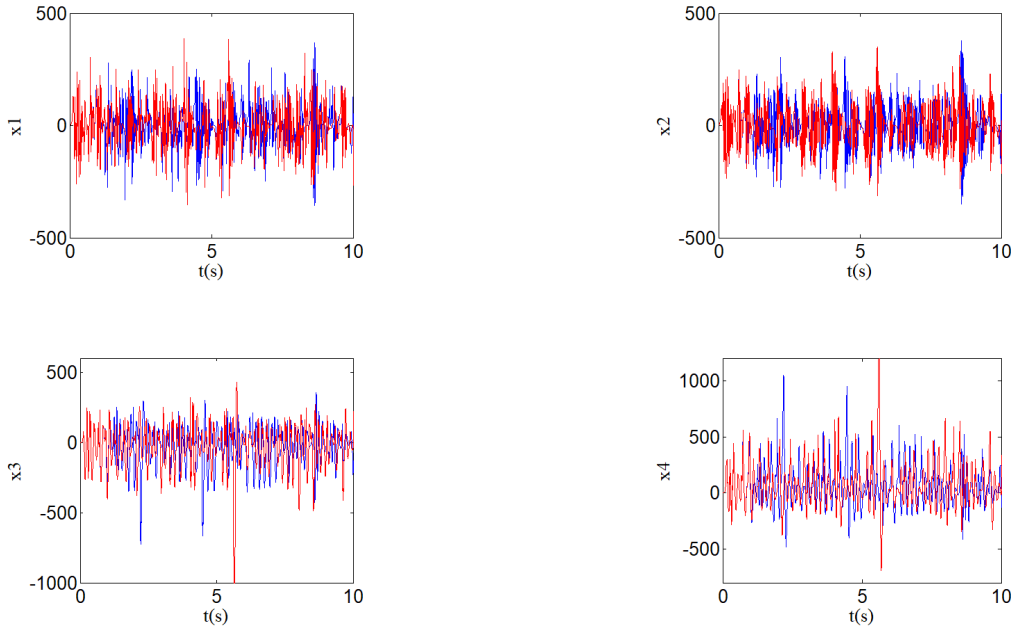


Figure 8. The hyperchaotic system initial value sensitivity with parameters $a = 50$, $b = 26$, $c = 13$, $d = 8$, $e = 33$ and $f = 30$.

3. The Image Encryption Algorithm and Security Analysis

3.1. The Image Encryption Algorithm Description

In this paper, a novel image encryption algorithm based on the fractional-order 2D Henon chaotic map, the 2D DWT and the 4D hyperchaotic system is proposed. The image encryption algorithm description is shown in Figure 9. Firstly, the original image is decomposed through two-level DWT to complete the transformation in the time-frequency domain for scrambling. Secondly, the fractional-order Henon chaotic system is used for image shuffling. Finally, the shuffled image generated in the previous step is xored by the stream cipher generated by the 4D hyperchaotic system for encryption.

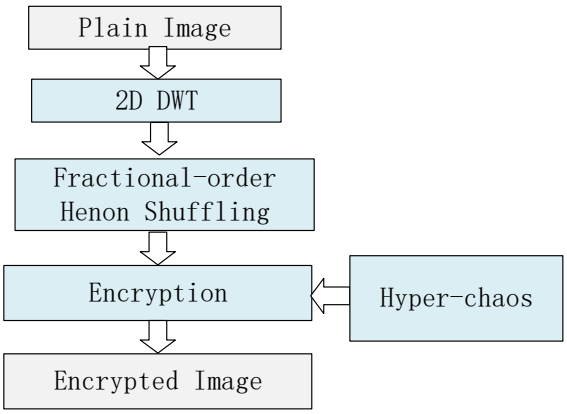


Figure 9. The block diagram of the image encryption algorithm.

The image encryption process is divided into six steps:

Step 1: Read a $m \times n$ dimension image as the plaintext input;

Step 2: Perform two-level DWT on the input image and complete time-frequency domain transformation, then get the image S.

Step 3: Fractional-order Henon chaotic system is used for image diffusion, which is the first layer of the image encryption. The chaotic system parameters are set as $\alpha = 0.99$ and $b = 0.3$, and the initial values of the system are set as $x_0 = 0$ and $y_0 = 0$. In order to eliminate the effect of the initial sequence of the chaotic system, the chaotic system is set to generate the encryption key K_1 after 1000 iteration. The image P is obtained after diffusion encryption.

Step 4: Generate the 4D hyperchaotic system stream cipher. The parameters of the chaotic system are set as $a = 50$, $b = 26$, $c = 13$, $d = 8$, $e = 33$ and $f = 30$, the initial values of the system are set as $x_0 = [0.1201\ 1.72\ 2.52\ 3.05]$. Similarly, the stream cipher after iteration of the chaotic system is generated as a secret key K_2.

Step 5: The image generated in Step 3 is further encrypted with the secret key K_2 generated by the 4D hyper-chaotic system in Step 4 to obtain the ciphertext image C.

Step 6: After the above five steps, the final ciphertext image C is generated, and the encryption process is completed.

The decryption process is the reverse of the encryption process.

3.2. Algorithm Security Analysis

3.2.1. Key Space Analysis

Key space refers to the value range of all keys in the encryption system. The key space of any encryption algorithm must be large enough to ensure that the encryption algorithm can resist exhaustive attacks [49]. In general, the key space of the encryption algorithm must be larger than 2^{100}. In image encryption, the size of the key space can be obtained by multiplying the value space of a single key. If the key of pixel value is K_1, when it is scrambled; the key is K_2, when it is diffused; then the key space is K_1K_2. If multiple iterations are carried out in the image encryption process, the key space is $(K_1K_2)^n$, and n is the iteration round.

In this scheme, the hyper-chaos system consists of six control parameters a, b, c, d, e and f, and four initial conditions x_1, x_2, x_3 and x_4, $b \in [15.425, 27]$, $a = 50$, $c = 13$, $d = 8$, $e = 33$ and $f = 30$. The hyperchaotic system can change in a large range of Lyapunov exponents space. In summary, there are two initial conditions in the process of the scrambling of the fractional-order Henon chaotic system. In the diffusion process, there are four initial conditions and six parameters the of hyper-chaos. If the accuracy of the computer is set as 10^{-15}, then the key space of the image encryption algorithm is $\left(10^{15}\right)^{12} \approx 2^{598} >> 2^{100}$ at least, which indicates that the key space of the algorithm is very large and can effectively resist exhaustive attack.

3.2.2. Key Sensitivity Analysis

Key sensitivity is an important index for security analysis of the encryption algorithms. Key sensitivity refers to that when the key changes slightly, the encrypted image will change greatly, that is to say, the small change of the key will make it impossible to carry out the decryption process correctly. In the design process of this encryption algorithm, the initial values and parameters of the system are usually associated with the pixels of the plaintext image, which can make the key sensitive and resist the known plaintext attack and the selective plaintext attack. In order to test the key sensitivity of this encryption algorithm, the value of each key makes minor changes, at the same time, keep the other key the same as the original key, then the modified key is used to decrypt the same cipher text image. Here, choose the initial condition $x_1 = 0.12$, at the same time, the rest of the initial conditions and control parameters are fixed, then change the initial condition $x_1' = 0.12 + 10^{-15}$ to decrypt. The contrast figures before and after encryption are shown in Figure 10. It can be seen from

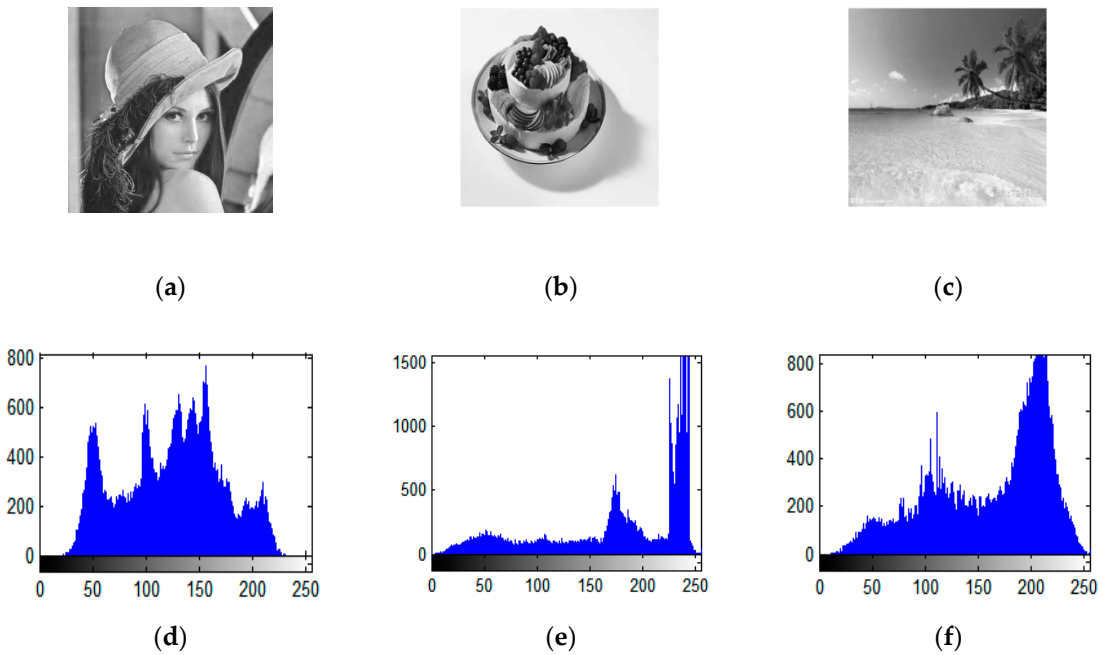
figure (b) that the correct decryption image cannot be obtained after the change of the initial condition by 10^{-15}. Therefore, the encryption algorithm has strong key sensitivity.

(**a**) (**b**)

Figure 10. The key sensitivity test: (**a**) The decrypted Lena image, using the correct initial key with initial condition $x_1 = 0.12$; (**b**) The decrypted Lena image, using the wrong initial key with initial condition $x_1' = 0.12 + 10^{-15}$.

3.2.3. Histogram Analysis

Histogram is an image that shows the distribution of each pixel value in the image by plotting the number of the pixels of each gray level in the image. The histogram distribution before encryption should be uneven, and the histogram after encryption should be flat and evenly distributed. The histograms of the encryption algorithm are shown in Figure 11. It can be seen that the histograms after several rounds of encryption are very flat and uniform, indicating that the encryption algorithm can hide the plaintext image information well.



(**a**) (**b**) (**c**)

(**d**) (**e**) (**f**)

Figure 11. *Cont.*

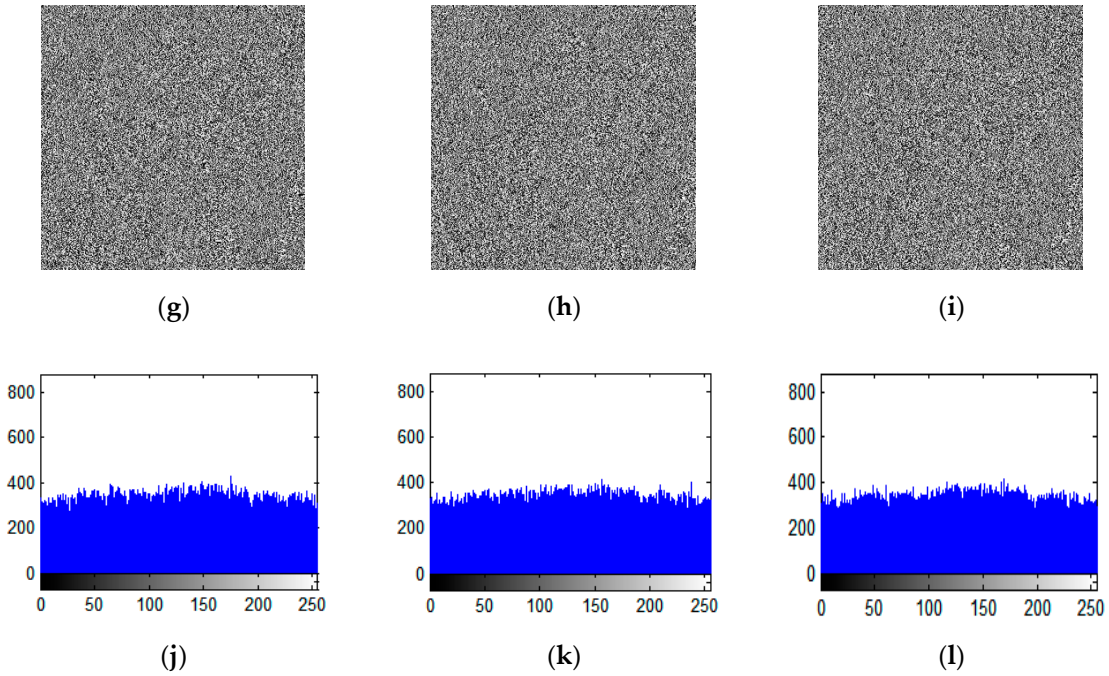


Figure 11. The histogram comparison tests before and after encryption: (**a**) The original Lena image; (**b**) The original Cake image; (**c**) The original Waterfront image; (**d**) The histogram of the Lena image; (**e**) The histogram of the Cake image; (**f**) The histogram of the Waterfront image; (**g**) The encrypted Lena image; (**h**) The encrypted Cake image; (**i**) The encrypted Waterfront image; (**j**) The histogram of the Lena image after encryption; (**k**) The histogram of the Cake image after encryption; (**l**) The histogram of the Waterfront image after encryption.

3.2.4. Differential Attack Analysis

Plaintext sensitivity is a standard to measure the security performance of an encryption algorithm. Plaintext with good sensitivity can resist certain differential attacks. In general, if a small change in the plaintext image can cause more than half of the pixels in the ciphertext image to change, the differential attack can be judged invalid. The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) can be used to measure the sensitivity of an encryption algorithm [50]. NPCR can show the percentage of the number of different pixels in the two ciphered images to the total number of images, while UACI can show the ratio of the average pixel changes to the maximum pixel values of the two ciphered images. The two indicators are defined as follows:

$$\mathrm{NPCR} = \frac{\sum_{i,j} M(i,j)}{L_1 \times L_2} \times 100\%, \tag{10}$$

$$\mathrm{UACI} = \frac{1}{L_1 \times L_2} \sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \times 100\%, \tag{11}$$

Here, C_1 and C_2 are the values before and after the pixel changes of the same position, $C_1(i,j)$ and $C_2(i,j)$ represent the pixel intensity on point (i,j) of the image before and after the changes. 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 1. The results show that the NPCR values were close to 1 and the UACI values were close to 33.5%. It shows that the encryption effect can resist certain differential attacks.

Table 1. NPCR and UACI.

Image	NPCR	UACI%
Lena	0.9955	33.25
Cake	0.9951	33.21
Waterfront	0.9962	33.28
Ref [2]	0.9962	33.51
Ref [40]	0.9957	33.32

3.2.5. Correlation Coefficient Analysis

In general, the correlation between the adjacent pixels of the plaintext image is relatively strong, namely the gray value of one pixel of the plaintext image is very close to the gray value of the surrounding pixels. Therefore, attackers can often infer the surrounding pixels from one pixel. The ciphered image produced by a good encryption algorithm should be as irrelevant as possible between adjacent pixels.

The adjacent pixels of a digital image can be divided into four types according to the position relations: horizontal adjacent pixels, vertical adjacent pixels, diagonal adjacent pixels and anti-diagonal adjacent pixels. The correlation coefficient is a measure of the degree of the correlation between two pixels or variables, and its value is in the range of $[-1, 1]$. The correlation coefficient is the quotient of the co-variance and standard deviation between two variables. The formula of the correlation coefficient r_{xy} is shown as follows:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x) \times D(y)}}, \tag{12}$$

Here, $\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$, $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$.

The x and y are the pixel values of two different images, N represents the number of all pixels, $\operatorname{cov}(x, y)$ represents the covariance, $D(x)$ represents the variance of the variable x, and $E(x)$ represents the average value. The more the observed values of the variables are, the less affection of the correlation coefficient by sampling error is, 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 degree of the two variables is, and the closer the relationship between them is. $r_{xy} > 0$ represents the positive correlation, $r_{xy} < 0$ represents the negative correlation, and $r_{xy} = 0$ represents the zero correlation.

In this paper, Lena image and its encrypted image are selected as the observation data, and the sampling points are 10,000 pairs. The experimental data of correlation coefficient before and after image encryption are shown in Figures 12–14. The comparative analysis of the correlation coefficient data are listed in Table 2. It can be seen from the above figures and the table, the image before encryption has a high correlation with the correlation coefficient close to 1, while the image after encryption is close to 0, which indicates that the encryption scheme can resist statistical attack well.

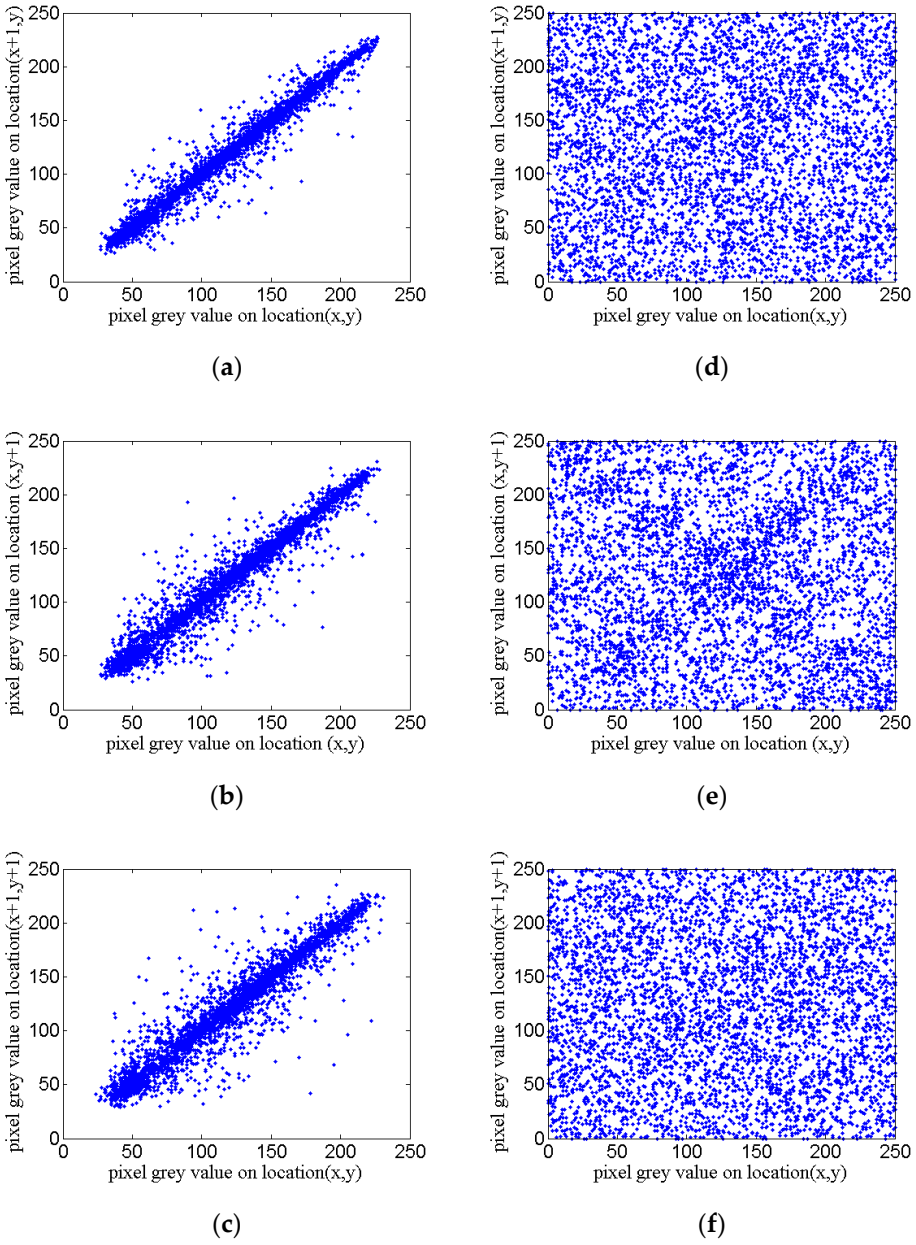


Figure 12. The comparison tests of correlation coefficient before and after Lena image encryption: (**a**) the horizontal correlation coefficient before encryption; (**b**) the vertical correlation coefficient before encryption; (**c**) the diagonal correlation coefficient before encryption; (**d**) the horizontal correlation coefficient after encryption; (**e**) the vertical correlation coefficient after encryption; (**f**) the diagonal correlation coefficient after encryption.

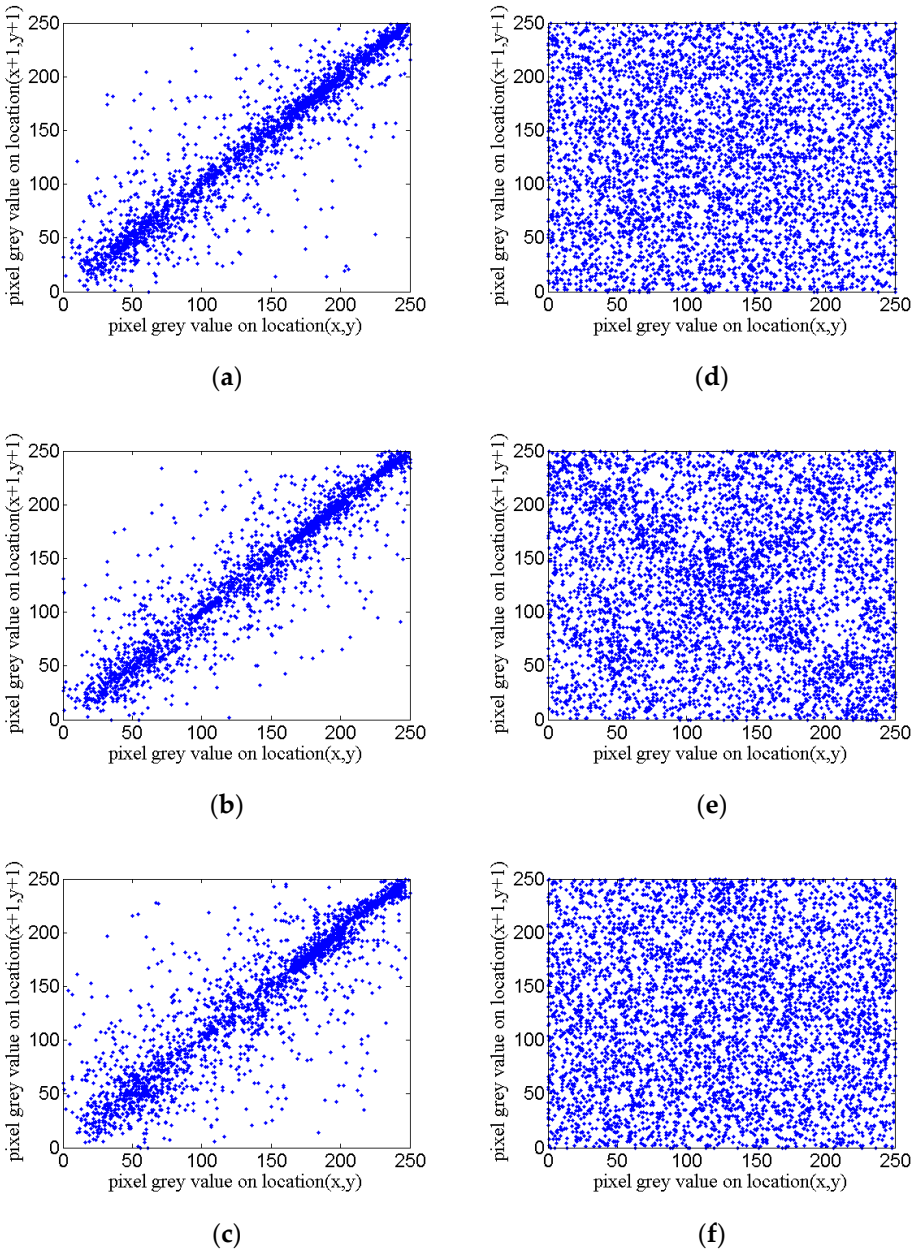


Figure 13. The comparison tests of correlation coefficient before and after cake image encryption: (**a**) the horizontal correlation coefficient before encryption; (**b**) the vertical correlation coefficient before encryption; (**c**) the diagonal correlation coefficient before encryption; (**d**) the horizontal correlation coefficient after encryption; (**e**) the vertical correlation coefficient after encryption; (**f**) the diagonal correlation coefficient after encryption.

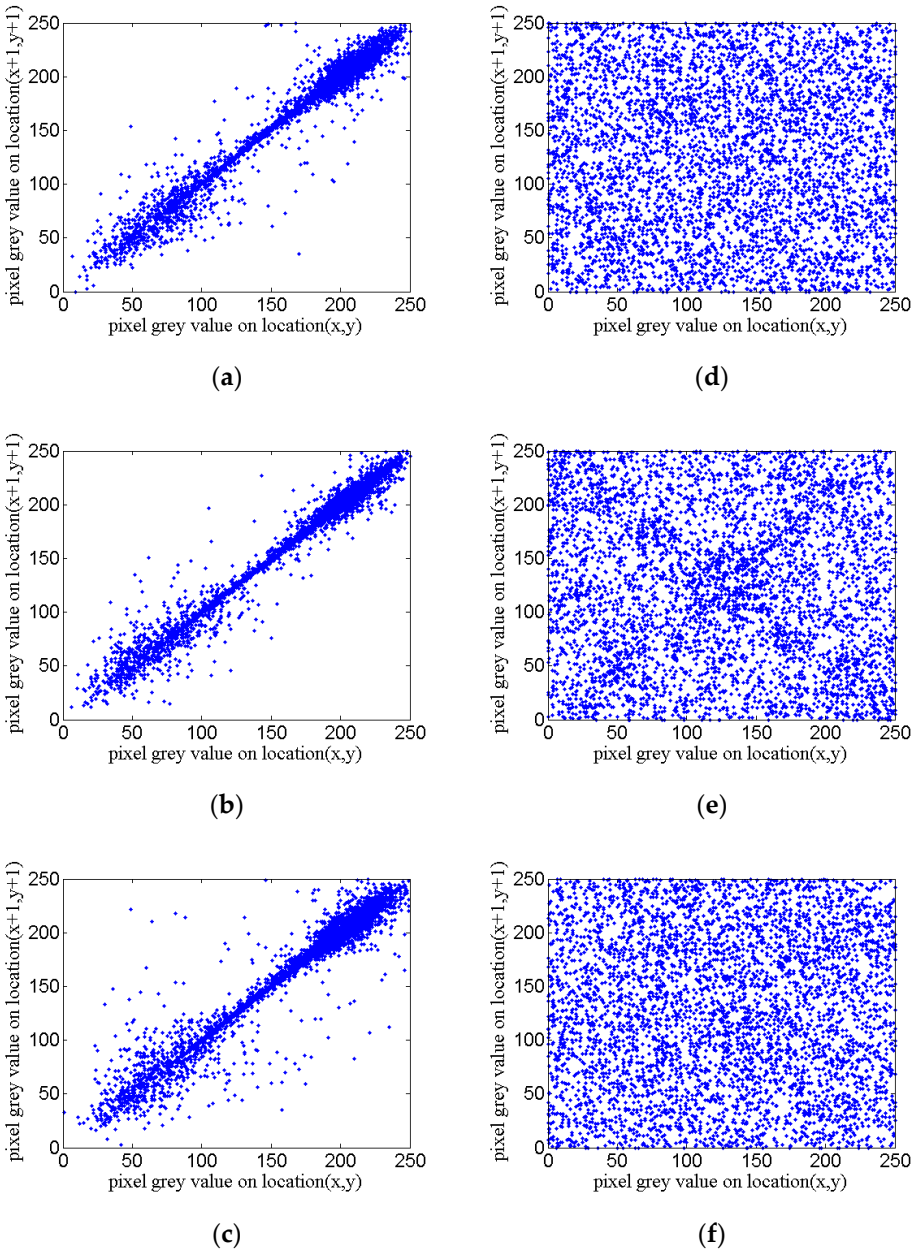


Figure 14. The comparison tests of correlation coefficient before and after waterfront image encryption: (**a**) the horizontal correlation coefficient before encryption; (**b**) the vertical correlation coefficient before encryption; (**c**) the diagonal correlation coefficient before encryption; (**d**) the horizontal correlation coefficient after encryption; (**e**) the vertical correlation coefficient after encryption; (**f**) the diagonal correlation coefficient after encryption.

Table 2. Correlation Coefficient Analysis.

Direction	Horizontal	Vertical	Diagonal
Lena before encryption	0.9863	0.9153	0.9214
Lena after encryption	−0.0082	−0.0059	0.0007
Cake before encryption	0.6153	0.6084	0.1729
Cake after encryption	0.0067	0.0053	0.0004
Waterfront before encryption	0.9796	0.6248	0.1705
Waterfront after encryption	−0.0067	0.0098	0.0001
[2] before encryption	0.9494	0.9667	0.9366
[2] after encryption	−0.0041	0.0023	0.0040
[40] before encryption	0.9494	0.9667	0.9366
[40] after encryption	0.0054	0.0035	0.0016
[46] before encryption	0.9577	0.9440	0.9126
[46] after encryption	−0.0082	0.0027	0.0030
[47] before encryption	0.9144	0.9545	0.9562
[47] after encryption	−0.0014	0.0028	0.0080

3.2.6. Information Entropy Analysis

Information entropy can be used to measure the distribution uncertainty of the gray value of the random distribution in the image. The better the randomness is, the greater the value of information entropy will be. The formula of the information entropy is shown as follows:

$$H(m) = \sum_{i=1}^{N} p(m_i) \times \log \frac{1}{p(m_i)}. \tag{13}$$

Here, $p(m_i)$ represents the occurrence probability of the symbol m_i, and N represents the total number of m_i. Since the states of 256 grayscale image can reach to 2^8, the maximum value of information entropy $H(m)$ can be 8. In this paper, the information entropy of the above three kinds of images are calculated and compared, which are shown in Table 3.

Table 3. Information Entropy Value.

Image	Information Entropy
Lena after encryption	7.9895
Cake after encryption	7.9886
Waterfront after encryption	7.9890
Ref [2]	7.9972
Ref [40]	7.9971
Ref [46]	7.9971
Ref [48]	7.9851

3.2.7. The Analysis of Plaintext Attack and Ciphertext Attack

The known plaintext attack, the ciphertext only attack, the chosen plaintext attack and the chosen ciphertext attack are four powerful types of attacks to measure image encryption algorithms. Among them, the chosen plaintext attack is the most powerful attack in the four attacks. Therefore, if an image encryption algorithm can resist the chosen plaintext attacks, it is considered that it also has the ability to resist the known plaintext attacks, the ciphertext only attacks and the chosen ciphertext attacks. In the differential attack analysis part, any small change in the image will lead to a completely different encrypted image, so it can be seen that the encryption algorithm in this paper has the ability to resist the differential attack, and it is known that the differential attack is a typical plaintext attack. The encryption algorithm, firstly uses the time-frequency domain exchange of DWT, and secondly uses the 2D fractional order chaotic system in the confusion stage, then at last uses the 4D hyper-chaos

in the diffusion stage with six parameters and four initial conditions, which has very large positive Lyapunov exponents, so it can output good random chaotic sequences. It can be seen that the final encrypted images are similar to the noise, and the histogram tests are also close to uniform distribution. Therefore, the image encryption algorithm proposed here has the ability to resist plaintext attack and ciphertext attack.

3.2.8. Analysis of Noise Attack

Anti-noise attack ability can be used to measure the anti-interference ability of an image encryption algorithm. When the plaintext image is encrypted and transmitted through the channel, it will be changed due to the noise attack. As a result, the image received at the receiving end cannot be decrypted correctly due to the noise added. Here, in order to test the anti-noise attack ability of the image encryption algorithm, the encrypted image is mixed with pepper and salt noise of different intensities, and then decrypted with the correct key. The images encrypted and decrypted by pepper and salt noise are shown in Figure 15. Through comparison and analysis, it can be known that the image encryption algorithm has a good ability to resist noise attack.

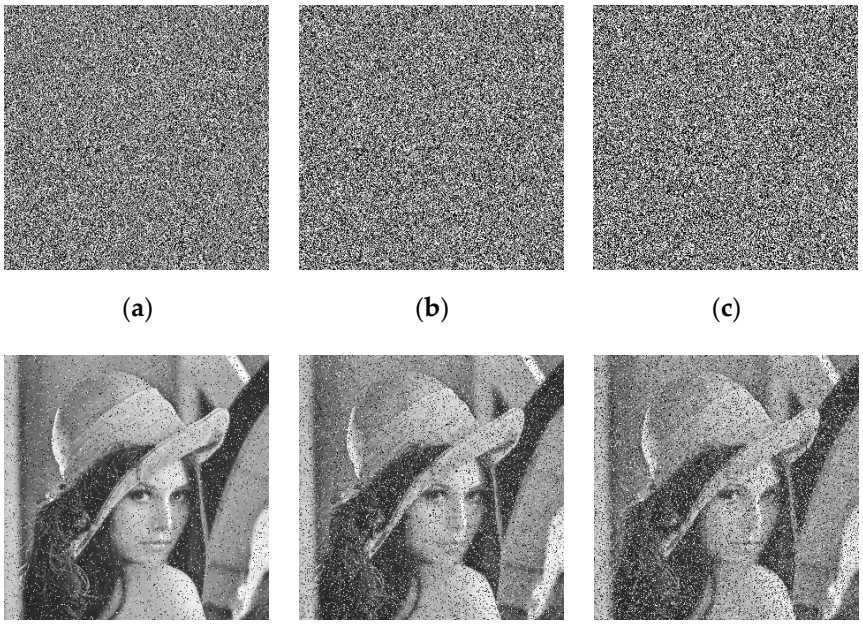


Figure 15. The ciphered images added by different levels of noises and the related decrypted images: (**a**) the ciphered image with noise intensity 0.1; (**b**) the ciphered image with noise intensity 0.2; (**c**) the ciphered image with noise intensity 0.3; (**d**) the decrypted image with noise intensity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

3.2.9. The Encryption Time Efficiency Analysis (Seconds)

The encryption time efficiency is an important index to measure the performance of an encryption algorithm. The time efficiency analysis results of this encryption algorithm at different resolutions are shown in Table 4. It can be seen from Table 4 that the encryption time will increase slightly with increasing resolution of Lena image.

Table 4. The Encryption Time Efficiency Analysis (Seconds).

Image	Time (s)
Lena 256×256	0.54
Lena 512×512	1.02
Lena 1024×1024	1.98

4. Conclusions

In this paper, a novel image encryption algorithm is proposed. The 2D DWT, the fractional-order Henon chaotic map and the 4D hyper-chaotic system are applied in the encryption. The original image is converted to the time-frequency domain by 2D DWT, and the transformed image is shuffled with the fractional-order Henon chaotic time series. Finally, the fully shuffled image is diffused and encrypted by the 4D hyperchaotic system. The whole image encryption process can achieve the time-frequency domain transformation and high-low dimensional chaotic systems hybrid encryption processes, so that the encryption effect of the algorithm is better than the ordinary chaotic encryption algorithms, and has a larger key space and a higher security. Based on the analysis of histogram, correlation coefficient, information entropy, key space, key sensitivity, differential attack and noise attack, it can be seen that the encryption algorithm has good statistical characteristics and can resist typical attacks. To sum up, it can be seen that the image encryption scheme can achieve a good encryption effect and a high security.

Author Contributions: L.D. conceived and wrote the paper. Q.D. gave some theoretical guidance. All authors have read and approved the final manuscript.

Funding: This work was supported by the Natural Science Foundation of China (No.61471158).

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

Abbreviations

1D	One-dimensional
2D	Two-dimensional
3D	Three-dimensional
4D	Four-dimensional
5D	Five-dimensional
7D	seven-dimensional
DNA	Deoxyribonucleic Acid
RGB	Red Green Blue
SPIHT	Set partitioning in Hierarchical Trees
FOC	Fractional-order Calculus
LH	Low-High
HL	High-Low
HH	High-High
LL	Low-Low
NPCR	Number of Pixels Change Rate
UACI	Unified Average Changing Intensity

References

1. Wu, Y.; Yang, G.; Jin, H.; Noonan, J.P. Image encryption using the two-dimensional logistic chaotic map. *J. Electron. Imaging* **2012**, *21*, 013014. [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. *Inform. Sci.* **2020**, *507*, 16–36. [CrossRef]
4. Wang, X.; Feng, L.; Zhao, H. Fast image encryption algorithm based on parallel computing system. *Inform. Sci.* **2019**, *486*, 340–358. [CrossRef]

5. Li, T.Y.; Shi, J.Y.; Li, X.S.; 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]
6. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image Vis. Comput.* **2006**, *24*, 926–934. [CrossRef]
7. Boriga, R.; Dascalescu, A.C.; Diaconu, A.V. A new one dimensional chaotic map and its use in a novel real-time image encryption scheme. *Adv. Multimed.* **2014**, *2014*, 409586. [CrossRef]
8. 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]
9. Ye, G.D.; Huang, X.L. An efficient symmetric image encryption algorithm based on an intertwining logistic map. *Neurocomputing* **2017**, *251*, 45–53. [CrossRef]
10. Sheela, S.J. Image encryption based on modifified Henon map using hybrid chaotic shift transform. *Multimed. Tools Appl.* **2018**, *77*, 25223–25251. [CrossRef]
11. Fridrich, J. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurcat. Chaos* **1998**, *8*, 1259–1284. [CrossRef]
12. Mandal, M.K. Symmetric key image encryption using chaotic Rossler system. *Secur. Commun. Netw.* **2014**, *7*, 2145–2152. [CrossRef]
13. Girdhar, A. A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences. *Multimed. Tools Appl.* **2018**, *77*, 27017–27039. [CrossRef]
14. Freud, S. On the Inflfluence of the Coupling Strength among Chua's Circuits on the Structure of Their Hyper-Chaotic Attractors. *Int. J. Bifurcat. Chaos* **2016**, *26*, 1650115. [CrossRef]
15. 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]
16. 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]
17. 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 Fract.* **2018**, *116*, 316–331. [CrossRef]
18. 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**, *32*, 31. [CrossRef]
19. Norouzi, B.; Mirzakuchaki, S.; Seyedzadeh, S.M.; Mosavi, M.R. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimed. Tools Appl.* **2014**, *71*, 1469–1497. [CrossRef]
20. Yuan, H.M.; Liu, Y.; Lin, T.; Hu, T.; Gong, L.H. A new parallel image cryptosystem based on 5D hyper-chaotic system. *Signal. Process. Image* **2017**, *52*, 87–96. [CrossRef]
21. Sun, S.; Guo, Y.; Wu, R. A Novel Image Encryption Scheme Based on 7D Hyperchaotic System and Row-column Simultaneous Swapping. *IEEE Access* **2019**, *7*, 28539–28547. [CrossRef]
22. 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] [PubMed]
23. Wang, L.Y.; Cheng, H. Pseudo-Random Number Generator Based on Logistic Chaotic System. *Entropy* **2019**, *21*, 960. [CrossRef]
24. Rubens, R. Quantum-chaotic key distribution in optical networks: From secrecy to implementation with logistic map. *Quantum Inform. Process.* **2018**, *17*, 329.
25. Garcia-Bosque, M.; Diez-Senorans, G.; Perez-Resa, A.; Sanchez-Azqueta, C.; Aldea, C.; Celma, S. 1 Gbps Chaos-Based Stream Cipher Implemented in 0.18 mu m CMOS Technology. *Electronics* **2019**, *8*, 623. [CrossRef]
26. Roy, A. Audio signal encryption using chaotic Henon map and lifting wavelet transforms. *Eur. Phys. J.* **2017**, *132*, 524. [CrossRef]
27. 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]
28. Jamal, R.K. Secure Communication Coupled Laser Based on Chaotic Rossler Circuits. *Quantum Opt.* **2019**, *51*, 79–91. [CrossRef]
29. Karimov, T.; Butusov, D.; Andreev, V.; Karimov, A.; Tutueva, A. Accurate Synchronization of Digital and Analog Chaotic Systems by Parameters Re-Identification. *Electronics* **2018**, *7*, 123. [CrossRef]
30. Mishra, J. Modifified Chua chaotic attractor with diffffferential operators with non-singular kernels. *Chaos Solitons Fract.* **2019**, *125*, 64–72. [CrossRef]

31. 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]
32. Sathiyamurthi, P.; Ramakrishnan, S. Testing and Analysis of Chen Chaotic Mapping for Speech Cryptography. *J. Test. Eval.* **2019**, *47*, 3028–3040. [CrossRef]
33. 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]
34. Ozkaynak, F.; Celik, V.; Ozer, A.B. A new S-box construction method based on the fractional-order chaotic Chen system. *Signal. Image Video Process.* **2017**, *11*, 659–664. [CrossRef]
35. Podlubny, I.; Petras, I.; Vinagre, B.M.; Dorcak, L. Analogue realizations of fractional-order controllers. *Nonlinear Dynam.* **2002**, *29*, 281–296. [CrossRef]
36. Wang, Z.; Huang, X.; Li, Y.X.; Song, X.N. A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system. *Chin. Phys. B* **2013**, *22*, 010504. [CrossRef]
37. Zhao, J.; Wang, S.; Chang, Y.; Li, X. A novel image encryption scheme based on an improper fractional-order chaotic system. *Nonlinear Dynam.* **2015**, *80*, 1721–1729. [CrossRef]
38. Huang, X.; Sun, T.; Li, Y.; Liang, J. A color image encryption algorithm based on a fractional-order hyperchaotic system. *Entropy* **2014**, *17*, 28–38. [CrossRef]
39. Landir, M.; Hamiche, H.; Kassim, S. A novel robust compression-encryption of images based on SPIHT coding and fractional-order discrete-time chaotic system. *Opt. Laser Technol.* **2019**, *109*, 534–546.
40. 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]
41. Vaish, A.; Kumar, M. Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain. *OPTIK* **2017**, *145*, 273–283. [CrossRef]
42. Shaheen, A.M.; Sheltami, T.R.; Al-Kharoubi, T.M.; Shakshuki, E. Digital image encryption techniques for wireless sensor networks using image transformation methods: DCT and DWT. *J. Ambient Intell. Hum. Comp.* **2019**, *10*, 4733–4750. [CrossRef]
43. Wu, X.J.; Wang, D.W.; Kurths, J.; Kan, H.B. A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Inform. Sci.* **2016**, *349*, 137–153. [CrossRef]
44. Atici, F.M.; Eloe, P.W. Initial Value Problems in Discrete Fractional Calculus. *Proc. Am. Math. Soc.* **2009**, *137*, 981–989. [CrossRef]
45. Abdeljawad, T. On Riemann and Caputo fractional differences. *Comput. Math. Appl.* **2011**, *62*, 1602–1611. [CrossRef]
46. Hu, T.C. Discrete Chaos in Fractional Henon Map. *Appl. Math.* **2014**, *5*, 2243–2248. [CrossRef]
47. Qi, G.Y.; Wyk, M.A.; Wyk, B.J.; Chen, G.R. On a new hyperchaotic system. *Phys. Lett. A* **2008**, *372*, 124–136. [CrossRef]
48. Stinson, D.R. *Cryptography: Theory and Practice*; CRC Press: Boca Raton, FL, USA, 2005.
49. 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]
50. Zhan, K.; Wei, D.; Shi, J.; Yu, J. Cross-utilizing hyperchaotic and DNA sequences for image encryption. *J. Electron. Imaging* **2017**, *26*, 013021. [CrossRef]