Hindawi
Complexity
Volume 2017, Article ID 9010251, 13 pages
https://doi.org/10.1155/2017/9010251

Research Article

A Novel Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System and DNA Computing

Taiyong Li,[1,2,3,4] Minggao Yang,[1] Jiang Wu,[1] and Xin Jing[1]

[1] *School of Economic Information Engineering, Southwestern University of Finance and Economics, 55 Guanghuacun Street, Chengdu 610074, China*
[2] *Collaborative Innovation Center for the Innovation and Regulation of Internet-Based Finance, Southwestern University of Finance and Economics, 55 Guanghuacun Street, Chengdu 610074, China*
[3] *Laboratory for Financial Intelligence and Financial Engineering, Southwestern University of Finance and Economics, 55 Guanghuacun Street, Chengdu 610074, China*
[4] *Institute of Chinese Payment System, Southwestern University of Finance and Economics, 55 Guanghuacun Street, Chengdu 610074, China*

Correspondence should be addressed to Taiyong Li; litaiyong@gmail.com

Received 20 July 2017; Accepted 12 October 2017; Published 23 November 2017

Academic Editor: Ahmed Elsaid

In the era of the Internet, image encryption plays an important role in information security. Chaotic systems and DNA operations have been proven to be powerful for image encryption. To further enhance the security of image, in this paper, we propose a novel algorithm that combines the fractional-order hyperchaotic Lorenz system and DNA computing (FOHCLDNA) for image encryption. Specifically, the algorithm consists of four parts: firstly, we use a fractional-order hyperchaotic Lorenz system to generate a pseudorandom sequence that will be utilized during the whole encryption process; secondly, a simple but effective diffusion scheme is performed to spread the little change in one pixel to all the other pixels; thirdly, the plain image is encoded by DNA rules and corresponding DNA operations are performed; finally, global permutation and 2D and 3D permutation are performed on pixels, bits, and acid bases. The extensive experimental results on eight publicly available testing images demonstrate that the encryption algorithm can achieve state-of-the-art performance in terms of security and robustness when compared with some existing methods, showing that the FOHCLDNA is promising for image encryption.

1. Introduction

Images, as one of the most popular media types, are widespread over various networks. How to prevent images from illegal copying and distribution in the era of the Internet is a critical issue. Therefore, image encryption has become one of the hottest research topics of information security in recent years. Although there exist some classical schemes such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA) for information security [1], they usually cannot be directly applied to image encryption to yield satisfactory results due to some intrinsic properties of images such as bulky data capacity, strong correlation, and high redundancy [2–4]. In contrast, the chaos-based image encryption has attracted much attention for research purposes and has been demonstrated to be effective and secure in recent years [5–9].

Chaotic systems have the following properties: pseudorandomness, extreme sensitivity to the initial values and system parameters, ergodicity, and unpredictability, which make it very suitable for image encryption [10]. Typically, chaos-based image encryption framework includes chaotic sequence generation, pixel position permutation, and pixel value diffusion. One-dimensional (1D) chaotic systems have simple forms and are easy to implement, and thus some researchers used them to encrypt images. For example, the authors used two 1D chaotic Logistic maps to generate the pseudorandom sequence for image encryption in [11]. Boriga et al. presented a new 1D chaotic map for real-time

image encryption [12]. However, since the 1D chaotic systems usually have only one variable and a few parameters, along with relatively simple structures and chaotic orbits, it is easy to estimate the orbits and to predict the initial values and/or parameters by little information extracted from them [13]. Therefore, in order to improve the security of image encryption, chaotic systems with two or more dimensions have been applied to image encryption. Fridrich put forward symmetric ciphers with two-dimensional (2D) chaotic maps and the experimental results demonstrated good diffusion properties with respect to the key and the plain image [14]. Hua et al. proposed an image encryption algorithm using 2D Sine Logistic modulation map that has better properties of chaos when compared with some existing chaotic systems [15]. Using the chaotic three-dimensional (3D) cat map extended from 2D Arnold's cat map [16] and 3D Chen's chaotic system [17], Chen et al. proposed a symmetric image encryption scheme for alternative permutation and diffusion [5]. The Lyapunov exponent (LE) is a type of measurement methodology for chaotic level, and a chaotic system is said to be hyperchaotic if it has two or more positive LEs [18]. Since hyperchaotic systems have more advantages such as richer dynamic phenomena and higher randomness than common chaotic systems, lots of hyperchaotic systems have been employed to encrypt images [19–23]. For example, Norouzi et al. used the key stream generated by a hyperchaotic system to perform one round diffusion on the image to attain good results [20]. A novel image encryption algorithm based on genetic recombination and hyperchaotic Lorenz system was put forward by Wang and Zhang [21]. Yuan et al. proposed a parallel image cryptosystem by combining the Logistic map and a five-dimensional (5D) hyperchaotic system [23].

Most of the above-mentioned literature uses integral-order chaotic systems for image encryption. It has been reported that fractional-order hyperchaotic systems, as a counterpart of integral-order chaos, show higher nonlinearity and degrees owing to the complex geometrical interpretation of fractional derivatives for the nonlocal effects either in time or in space [24, 25]. Therefore, the fractional-order hyperchaotic systems have great potential in information security. Wang et al. applied the fractional-order hyperchaotic Lorenz system to color image encryption. To enhance the security of images, both system parameters and derivative order were embedded in the scheme [25]. The 3D fractional-order Lorenz system and Chen chaotic systems were employed to encrypt images by Wu et al. and Zhao et al., respectively [3, 26]. Huang et al. used a four-dimensional (4D) fractional-order hyperchaotic neural network system to cipher color images, and the experiments demonstrated the effectiveness of the system [27].

Most image encryption algorithms are performed on pixel-level or bit-level data. With the development of bioinformatics, some image encryption algorithms based on deoxyribonucleic acid (DNA) have emerged since Adleman completed the first experiment on DNA computing [28], due to the properties of DNA: massive parallelism, huge storage, and ultralow power consumption [29–34]. Typically, DNA-based image encryption consists of three steps: DNA encoding, DNA operations, and DNA decoding. The bit stream of images is encoded as DNA sequences with some encoding rules in the step of DNA encoding. Then, different DNA operations such as addition, subtraction, and exclusive OR (XOR) are performed on DNA. The types of both encoding and operations are usually determined by chaotic sequences. Finally, the results of DNA operations are decoded to bits with the counterpart of corresponding encoding rules. Zhang et al. used Logistic maps and two DNA operations (addition and complement) to encrypt image blocks, but the blocks led to low robustness against noise [33]. In the RGB image encryption scheme by Liu et al., DNA addition and complement operations were carried out on each channel of RGB image with the DNA sequence matrix generated from Logistic map [34]. Zhan et al. jointly used a hyperchaotic system and DNA computing to encrypt images, where the hyperchaotic sequence was applied to all steps. However, two important evaluation standards, that is, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI), still need to be improved [29].

Motivated by the above analysis, this paper aims at proposing a novel image encryption algorithm that incorporates the fractional-order hyperchaotic Lorenz (FOHCL) system and fractional-order hyperchaotic Lorenz DNA (FOHCLDNA) computing in order to improve the security of image encryption. Specifically, the proposed FOHCLDNA is mainly composed of six stages: (1) the FOHCL is firstly applied to generating the pseudorandom sequence for encryption; (2) global pixel diffusion, global pixel permutation, and 2D permutation are carried out on pixels; (3) global bit permutation and 3D permutation are conducted on bits; (4) the bit stream of image is encoded as DNA sequence according to the encoding rules decided by the hyperchaotic sequence; (5) one of the DNA operations (addition, subtraction, or XOR) is carried out on each acid base, and, at the same time, global DNA permutation and 3D permutation further improve the security. Both the types of DNA operations and the orders of DNA permutation are determined by the hyperchaotic sequence; (6) the encrypted DNA sequence is decoded to bit stream, followed by bit-to-pixel decoding. Finally, the encrypted image is obtained. The main contributions of this paper are four aspects: (1) different from most existing literature that uses integral-order chaotic or hyperchaotic systems, the proposed FOHCLDNA uses a fractional-order hyperchaotic system for image encryption; (2) a simple but effective pixel diffusion is proposed; (3) permutation is carried out at different levels, that is, pixels, bits, and acid bases, while both the DNA encoding rule and DNA operation for each acid base are determined by corresponding hyperchaotic sequence; (4) extensive experiments demonstrate that the FOHCLDNA is promising for image encryption. The novelty of this paper is threefold: (1) it is a good attempt to integrate fractional-order hyperchaotic system and DNA computing to enhance the security of image encryption; (2) the simple pixel diffusion can spread the little change in one pixel to all other pixels; (3) several permutation operations performed at different levels can further improve the security.

The remainder of this paper is organized as follows. A brief description of the fractional-order hyperchaotic

Table 1: Encoding and decoding rules of DNA.

Rule	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

system and DNA computing is given in Section 2. In Section 3, we propose the novel image encryption algorithm (FOHCLDNA) in detail. Experimental results, analysis, and comparison are presented in Section 4. Concluding remarks of the FOHCLDNA are summarized in Section 5.

2. Related Work

2.1. Fractional-Order Hyperchaotic Lorenz System. The Lorenz systems and their variants are among the most popular chaotic/hyperchaotic systems in image encryption. The fractional-order hyperchaotic Lorenz (FOHCL) system shows good complex dynamics [35, 36], and some previous research has demonstrated its power in image encryption [25, 37, 38]. Therefore, in this paper, we use a four-dimensional FOHCL system to generate the chaotic sequence that the algorithm needs [25, 35]. The FOHCL can be described as follows:

$$\begin{aligned}
\frac{d^{q1}x_1}{dt^{q1}} &= \alpha\left(x_2 - x_1\right) + x_4,\\
\frac{d^{q2}x_2}{dt^{q2}} &= \gamma x_1 - x_2 - x_1 x_3,\\
\frac{d^{q3}x_3}{dt^{q3}} &= x_1 x_2 - \beta x_3,\\
\frac{d^{q4}x_4}{dt^{q4}} &= -x_2 x_3 + \phi x_4,
\end{aligned} \tag{1}$$

where α, β, γ, ϕ, and q_i $(i = 1, 2, 3, 4)$ are the system parameters. When $\alpha = 10$, $\beta = 8/3$, $\gamma = 28$, $\phi = -1$, $q_i = 0.98$ $(i = 1, 2, 3, 4)$, and the initial values $x_1^0 = 12$, $x_2^0 = 22$, $x_3^0 = 31$, and $x_4^0 = 4$, the system exhibits a hyperchaotic behavior with 2 positive values among all the 4 Lyapunov exponents ($\lambda_1 = 0.3362$, $\lambda_2 = 0.1568$, $\lambda_3 = 0$, and $\lambda_4 = -15.1724$) [35]. Figure 1 shows the attractor of the FOHCL system.

2.2. Deoxyribonucleic Acid (DNA) Computing. Deoxyribonucleic acid (DNA) is a kind of biological macromolecule, and the knowledge of DNA sequence is widely used in genetic engineering, biotechnology, and identification. An individual DNA sequence is mainly composed of carbohydrate and four different nucleic acid bases: A (Adenine), G (Guanine), C (Cytosine), and T (Thymine), where T and A; C and G are complementary pairs. The number of DNA coding combinations is 4! = 24 in total, which only have eight kinds of DNA bases legally to meet the DNA complementary rules, as shown in Table 1 [29, 39]. In the theory of binary system, 0 and 1 are complementary pairs such as 00 (0) and 11 (3), 01 (1) and 10 (2). Each pixel value of grayscale image in binary sequence is 8 bits, and if every 2 bits is represented by a letter, the representation of a pixel would be a 4-length nucleotide string. For example, for a pixel value 161 in decimal, its binary combination is "10010011," and the corresponding DNA sequence is "GCAT" by adopting the first encoding rule. If any other DNA coding rules are used to code the same binary sequence, the result will definitely be different.

Table 2: Addition (++) operation.

++	A	G	C	T
A	C	T	A	G
G	T	C	G	A
C	A	G	C	T
T	G	A	T	C

Table 3: Subtraction (−−) operation.

--	A	G	C	T
A	C	T	G	A
G	T	C	A	G
C	A	G	C	T
T	G	A	T	C

Table 4: XOR (⊗⊗) operation.

⊗⊗	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

With the encoding rules, the operations of addition (++), subtraction (−−), and XOR (⊗⊗) are listed in Tables 2–4.

3. Image Encryption Scheme

3.1. Hyperchaotic Sequence Generation. Since fractional-order hyperchaotic systems have good properties for image encryption, we use the FOHCL system described in Section 2.1 for generating the hyperchaotic sequence. The generating process is comprised of three steps.

Step 1. To eliminate the adverse effects, the FOHCL system is firstly iterated N_0 times and then the generated sequence is removed.

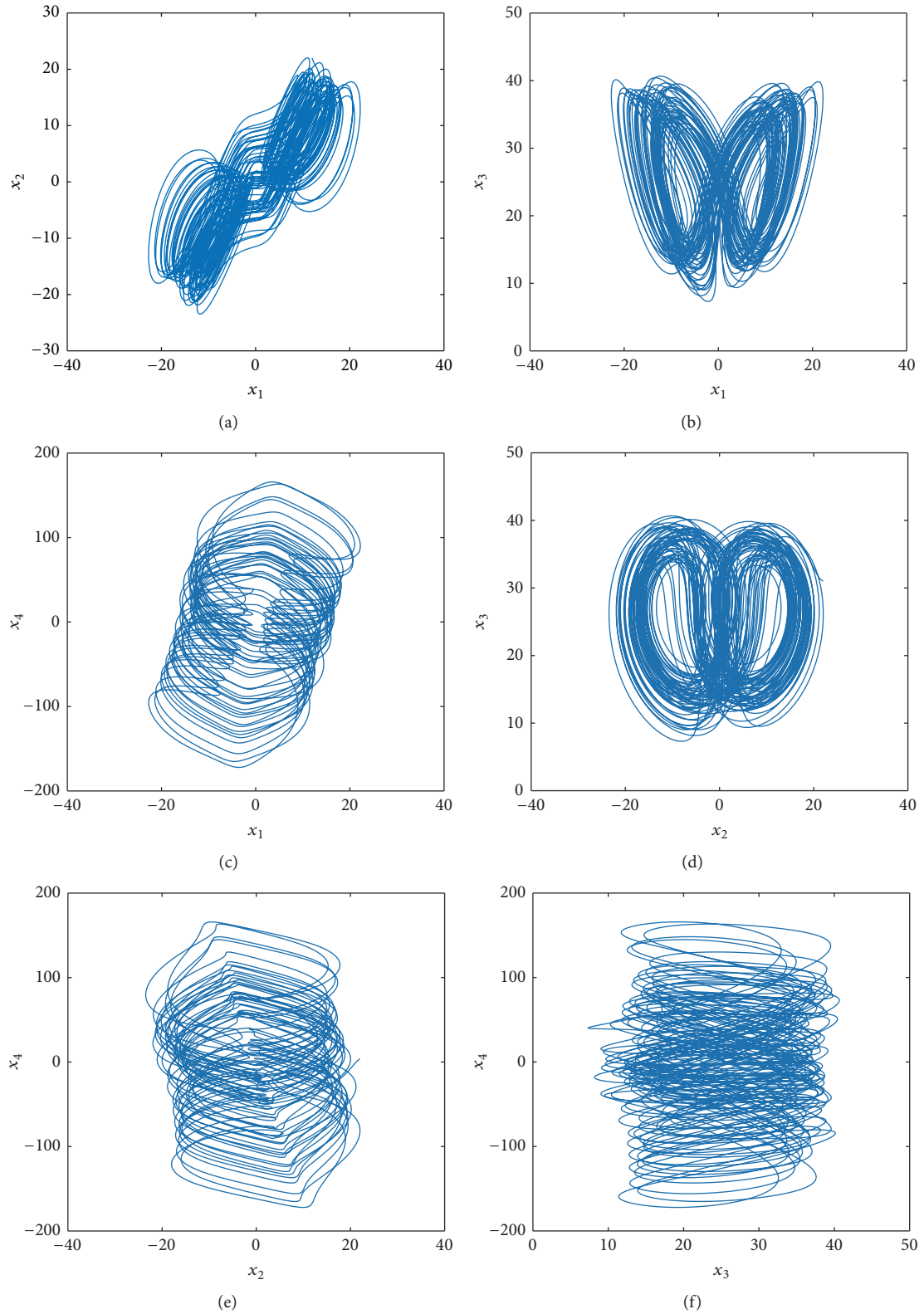

Figure 1: Phase diagrams of the fractional-order Lorenz hyperchaotic attractor. (a) x_1-x_2 plane, (b) x_1-x_3 plane, (c) x_1-x_4 plane, (d) x_2-x_3 plane, (e) x_2-x_4 plane, and (f) x_3-x_4 plane.

Step 2. The FOHCL system continues to iterate $N = \lceil (30hw + 3(h+w)+13)/4 \rceil$ times, where $\lceil \cdot \rceil$ denotes the ceiling operation and h and w denote the width (column) and the height (row) of the image to encrypt, respectively. For the jth iteration, four state values denoted by $s^j = \{x_1^j, x_2^j, x_3^j, x_4^j\}$ are obtained by (1).

Step 3. After the whole iteration, the fractional-order hyperchaotic sequences K can be obtained by concatenating all the s^j $(j = 1, 2, \ldots, N)$ as

$$\begin{aligned} K &= \left\{s^1, s^2, \ldots, s^N\right\} \\ &= \left\{x_1^1, x_2^1, x_3^1, x_4^1, \ldots, x_1^N, x_2^N, x_3^N, x_4^N\right\} \\ &= \left\{k^1, k^2, k^3, \ldots, k^{4N-2}, k^{4N-1}, k^{4N}\right\}. \end{aligned} \tag{2}$$

The purposes of the generated sequence K for encryption are two aspects: (1) sorting subsequence of K to get the index of original data for permutation; (2) using subsequence of K to change the values of images for diffusion. In our scheme, for the first purpose, we directly use the original values of K for sorting while, for the second purpose, we map the hyperchaotic subsequence of K with n values to the integer range of $[0, 255]$ by

$$S^i = \mathrm{mod}\left(\left\lfloor \mathrm{mod}\left(\left(\left|k^i\right| - \left\lfloor \left|k^i\right| \right\rfloor\right) \times 10^{15}, 10^8\right)\right\rfloor, 256\right), \quad i = 1, 2, 3, \ldots, n, \tag{3}$$

where S^i is the ith integer in the generated integer sequence, mod is the modulo operation, $|\cdot|$ is the absolute value operation, and $\lfloor \cdot \rfloor$ denotes flooring operation [29].

3.2. Global Pixel Diffusion. In our scheme, we carry out a simple two-step diffusion for image on pixels. Specifically, for a given image I of size $h \times w$, we can transform the image into a 1D pixel sequence $S = \{s^i\}$, $i = 1, 2, \ldots, L$, where $L = h \times w$. Suppose we have an initial key C^0 and a key sequence $K = \{k^i \in [0, 255]\}$, $i = 1, 2, \ldots, L$; the first-step diffusion can be described as follows:

$$\begin{aligned} D^1 &= s^1 \otimes \mathrm{mod}\left(C^0 + k^1, 256\right), \\ D^i &= s^i \otimes \mathrm{mod}\left(D^{i-1} + k^i, 256\right), \end{aligned} \tag{4}$$

and the second-step diffusion can be formulated as follows:

$$\begin{aligned} D^1 &= D^1 \otimes \mathrm{mod}\left(\left|D^L - k^1\right|, 256\right), \\ D^i &= D^i \otimes \mathrm{mod}\left(\left|D^{i-1} - k^i\right|, 256\right), \end{aligned} \tag{5}$$

and in both (4) and (5), $\otimes$ is XOR operation and D is the result of pixel diffusion.

3.3. Global Permutation and 2D and 3D Permutation. In this approach, several permutations are carried out at different levels, that is, pixel level, bit level, and DNA level. For an image of size $h \times w$, global pixel/bit/DNA permutation means permuting all pixels/bits/DNA with corresponding hyperchaotic subsequences. Since pixel-level data is a 2D plane of size $h \times w$, we can permute the image firstly by row and then by column, which is called 2D permutation. Bit-level and DNA-level data are a 3D cube of size $h \times w \times 8$ and $h \times w \times 4$, respectively, and we can permute the image by row, column, and depth, respectively, which is called 3D permutation in this paper. Specifically, the global permutation can be summarized as follows.

Step 1. Arrange the pixels/bits/acid bases into a 1D vector v with the length of $L = h \times w / h \times w \times 8 / h \times w \times 4$.

Step 2. Extract a subsequence with the length of L from the hyperchaotic sequence K. Sort the subsequence in ascending order to get the index sequence i^x, $x = 1, 2, \ldots, L$.

Step 3. According to i^x, rearrange the vector v to get the new vector v' by

$$v'_x = v_{i^x}, \quad x = 1, 2, \ldots, L. \tag{6}$$

The 3D permutation is to permute planes at different directions in 3D spaces. The operations in each direction are very similar. For simplicity, here we only give the operation in the direction of width as follows.

Step 1. Extract a subsequence of length $L = h$ from the hyperchaotic sequence K. Sort the subsequence in ascending order to get the index sequence i^x, $x = 1, 2, \ldots, L$.

Step 2. According to i^x, rearrange the plane p to get the new vector p' by

$$p'_x = p_{i^x}, \quad x = 1, 2, \ldots, L. \tag{7}$$

It is clear that the 2D permutation is a special case of the 3D permutation. The proposed scheme extracts subsequence with $L = h + w$, $h + w + 8$, and $h + w + 4$ from K for 2D pixel permutation, 3D bit permutation, and 3D DNA permutation, respectively. Note that the proposed global permutation and 3D permutation at bit-level data or DNA-level data can change the positions of bits or DNAs to lead the values of pixels changed, and thus they can simultaneously permute and diffuse the images at bit-level or DNA-level data.

3.4. FOHCLDNA: The Proposed Image Encryption Scheme. With the above-mentioned description, the flowchart of the proposed FOHCLDNA is shown in Figure 2, and the details are as follows.

Step 1. Let $h \times w$ denote the size of the input image P. Concatenate the four sequences generated by (1) to compose one hyperchaotic sequence K using (2).

Step 2 (conduct pixel-level encryption). Extract the first $h+w$ items from K to carry out row and column permutation (2D permutation) on P to obtain P^0. Extract the next $h \times w$ items from K to carry out global pixel permutation on P^0 to obtain P^1. Extract the next $h \times w + 1$ items from K to compose a new

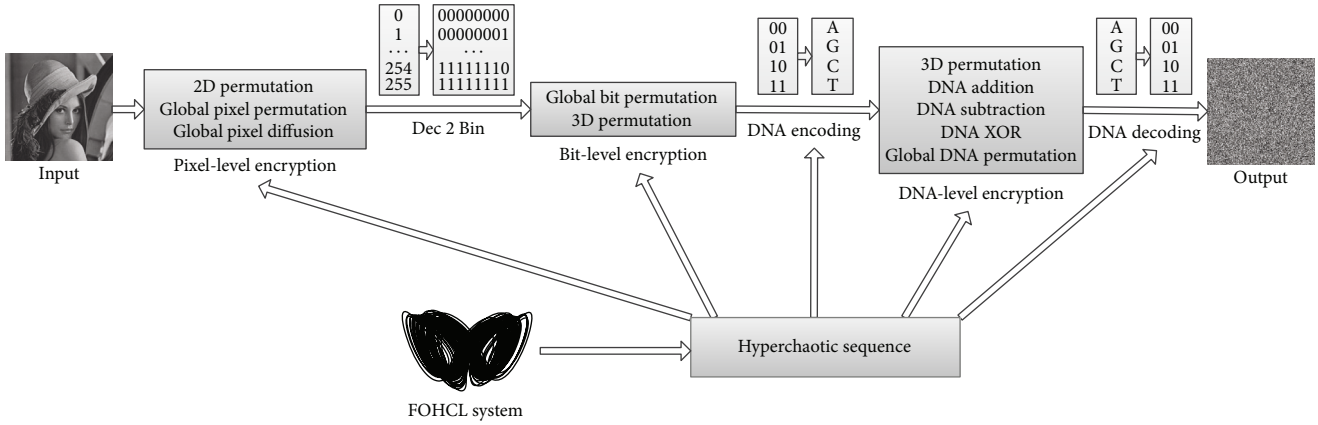

Figure 2: The flowchart of the proposed FOHCLDNA algorithm.

sequence S^0 and then map S^0 to the integer range of $[0, 255]$ by (3) to obtain sequence S^1. Use the first item in S^1 as the initial value and the rest as the key to carry out global pixel diffusion on P^1 to obtain P^2.

Step 3. P^2 is encoded to a bit sequence B^0.

Step 4 (conduct bit-level encryption). Use the next $h \times w \times 8$ items from K to perform global bit permutation on B^0 to obtain B^1. Use the next $h + w + 8$ items from K to perform 3D permutation on B^1 to obtain B^2.

Step 5 (DNA encoding). Map the next $h \times w \times 4$ items in K to the integer range of $[0, 255]$ by (3) to obtain sequence S^2. Encode the ith pair bits in B^2 with the DNA rule decided by (8) to obtain D^0:

$$\text{Rule} = \text{mod}\left(S_i^2, 8\right) + 1, \tag{8}$$

where S_i^2 denotes the ith item in the sequence S^2.

Step 6 (conduct DNA-level encryption). Use the next $h+w+4$ items from K to perform 3D permutation on D^0 to obtain D^1. Map the next $h \times w \times 4$ items in K to the integer range of $[0, 255]$ by (3) to obtain sequence S^3. Create a mask DNA matrix M of size $h \times w \times 4$ using the next $h \times w \times 4$ items in K. For the ith DNA in D^1, conduct DNA operation with ith DNA in M to obtain D^2. The operation type is decided by

$$\text{op} = \text{mod}\left(S_i^3, 3\right) + 1, \tag{9}$$

where op denotes the type of DNA operation. When op equals 1, 2, and 3, the corresponding DNA operation is $+$, $-$, and $\otimes$, respectively. Extract the next $h \times w \times 4$ items from K to carry out global DNA permutation on D^2 to obtain D^3.

Step 7 (DNA decoding). Map the next $h \times w \times 4$ items in K to the integer range of $[0, 255]$ by (3) to obtain sequence S^4. Decode the ith DNA in D^2 with the DNA rule decided by (10) to obtain a binary sequence B^3:

$$\text{Rule} = \text{mod}\left(S_i^4, 8\right) + 1. \tag{10}$$

Note that for a specified acid base, the encoding rule to generate it and the decoding rule to decode it may be different because of the difference between S^2 and S^4.

Step 8. The binary sequence B^3 is converted to the cipher image Q.

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

The proposed FOHCLDNA enhances the security of images in several aspects. Firstly, the hyperchaotic sequence with high nonlinearity and complex dynamics generated by the FOHCL is used throughout the process of image encryption. Secondly, the global pixel diffusion can spread little change in one pixel to all the other pixels, leading to a good result of diffusion. Thirdly, permutations are performed on different levels, that is, pixels, bits, and acid bases. Specially, for each two adjacent bits in a pixel and each acid base, a unique DNA rule determined by the hyperchaotic sequence is used to perform DNA encoding and DNA decoding, respectively. The operation type of each acid base is also decided by the sequence when the image is operated with the DNA mask image. All these properties enhance the security of images.

4. Experimental Results

4.1. Experimental Settings. In order to evaluate the performance of the proposed FOHCLDNA, we compare it with some state-of-the-art schemes, such as the hyperchaotic and DNA sequence-based method (HC-DNA) [29], the image encryption using cipher diffusion in crisscross pattern (CDCP) [40], and a class hyperchaos-based scheme (CHC) [41]. The parameters for the compared schemes are set as given by the authors. We set the parameters of the FOHCLDNA as follows. The initial values for the FOHCL system are $x_1^0 = 12$, $x_2^0 = 22$, $x_3^0 = 31$, and $x_4^0 = 4$. And

Table 5: Testing images.

Image	Size ($h \times w$)
Lena	256×256
Cameraman	256×256
Circuit	280×272
Peppers	512×512
Barbara	566×402
Bridge	512×512
Plane	512×512
Aerial	366×364

the preiterating times N_0 are set to 10000. All the fractional orders q_i, $i = (1, 2, 3, 4)$ are set to a fixed value 0.98.

Eight publicly accessed images with different sizes are used to test the proposed FOHCLDNA, as listed in Table 5.

All the experiments were conducted by Matlab 8.6 (Mathworks, Natick, MA, USA) on a 64-bit Windows 7 (Microsoft, Redmond, WA, USA) with 32 GB memory and 3.4 GHz I7 CPU.

4.2. Security Key Analysis. Key space and sensitivity to secret key are two essential points in encryption. A good encryption scheme should have an enough large key space and be extremely sensitive to any small changes in its security key. Both a large key space and extreme sensitivity can resist brute-force attacks.

4.2.1. Key Space. Basically, the security keys of the proposed FOHCLDNA are composed of 4 initial values, that is, $(x_1^0, x_2^0, x_3^0, x_4^0)$. If the precision of each initial value is 10^{-16}, the key space size is $10^{16\times4} = 10^{64} \approx 2^{212}$. From the view of cryptology, the size of the key space larger than 2^{100} is capable of providing a high-level security [1, 42]. Therefore, the key space of the FOHCLDNA is large enough to resist brute-force attacks from current computers. In addition, the fractional orders of the FOHCL can also be used as keys to further enhance the key space.

4.2.2. Sensitivity to Secret Key. The extreme sensitivity of an image encryption algorithm implies that even one bit changed in the keys will lead to a completely different encrypted image. In other words, if the security key changes a little, the decrypted image will be completely different from the input image.

To demonstrate the sensitivity to secret key of the FOHCLDNA, we decrypt the cipher images twice. In the first run, we use the exact encryption keys ($x_1^0 = 12$, $x_2^0 = 22$, $x_3^0 = 31$, $x_4^0 = 4$) to decrypt the cipher images, while, in the second run, we attempt to decrypt the cipher images with slightly different keys ($x_1^0 = 12 + 10^{-15}$, $x_2^0 = 22$, $x_3^0 = 31$, and $x_4^0 = 4$). We conduct the experiments on the images of Lena, Circuit, Peppers, and Plane, and the results are shown in Figure 3. As we can see, the decrypted images with the slightly different keys are completely different from those decrypted with the correct keys, showing that the proposed FOHCLDNA has high sensitivity to secret key.

4.3. Statistical Analysis. A good cryptosystem should have the ability to resist all kinds of statistical attacks. Hence statistical analysis is another widely used and effective way to analyze a cryptosystem. Typical statistical analysis includes histogram analysis, information entropy, and correlation analysis.

4.3.1. Histogram Analysis. For image encryption, histogram is a popular tool to measure the distribution of pixel values in the plain image and the cipher image. The histogram of a plain image is usually unevenly distributed while that of cipher image by a good encryption scheme should be close to a uniform distribution. To put it another way, as far as the effectiveness of encryption schemes, the flatter the histogram of the cipher image is, the better the encryption scheme is.

The histograms of the plain images and their corresponding cipher images are shown in Figure 4. It can be seen from Figure 4 that the histograms of the plain images are irregularly distributed while all those of cipher images are very close to a uniform distribution. The results demonstrate that the proposed FOHCLDNA can resist histogram attacks.

4.3.2. Information Entropy. Information entropy (IE) is used to reflect the complexity of a system. For the 8-bit grayscale images used in the experiments, their intensity has 2^8 kinds of possible values ($[0, 255]$). The IE can be defined as

$$\mathrm{IE} = -\sum_{i=0}^{255} p(i) \log_2 p(i), \tag{11}$$

where $p(i)$ is the probability that the pixel value i appears [29]. When each pixel of cipher image has the same probability, that is, 1/256, IE reaches the ideal value 8.

The IEs of input images and cipher images are shown in Table 6. It can be seen that the IEs of input images are far below 8, while those of cipher images are very close to the ideal value. Among the encryption schemes, the FOHCLDNA achieves 4 out of 8 optimal values while all the IEs by HC-DNA are less than those by any other schemes. It is demonstrated that the FOHCLDNA is secure enough to resist entropy attacks.

4.3.3. Correlation Analysis. Two adjacent pixels in a natural image usually have high correlation. A good image encryption algorithm should be capable of reducing such correlation dramatically. Correlation coefficient γ is a popular metric to measure the correlation that can be formulated as follows [25]:

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2, \\ \mathrm{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right), \\ \gamma &= \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)\, D(y)}}, \end{aligned} \tag{12}$$

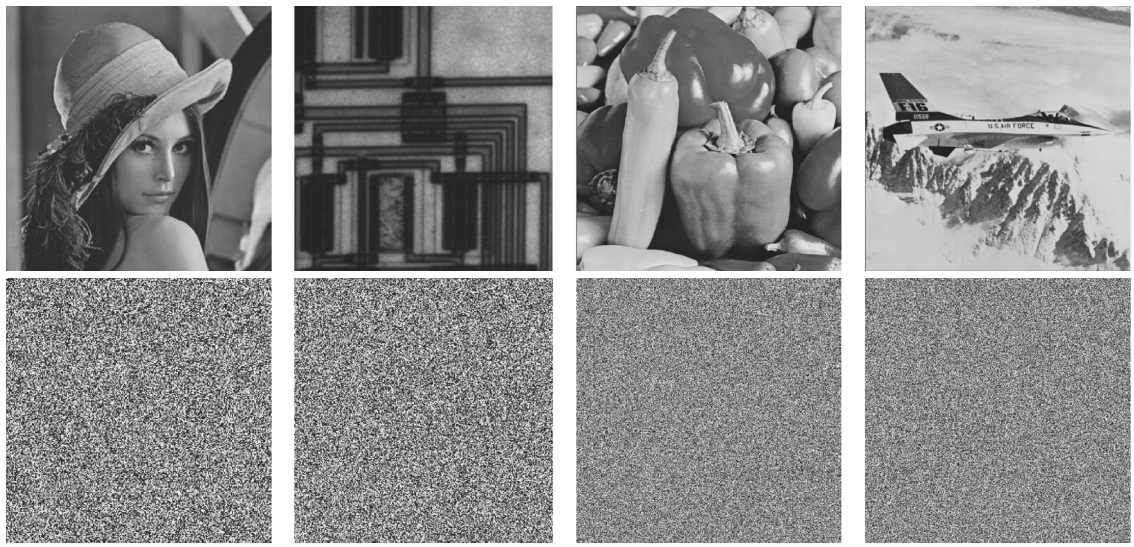

Figure 3: Decrypted images of Lena, Circuit, Peppers, and Plane. The first row is with correct keys: $x_1^0 = 12$, $x_2^0 = 22$, $x_3^0 = 31$, and $x_4^0 = 4$. The second row is with slightly different keys: $x_1^0 = 12 + 10^{-15}$, $x_2^0 = 22$, $x_3^0 = 31$, and $x_4^0 = 4$.

Table 6: The IE of the testing images.

Image	Input images	Cipher images			
		FOHCLDNA	HC-DNA [29]	CDCP [40]	CHC [41]
Lena	7.2283	7.9971	7.9964	7.9968	**7.9974**
Cameraman	7.1048	7.9973	7.9964	**7.9976**	7.9972
Circuit	7.2069	7.9975	7.9946	**7.9976**	7.9974
Peppers	7.5925	**7.9994**	7.9992	7.9993	**7.9994**
Barbara	7.1674	**7.9993**	7.9991	**7.9993**	7.9992
Bridge	5.7056	**7.9993**	7.9990	**7.9993**	**7.9993**
Plane	6.7059	**7.9993**	7.9990	7.9992	7.9992
Aerial	7.7357	7.9986	7.9985	**7.9987**	**7.9987**

where x and y are the gray levels of two neighbouring pixels in an image and N denotes the total number of pixels involved in the image.

To analyze the correlation of the image encryption schemes, we firstly calculate the correlation coefficients for all input images and cipher images in different directions, that is, horizontal γ_h, vertical γ_v, and diagonal γ_d, respectively [29], as listed in Table 7. From this table, it can be found that the correlation coefficients of all the input images are close to 1 in all directions, while those of the cipher images are round 0, showing that the encryption schemes can dramatically reduce the correlation of the adjacent pixels of the images. Specifically, the FOHCLDNA outperforms the rest schemes on 7 out of 24 correlation coefficients, whereas the HC-DNA achieves the optimal value only three times.

To have a further correlation analysis, we randomly select 4000 pairs of adjacent pixels in horizontal direction from each input image and corresponding cipher image by the FOHCLDNA, respectively, to show their adjacent-pixel distribution maps in Figure 5. It can be seen that the values of input images are distributed near the diagonal of coordinate plane, indicating strong correlation of input images. However, the correlation is completely destroyed by the FOHCLDNA so that the values of cipher images are distributed over almost the whole plane, showing very weak correlation in cipher images.

4.4. Analysis of Resisting Differential Attacks. According to the theory of cryptography, a good image encryption algorithm should also be very sensitive to the plain images; that is, a little change (e.g., a bit change) in a plain image can lead to a completely different cipher image. An image encryption scheme that has such a property can effectively resist differential attacks.

The number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are two important metrics for differential attack analysis. NPCR is defined as the variation ratio of two cipher images when the value of a pixel in the input image is slightly changed. UACI indicates the average intensity of the differences between the same cipher images. Mathematically, NPCR and UACI between

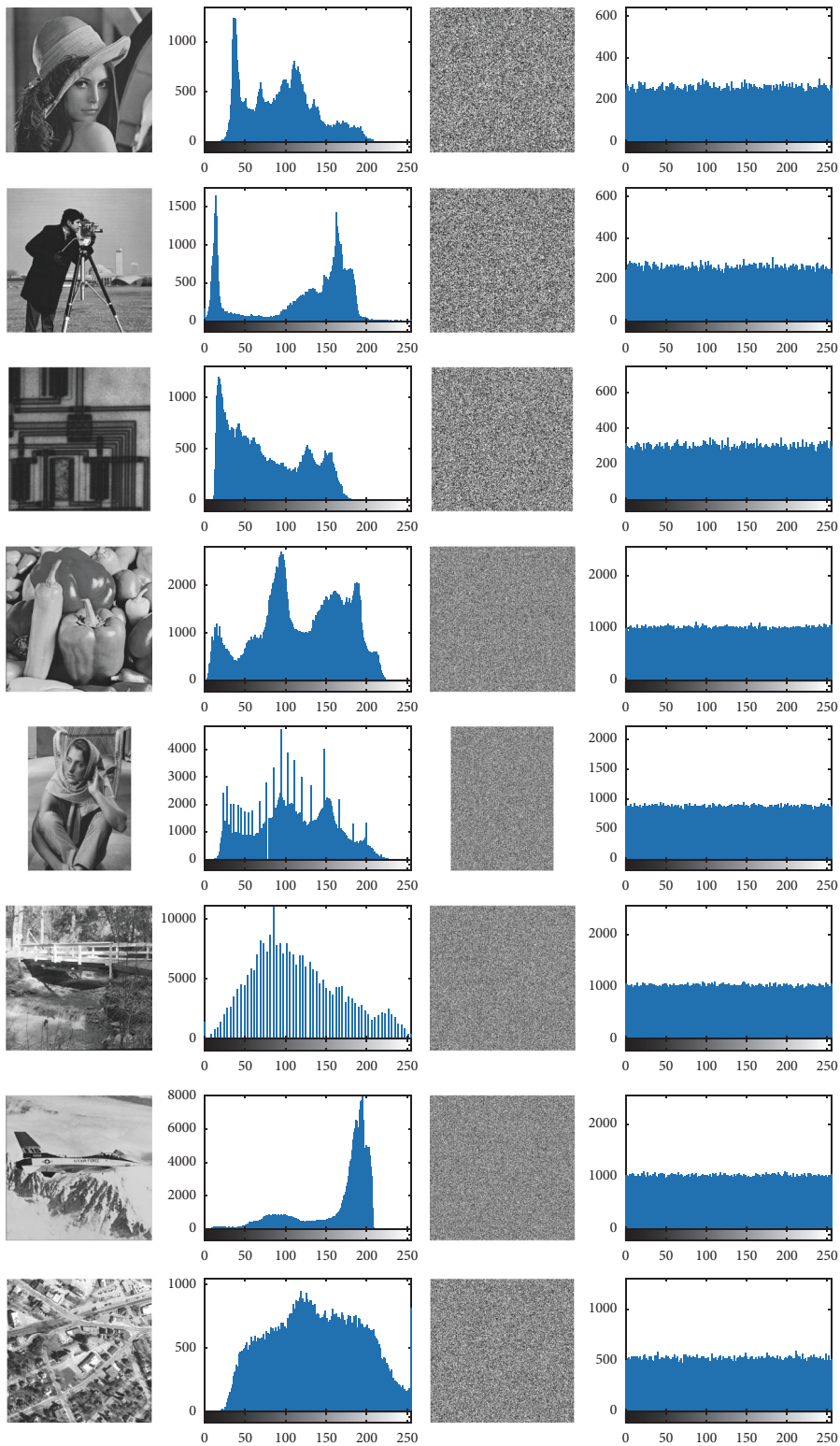

Figure 4: Histograms of the plain images and their corresponding cipher images. The first column is plain images. The second column is the histograms of the plain images. The third column is cipher images. And the fourth column is the histograms of the cipher images.

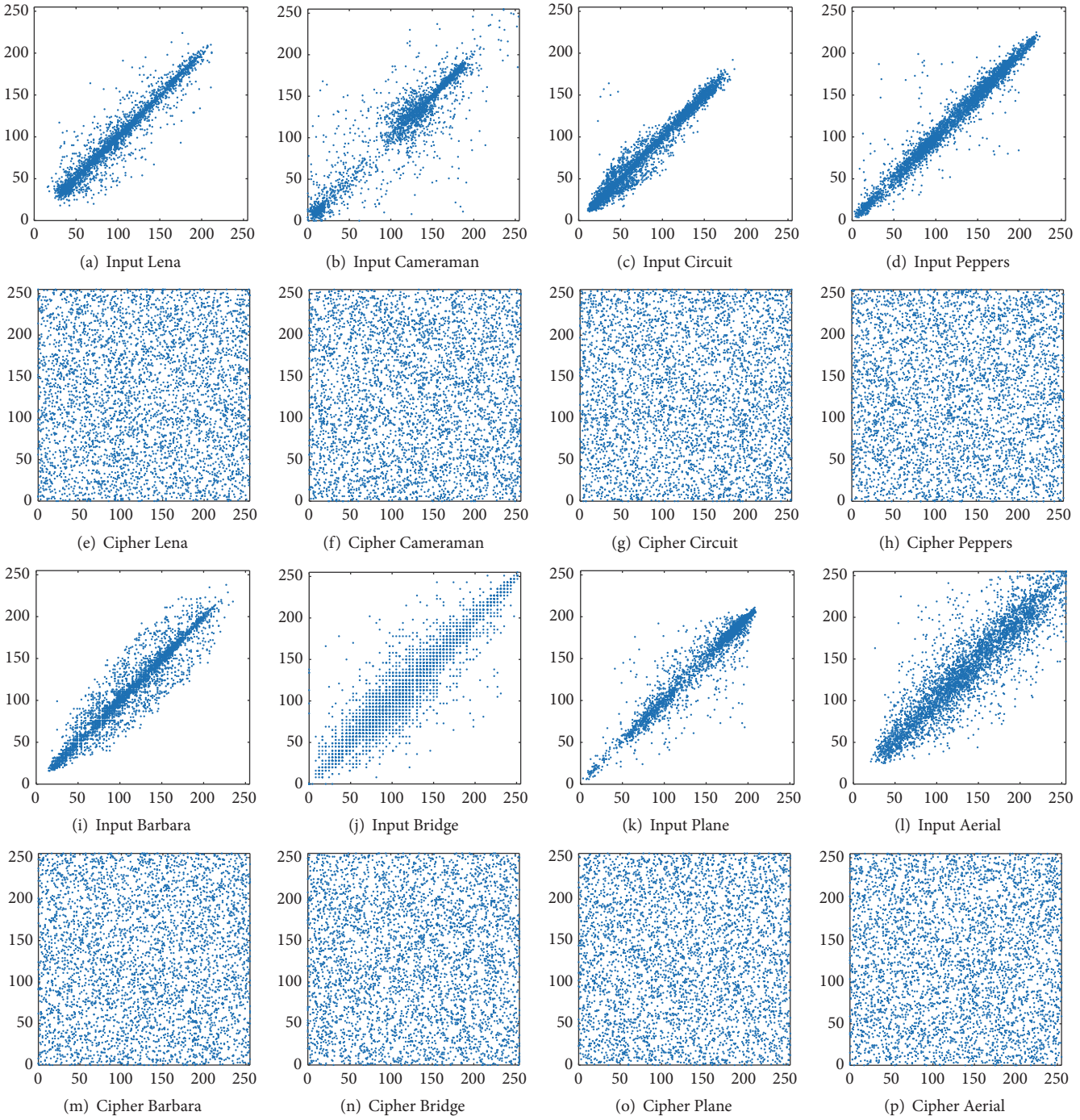

Figure 5: The adjacent-pixel distribution maps of the input images and the corresponding cipher images in horizontal direction.

two cipher images Q^1 and Q^2 can be formulated as (13) and (14), respectively:

$$\text{NPCR} = \frac{1}{hw}\sum_{i=1}^{h}\sum_{j=1}^{w} d_{ij} \times 100\%, \tag{13}$$

$$\text{UACI} = \frac{1}{hw}\sum_{i=1}^{h}\sum_{j=1}^{w} \frac{\left|Q_{ij}^1 - Q_{ij}^2\right|}{255} \times 100\%, \tag{14}$$

where h and w are the height and the width of the image, respectively, and d_{ij} is defined as follows:

$$d_{ij} = \begin{cases} 0, & Q_{ij}^1 = Q_{ij}^2, \\ 1, & Q_{ij}^1 \neq Q_{ij}^2. \end{cases} \tag{15}$$

Generally speaking, the more NPCR gets close to 100% and the bigger UACI is, the more encryption scheme becomes

Table 7: The correlation coefficients γ of the testing images.

Image	γ	Input images	Cipher images			
			FOHCLDNA	HC-DNA [29]	CDCP [40]	CHC [41]
Lena	γ_h	0.9494	0.0054	0.0019	−0.0021	**0.0006**
	γ_v	0.9667	0.0035	−0.0030	−0.0042	**−0.0003**
	γ_d	0.9366	**0.0016**	0.0018	−0.0022	0.0048
Cameraman	γ_h	0.9329	**−0.0010**	0.0076	−0.0022	−0.0069
	γ_v	0.9566	−0.0088	−0.0091	−0.0054	**−0.0044**
	γ_d	0.9117	0.0027	−0.0012	0.0048	**0.0010**
Circuit	γ_h	0.9766	**0.0012**	0.0019	0.0026	−0.0036
	γ_v	0.9775	−0.0071	0.0041	0.0030	**0.0022**
	γ_d	0.9678	**−0.0001**	−0.0012	0.0021	0.0018
Peppers	γ_h	0.9733	**−0.0009**	**0.0009**	−0.0015	−0.0017
	γ_v	0.9763	−0.0021	0.0041	−0.0012	**−0.0003**
	γ_d	0.9650	−0.0013	0.0008	0.0017	**−0.0006**
Barbara	γ_h	0.8271	**0.0010**	0.0011	−0.0038	0.0034
	γ_v	0.9501	−0.0030	0.0006	−0.0028	**0.0003**
	γ_d	0.8310	0.0007	−0.0038	**−0.0004**	0.0009
Bridge	γ_h	0.9388	−0.0029	**0.0007**	0.0036	0.0008
	γ_v	0.9217	−0.0033	0.0036	**0.0014**	0.0035
	γ_d	0.8988	**−0.0002**	0.0023	0.0018	0.0027
Plane	γ_h	0.9599	0.0017	−0.0017	**0.0004**	0.0005
	γ_v	0.9613	0.0021	0.0020	0.0018	**−0.0003**
	γ_d	0.9359	0.0015	**−0.0007**	0.0013	0.0010
Aerial	γ_h	0.9083	0.0015	−0.0010	**−0.0006**	−0.0025
	γ_v	0.8891	−0.0022	0.0034	**0.0010**	−0.0045
	γ_d	0.8502	−0.0015	0.0022	0.0026	**−0.0014**

Table 8: The average NPCR (%) of running the schemes 10 times.

Image	FOHCLDNA	HC-DNA [29]	CDCP [40]	CHC [41]
Lena	99.5723	68.1731	**100.0000**	99.6103
Cameraman	99.5853	44.7412	**100.0000**	99.6089
Circuit	99.5962	44.1423	**99.6663**	99.6026
Peppers	99.5845	58.9414	**99.7145**	99.6061
Barbara	99.5857	58.6456	**100.0000**	99.6035
Bridge	99.5798	49.3543	**99.7100**	99.6089
Plane	99.5846	65.2526	99.5881	**99.6067**
Aerial	99.5802	53.0030	**100.0000**	99.6093

effective in resisting differential attacks. For a 256-level gray image, the maximum theoretical values for NPCR and UACI are 99.6094% and 33.4635%, respectively [29].

We randomly change one bit in the plain images to compute one value of NPCR and UACI. We repeat the process 10 times and report the average values of NPCR and UACI in Tables 8 and 9, respectively.

It can be shown that although the values by the FOHCLDNA are not as good as those by CDCP and CHC, they are very close to the maximum theoretical values. The FOHCLDNA apparently outperforms HC-DNA in terms of NPCR and UACI. The results show that the global pixel diffusion is effective and the FOHCLDNA has the capability of resisting differential attacks.

5. Conclusions

In this paper, we propose a novel image encryption algorithm based on a fractional-order hyperchaotic Lorenz system and DNA computing (FOHCLDNA). The fractional-order hyperchaotic Lorenz system is adopted to generate the pseudorandom sequence that is utilized throughout the process of encryption. Besides pixel-level and bit-level operations, DNA operations such as DNA addition, DNA subtraction, and DNA XOR are also introduced to the algorithm. A simple pixel diffusion is used to spread the slight change in one pixel to all other pixels. Several types of permutation are carried out on different level data. Through the results of extensive experiments and corresponding security analysis,

Table 9: The average UACI (%) of running the schemes 10 times.

Image	FOHCLDNA	HC-DNA [29]	CDCP [40]	CHC [41]
Lena	33.3159	31.7168	**33.5530**	33.4333
Cameraman	33.3727	17.3423	33.4064	**33.4724**
Circuit	33.1996	15.2453	33.4253	**33.5338**
Peppers	33.2703	23.4302	33.4135	**33.4672**
Barbara	33.3261	24.0960	**33.4946**	33.4446
Bridge	33.3062	18.0547	**33.4779**	33.4620
Plane	33.3532	24.9252	**33.4753**	33.4446
Aerial	33.3311	20.3190	**33.4911**	33.4392

it can be found that the FOHCLDNA is highly sensitive to the secret key, has a larger secret key space, and can resist some known attacks, such as brute-force attacks, statistical attacks, and differential attacks. All these properties indicate that the FOHCLDNA is promising for image encryption. In the future, the FOHCLDNA could be extended to color image encryption.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Major Research Plan of the National Natural Science Foundation of China (Grant no. 91218301), the Fundamental Research Funds for the Central Universities (Grants no. JBK170944, no. JBK170505, and no. JBK130503), the Natural Science Foundation of China (Grant no. 71473201), and the Scientific Research Fund of Sichuan Provincial Education Department (Grant no. 17ZB0433).

References

[1] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley and Sons, Indianapolis, IN, USA, 2015.

[2] A. A. A. El-Latif, L. Li, and X. Niu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system," *Multimedia Tools and Applications*, vol. 70, no. 3, pp. 1559–1584, 2014.

[3] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.

[4] X. Zhang, X. Fan, J. Wang, and Z. Zhao, "A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution," *Multimedia Tools and Applications*, vol. 75, no. 4, pp. 1745–1763, 2016.

[5] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[6] Z. Zhu, W. Zhang, K. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

[7] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Optics & Laser Technology*, vol. 82, pp. 121–133, 2016.

[8] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.

[9] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Optics and Lasers in Engineering*, vol. 91, pp. 41–52, 2017.

[10] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, Article ID 013014, 2012.

[11] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[12] R. Boriga, A. C. Dascalescu, and A.-V. Diaconu, "A new one-dimensional chaotic map and its use in a novel real-time image encryption scheme," *Advances in Multimedia*, vol. 2014, Article ID 409586, 15 pages, 2014.

[13] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, and V. Fernandez, "On the security of a new image encryption scheme based on chaotic map lattices," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 18, no. 3, Article ID 033112, 2008.

[14] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[15] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.

[16] G. Chen and X. Dong, *From Chaos to Order: Methodologies, Perspectives, and Applications*, Series on Nonlinear Science, World Scientific, 1998.

[17] T. Ueta and G. Chen, "Bifurcation analysis of Chen's equation," *International Journal of Bifurcation and Chaos*, vol. 10, no. 8, pp. 1917–1931, 2000.

[18] A. Wolf, J. B. Swift, and H. L. A. Swinney, "Determining Lyapunov exponents from a time series," *Physica D: Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.

[19] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29–37, 2012.

[20] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimedia Tools and Applications*, vol. 71, no. 3, pp. 1469–1497, 2014.

[21] X. Wang and H. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 1, pp. 333–346, 2016.

[22] N. Zhou, Y. Hu, L. Gong, and G. Li, "Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations," *Quantum Information Processing*, vol. 16, no. 6, 2017.

[23] H.-M. Yuan, Y. Liu, T. Lin, T. Hu, and L.-H. Gong, "A new parallel image cryptosystem based on 5D hyper-chaotic system," *Signal Processing: Image Communication*, vol. 52, pp. 87–96, 2017.

[24] I. Podlubny, I. Petráš, B. M. Vinagre, and L. Dorcák, "Analogue realizations of fractional-order controllers," *Nonlinear Dynamics*, vol. 29, no. 1–4, pp. 281–296, 2002.

[25] Z. Wang, X. Huang, Y.-X. Li, and X.-N. Song, "A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system," *Chinese Physics B*, vol. 22, no. 1, Article ID 010504, 2013.

[26] J. Zhao, S. Wang, Y. Chang, and X. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dynamics*, vol. 80, no. 4, pp. 1721–1729, 2015.

[27] X. Huang, T. Sun, Y. Li, and J. Liang, "A color image encryption algorithm based on a fractional-order hyperchaotic system," *Entropy*, vol. 17, no. 1, pp. 28–38, 2014.

[28] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024, 1994.

[29] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and DNA sequences for image encryption," *Journal of Electronic Imaging*, vol. 26, no. 1, Article ID 013021, 2017.

[30] Q. Zhang, L. Liu, and X. Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps," *AEU-International Journal of Electronics and Communications*, vol. 68, no. 3, pp. 186–192, 2014.

[31] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools and Applications*, vol. 75, no. 11, pp. 6303–6319, 2016.

[32] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and Secure hash algorithm SHA-2," *Nonlinear Dynamics*, vol. 83, no. 3, pp. 1123–1136, 2016.

[33] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11-12, pp. 2028–2035, 2010.

[34] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, 2012.

[35] X. Wang and J. Song, "Synchronization of the fractional order hyperchaos lorenz systems with activation feedback control," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 8, pp. 3351–3357, 2009.

[36] S. Wang and R. Wu, "Dynamic analysis of a 5D fractional-order hyperchaotic system," *International Journal of Control, Automation, and Systems*, vol. 15, no. 3, pp. 1–8, 2017.

[37] J. He, S. Yu, and J. Cai, "A method for image encryption based on fractional-order hyperchaotic systems," *Journal of Applied Analysis and Computation*, vol. 5, no. 2, pp. 197–209, 2015.

[38] X. Wu, "A color image encryption algorithm using the fractional-order hyperchaotic systems," in *Proceedings of the 5th International Workshop on Chaos-Fractals Theories and Applications, IWCFTA ('12)*, pp. 196–201, China, October 2012.

[39] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6229–6245, 2017.

[40] C. Zhu, Y. Hu, and K. Sun, "New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in criss-cross pattern," *Journal of Electronics & Information Technology*, vol. 34, no. 7, pp. 1735–1743, 2012.

[41] C.-X. Zhu and K.-H. Sun, "Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms," *Acta Physica Sinica*, vol. 61, no. 12, p. 120503, 2012.

[42] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 2005.