Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 6795964, 12 pages
https://doi.org/10.1155/2020/6795964

Research Article

Anticontrol of a Fractional-Order Chaotic System and Its Application in Color Image Encryption

Yujun Niu,[1] **Xuming Sun**,[1] **Cheng Zhang**,[1] **and Hongjun Liu**[2]

[1]*School of Information Engineering, Dalian University, Dalian 116622, China*
[2]*School of Mathematical Sciences, University of Jinan, Jinan 250022, China*

Correspondence should be addressed to Yujun Niu; niuyujun@dlu.edu.cn

Received 20 November 2019; Revised 31 January 2020; Accepted 5 February 2020; Published 11 March 2020

Guest Editor: Jesus M. Muñoz-Pacheco

This paper investigates the anticontrol of the fractional-order chaotic system. The necessary condition of the anticontrol of the fractional-order chaotic system is proposed, and based on this necessary condition, a 3D fractional-order chaotic system is driven to two new 4D fractional-order hyperchaotic systems, respectively, without changing the parameters and fractional order. Hyperchaotic properties of these new fractional dynamic systems are confirmed by Lyapunov exponents and bifurcation diagrams. Furthermore, a color image encryption algorithm is designed based on these fractional hyperchaotic systems. The effectiveness of their application in image encryption is verified.

1. Introduction

In recent years, how to make a dynamic system chaotic or enhance the chaos of the system, that is to say, study on the anticontrol of the chaotic system, has become a very hot research topic [1–7]. A feedback control design method is proposed to make all the Lyapunov exponents of the discrete-time dynamical system strictly positive by Chen and Lai [1]. Based on time-delay feedback, a systematic design approach is developed for anticontrol of chaos in a continuous-time system [2, 3]. Li et al. present a simple parameter perturbation control technique to drive a unified chaotic system to hyperchaotic [4]. In [5], a state feedback control is used to design a hyperchaotic Chua system with piecewise-linear nonlinearity. A systematic methodology is proposed to construct the continuous-time autonomous hyperchaotic system with multiple positive Lyapunov exponents, and a 6-dimensional hyperchaotic circuit is implemented [6, 7].

In the aforementioned works, the dynamical systems are all chaotic systems with integer order. However, compared with the integer-order chaotic system, the fractional-order system has higher nonlinearity. Moreover, the derivative orders can be used as secret keys in the encryption algorithm based on the chaotic system. At the same time, because high-dimensional chaotic systems have multiple positive Lyapunov exponents and control parameters, it can display more complex dynamical behaviors. Therefore, study on the fractional-order hyperchaotic systems has attracted interest of many scholars [8–19]. Some new high-dimensional fractional-order chaotic systems have been proposed and studied, including dynamic analysis [8–11], control [12, 13], synchronization [14, 15], circuit implementation [16], and application in information encryption [17–19]. But, these fractional-order hyperchaotic systems are obtained by directly modifying the order of integer-order hyperchaotic systems, instead of getting from the anticontrol of the fractional-order system.

Inspired by the above discussions, in this paper, based on linear feedback and nonlinear feedback, we directly drive the 3D fractional-order chaotic system to two new 4D fractional-order hyperchaotic systems, respectively, without changing the parameters and fractional order. We propose the necessary conditions of the anticontrol for the fractional-order chaotic system and to calculate the Lyapunov exponents and bifurcation diagrams of the new fractional hyperchaotic dynamic systems. Furthermore, based on these two fractional-order hyperchaotic systems, a color image encryption algorithm is designed. The security analysis verifies that these hyperchaotic systems are effective for image encryption.

2. Problem Formulation

A 3D autonomous chaotic system is proposed by Qi et al. [20], which can be described as

$$\begin{cases} \dot{x} = a(y - x) + yz, \\ \dot{y} = cx - y - xz, \\ \dot{z} = xy - bz, \end{cases} \tag{1}$$

where x, y, and z are state variables. When the parameters $a = 35$, $b = 8/3$, and $c = 55$, system (1) shows a chaotic behavior. The fractional-order equation of system (1) can be expressed as

$$\begin{cases} \dfrac{\mathrm{d}^{q_1} x}{\mathrm{d}t^{q^1}} = a(y - x) + yz, \\ \dfrac{\mathrm{d}^{q_2} y}{\mathrm{d}t^{q^2}} = cx - y - xz, \\ \dfrac{\mathrm{d}^{q_3} z}{\mathrm{d}t^{q^3}} = xy - bz, \end{cases} \tag{2}$$

where q_i is the fractional order, $0 < q_i \le 1\,(i = 1, 2, 3)$. According to the algorithm presented by Wolf et al. [21], we calculate the largest Lyapunov exponent of fractional-order system (2). When $q_1 = q_2 = q_3 = 0.96$, system (2) exhibits a chaotic behavior with the largest Lyapunov exponent 2.168. In this paper, the numerical simulation of fractional-order systems is derived according to Caputo derivative. More detailed introduction about Caputo derivative definition can be seen in [22].

In the following, fractional-order chaotic system (2) is driven to two new 4D fractional-order hyperchaotic systems, respectively, with the same parameters and fractional order, that is, $a = 35$, $b = 8/3$, $c = 55$, and $q_1 = q_2 = q_3 = 0.96$.

3. New Fractional-Order Hyperchaotic Systems

About the anticontrol of the fractional-order chaotic systems, we give the two necessary conditions as follows:

(1) The new dynamic system must be dissipative

(2) None of equilibriums of the new fractional-order system is stable

The stable and unstable region division at the zero equilibrium of the fractional-order system is shown in Figure 1. According to the stability theory of the fractional-order system [23], it can be proved that, for n-dimensional fractional system, if all the eigenvalues $(\lambda_1, \lambda_2, ..., \lambda_n)$ of the Jacobian matrix of some equilibrium point satisfy

$$\left|\arg(\lambda_i)\right| > \frac{\alpha\pi}{2}, \quad \alpha = \max(q_1, q_2, \ldots, q_n),\ i = 1, 2, \ldots, n, \tag{3}$$

then the fractional-order system is asymptotically steady at the equilibrium. From Figure 1, it can be seen that, for the fractional-order system, as long as there is a stable equilibrium, it will be steady at one point; it is in chaos only when

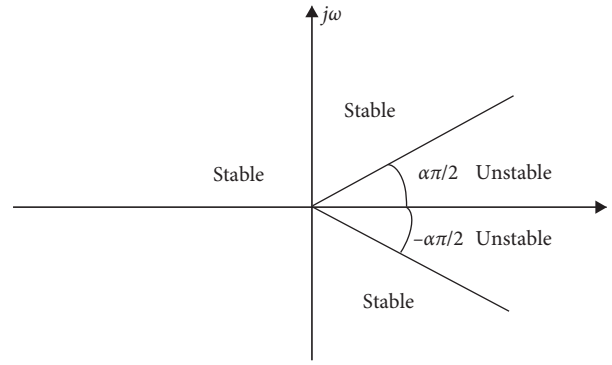

Figure 1: Stability region of the fractional-order system.

none equilibrium is stable. Moreover, a dynamic system with chaotic characteristics must be dissipative. Therefore, the above necessary conditions can be obtained.

In the following, we analyze the dynamical behaviors of fractional-order system (2). We can calculate that system (2) has three equilibriums $S_0(-19.3091, -7.5418, 54.6094)$, $S_1(19.3091, 7.5418, 54.6094)$, and $S_2(0, 0, 0)$.

For the equilibrium $S_0(-19.3091, -7.5418, 54.6094)$, it can be calculated that the eigenvalues of the Jacobian matrix are $\lambda_1 = -43.0978$, $\lambda_2 = 2.2156 + 24.4545i$, and $\lambda_3 = 2.2156 - 24.4545i$. Further, it can be obtained that $\arg(\lambda_1) = \pi$, $\arg(\lambda_2) = 1.4797$, and $\arg(\lambda_3) = -1.4797$. From formula (3), when $q_i > 0.9420\,(1.4797 \times 2/\pi)$, $i = 1, 2, 3$, $S_0(-19.3091, -7.5418, 54.6094)$ is unstable equilibrium. In the same way, it can be obtained that the equilibrium $S_1(19.3091, 7.5418, 54.6094)$ is unstable when $q_i > 0.9420\,(1.4797 \times 2/\pi)$, $i = 1, 2, 3$, and $S_2(0, 0, 0)$ is unstable equilibrium of system (2).

To sum up, when $q_i > 0.9420$, $i = 1, 2, 3$, S_0, S_1, and S_2 are all unstable equilibriums of system (2). So, the value of fractional order of system (2) must be between 0.9420 and 1. Finally, we select 0.96 as fractional order of system (2).

3.1. Fractional Hyperchaotic System Obtained by Linear Feedback. For convenience of expression, the variables of system (2) are replaced with $x_i\,(i = 1, \ldots, 3)$. With the same parameters and fractional order, a new 4-dimensional fractional-order dynamic system is obtained by introducing a linear feedback control term $(\mathrm{d}^{q_4} x_4/\mathrm{d}t^{q_4}) = -63x_2 + r_1 x_4$ to the equation of system (2) as follows:

$$\begin{cases} \dfrac{\mathrm{d}^{q_1} x_1}{\mathrm{d}t^{q_1}} = a(x_2 - x_1) + x_2 x_3, \\ \dfrac{\mathrm{d}^{q_2} x_2}{\mathrm{d}t^{q_2}} = cx_1 - x_2 - x_1 x_3 + x_4, \\ \dfrac{\mathrm{d}^{q_3} x_3}{\mathrm{d}t^{q_3}} = x_1 x_2 - bx_3, \\ \dfrac{\mathrm{d}^{q_4} x_4}{\mathrm{d}t^{q_4}} = -63x_1 + r_1 x_4, \end{cases} \tag{4}$$

where r_1 is a control parameter, and system (4) is possible to be chaotic only when its value satisfies the above necessary condition of the anticontrol.

In order to ensure the dissipative structure of system (4), the requirement is that

$$\nabla V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} + \frac{\partial \dot{x}_4}{\partial x_4} = -a - 1 - b + r_1 = r_1 - 38.7 < 0. \tag{5}$$

It is concluded that the value of control parameter r_1 must be less than 38.7. In order to maintain the dissipative structure better, we choose $r_1 = 0.6$ near zero.

When $a = 35$, $b = 8/3$, $c = 55$, and $r_1 = 0.6$, we calculate that system (4) has three equilibriums $S_0(0, 0, 0, 0)$, $S_1(0.0487, 0.0088, 0.1598, 5.1141)$, and $S_2(-0.0487, -0.0088, 0.1598, -5.1141)$.

First, let us study whether equilibrium $S_0(0, 0, 0, 0)$ is stable. The Jacobian matrix of system (4) at equilibrium point S_0 is as follows:

$$J = \begin{Bmatrix} -a & a + x_3 & x_2 & 0 \\ c - x_3 & -1 & -x_1 & 1 \\ x_2 & x_1 & -b & 0 \\ -63 & 0 & 0 & r_1 \end{Bmatrix} = \begin{Bmatrix} -a & a & 0 & 0 \\ c & -1 & 0 & 1 \\ 0 & 0 & -b & 0 \\ -63 & 0 & 0 & r_1 \end{Bmatrix}. \tag{6}$$

It is calculated that the eigenvalues of the Jacobian matrix are $\lambda_1 = -65.4068$, $\lambda_2 = 28.1963$, $\lambda_3 = 1.8105$, and $\lambda_4 = -2.6667$. Furthermore, we can get that $\arg(\lambda_1) = \pi$, $\arg(\lambda_2) = 0$, $\arg(\lambda_3) = 0$, and $\arg(\lambda_4) = \pi$, without satisfying that $|\arg(\lambda_i)| > 0.96 \times \pi/2$ $(i = 1, 2, \ldots, 4)$. Therefore, it can be concluded that S_0 is unstable equilibrium.

Next, $S_1(0.0487, 0.0088, 0.1598, 5.1141)$ is chosen to study. We can compute that the eigenvalues of the Jacobian matrix $\lambda_1 = -65.4416$, $\lambda_2 = 28.2276$, $\lambda_3 = 1.8140$, and $\lambda_4 = -2.6666$, and we can obtain that $\arg(\lambda_1) = \pi$, $\arg(\lambda_2) = 0$, $\arg(\lambda_3) = 0$, and $\arg(\lambda_4) = \pi$. So, the equilibrium S_1 is not stable. In the same way, it can be obtained that $S_2(-0.0487, -0.0088, 0.1598, -5.1141)$ is also unstable.

To sum up, when $r_1 = 0.6$, S_0, S_1, and S_2 are all unstable equilibriums of system (4). We obtain the Lyapunov exponents of system (4): $\lambda_1 = 1.4272$, $\lambda_2 = 0.3705$, $\lambda_3 = -0.0028$, and $\lambda_4 = -41.3635$ when $r_1 = 0.6$ and $q_1 = q_2 = q_3 = q_4 = 0.96$. Therefore, it is proved that system (4) shows a hyperchaotic behavior. The part of projections of the hyperchaotic attractor is shown in Figure 2.

According to the method presented by Ramasubramanian and Sriram [24], when $-1.5 \le r_1 \le 2$, the Lyapunov exponent spectrum of fractional-order system (4) is calculated, and it is shown in Figure 3(a). The corresponding bifurcation diagram of system (4) is shown in Figure 3(b). From Figure 3, it is easy to observe that when $-1.05 \le r_1 \le 1.7$, fractional-order system (4) is hyperchaotic with satisfying that $\lambda_1 > 0$, $\lambda_2 > 0$, $\lambda_3 = 0$, and $\lambda_4 < 0$.

3.2. Fractional Hyperchaotic System Obtained by Nonlinear Feedback. The variables of system (2) are taken the place of y_i $(i = 1, \ldots, 3)$, and a nonlinear feedback control term is added to system (2). A new 4D fractional-order dynamic system is obtained as follows:

$$\begin{cases} \dfrac{d^{q_1} y_1}{dt^{q_1}} = a(y_2 - y_1) + y_2 y_3, \\ \dfrac{d^{q_2} y_2}{dt^{q_2}} = c y_1 - y_2 - y_1 y_3 + y_4, \\ \dfrac{d^{q_3} y_3}{dt^{q_3}} = y_1 y_2 - b y_3, \\ \dfrac{d^{q_4} y_4}{dt^{q_4}} = -y_1 y_3 + r_2 y_4, \end{cases} \tag{7}$$

where r_2 is a control parameter, and we choose $r_2 = 1.2$ in order to ensure system (7) be dissipative.

When $r_2 = 1.2$, it can be computed that system (7) has only one equilibrium $S_0(0, 0, 0, 0)$. Furthermore, we can calculate that $\arg(\lambda_1) = \pi$, $\arg(\lambda_2) = 0$, $\arg(\lambda_3) = \pi$, and $\arg(\lambda_4) = 0$. So, it is not satisfied that $|\arg(\lambda_i)| > 0.96 \times (\pi/2)$. Therefore, S_0 is not stable equilibrium.

When $r_2 = 1.2$ and $q_1 = q_2 = q_3 = q_4 = 0.96$, fractional-order system (7) displays a hyperchaotic behavior with Lyapunov exponents $\lambda_1 = 1.3551$, $\lambda_2 = 0.2182$, $\lambda_3 = 0.0039$, and $\lambda_4 = -30.2820$. The part of projections of the hyperchaotic attractor is shown in Figure 4.

When $0.5 \le r_2 \le 2.5$, the Lyapunov exponent spectrum of system (7) is computed according to Ramasubramanian and Sriram method [24]. It is shown in Figure 5(a), and the corresponding bifurcation diagram of system (7) is shown in Figure 5(b). From Figure 5, it can be seen that when $1.1 \le r_2 \le 1.95$, system (7) is hyperchaotic with two positive, a zero, and a negative Lyapunov exponents.

4. Image Encryption Based on the Fractional-Order Hyperchaotic Systems

In this section, a color image encryption algorithm is designed based on fractional-order hyperchaotic system (4) and system (7).

4.1. Design of Image Encryption Algorithm

4.1.1. Permutation Process. In order to break the correlation of the neighboring pixels in the plaintext, the plain image is permutated in bit-level. A color image with size of $m \times n$ is chosen as the plain image P.

Step 1. First, the plain image P is converted into a grayscale image whose size is $m \times 3n$ according to the red, green, and blue components of the color image. Then, each pixel of the grayscale image is transformed into an 8-bit array. So, the whole plain image P is changed into a binary matrix P_b with a size of $m \times 24n$.

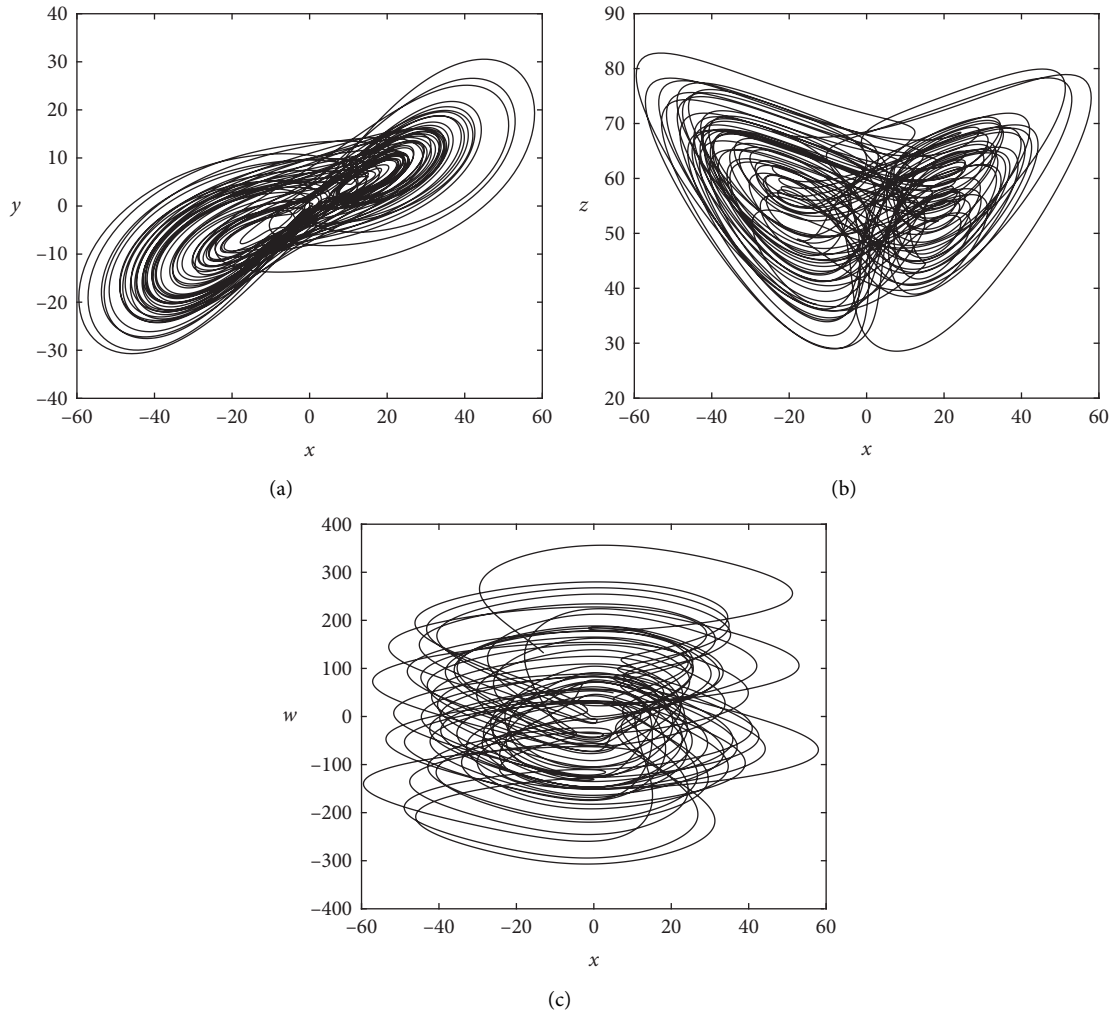

Figure 2: When $r_1 = 0.6$, the part of projections of the attractor of system (4).

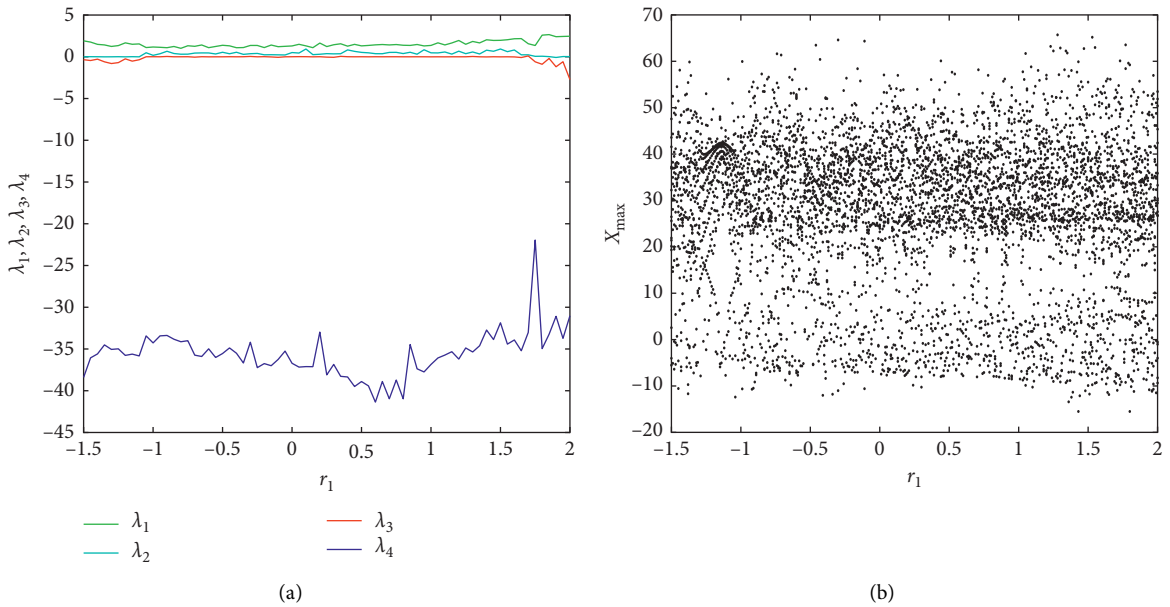

Figure 3: Lyapunov exponents and bifurcation diagram of system (4) for $-1.5 \le r_1 \le 2$. (a) Lyapunov exponents. (b) Bifurcation diagram.

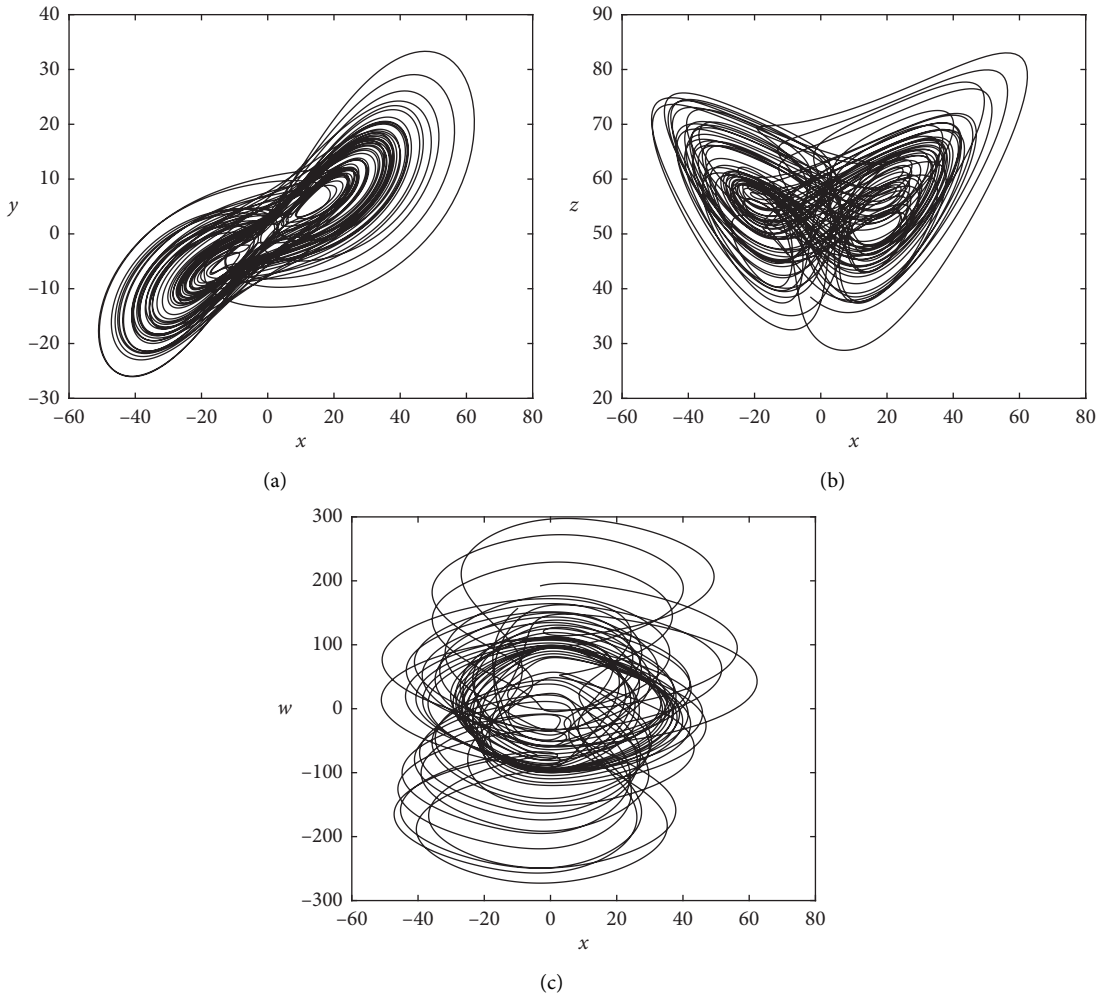

Figure 4: When $r_2 = 1.2$, the part of projections of the hyperchaotic attractor of system (7).

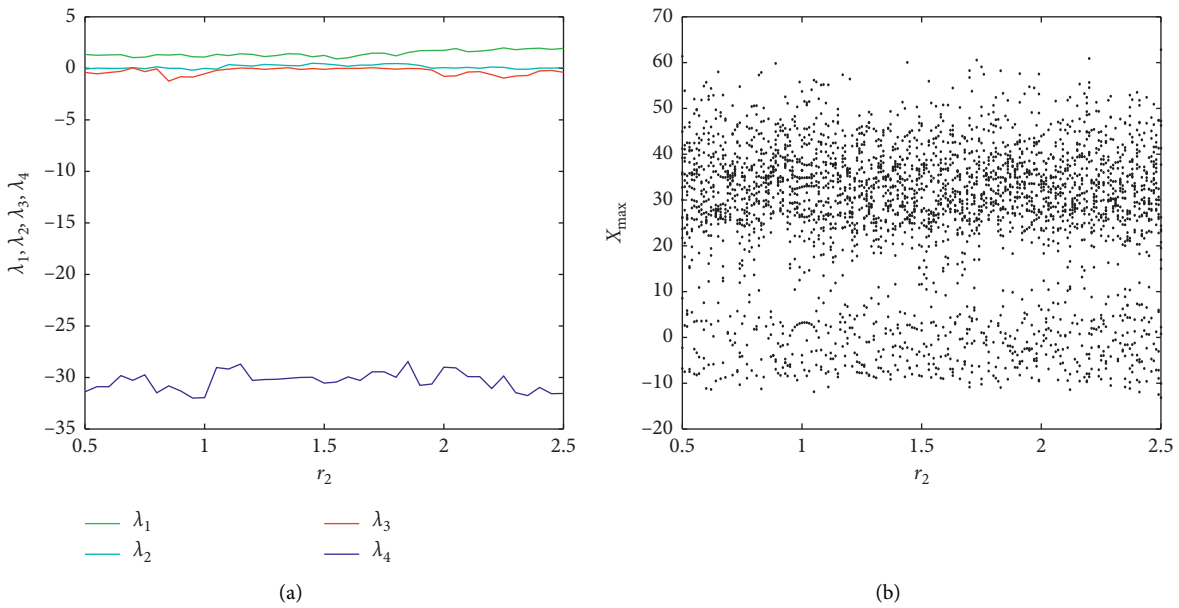

Figure 5: Lyapunov exponents and bifurcation diagram of system (7) for $0.5 \le r_2 \le 2.5$. (a) Lyapunov exponents. (b) Bifurcation diagram.

Step 2. The sequences $(x_1(i), x_2(i), x_3(i), x_4(i))$ are generated by fractional-order hyperchaotic system (4) with initial values $(x_1(0), x_2(0), x_3(0), x_4(0))$. The key vectors key_h and key_v are produced by equations (8) and (9), respectively:

$$\text{key}_h(i) = \text{abs}\left(x_1(i) + x_2(i) \times g\right) - \text{floor}\left(\text{abs} \cdot \left(x_1(i) + x_2(i) \times g\right)\right), \quad i = 1, 2, \ldots, m, \tag{8}$$

$$\text{key}_v(j) = \text{abs}\left(x_3(j) \times g + x_4(j)\right) - \text{floor}\left(\text{abs} \cdot \left(x_3(j) \times g + x_4(j)\right)\right), \quad j = 1, 2, \ldots, 24n, \tag{9}$$

where g is a disturbance item related to the plain image, which can be obtained by equation (10) as follows:

$$g = \frac{\text{sum}(P_b)}{mn}, \tag{10}$$

where sum (P_b) is the sum of all the elements with value of 1 in the matrix P_b. Therefore, the key vectors key_h and key_v are related to the plain image P. Because different plain images are encrypted by different keys, this algorithm can resist the chosen plaintext attack.

Step 3. Set two auxiliary vectors $h(i)$, $i = 1, 2, \ldots, m$ and $v(j)$, $j = 1, 2, \ldots, 24n$. They represent the line numbers and the column numbers of P_b in the ascending order, respectively. Next, the vectors h' and v' are generated by equations (11) and (12), separately. Then, a binary matrix is obtained by permuting the rows and columns of image P_b, respectively, according to the vectors h' and v'. Finally, we transform this binary matrix into color image P_c.

$$h'(i) = h\left(\text{floor}\left(\text{key}_h(i) \times m\right) \bmod i\right), \quad i = 1, 2, \ldots, m, \tag{11}$$

$$v'(j) = v\left(\text{floor}\left(\text{key}_v(j) \times 24n\right) \bmod j\right), \quad j = 1, 2, \ldots, 24n. \tag{12}$$

4.1.2. Encryption Algorithm. In this stage, the permutated color image P_c is encrypted in pixel-level, and the detailed steps are as follows:

Step 1. Separate the permuted color image P_c into red, green, and blue grayscale images, and the i-th pixel value of these three grayscale images is represented by r_i, g_i, and b_i $(i = 1, 2, \ldots, mn)$, respectively.

Step 2. With initial values $(y_1(0), y_2(0), y_3(0), y_4(0))$, the sequences $(y_1(i), y_2(i), y_3(i), y_4(i))$ are produced by fractional-order hyperchaotic system (7). Then, an integer sequence $sk_j(i)$ between 0 and 255 is obtained:

$$sk_j(i) = \left(\text{abs}\left(y_u(i) + y_v(i)\right)\right) - \text{floor}\left(\text{abs} \cdot \left(y_u(i) + y_v(i)\right)\right) \times 10^{14} \bmod 256, \quad j = 1, \ldots, 6, \tag{13}$$

where $u, v \in \{1, 2, 3, 4\}$ and $u \neq v$. The encryption key sequences $(\text{key}_r(i), \text{key}_g(i), \text{key}_b(i))$ can be gained by the key selection table, and it is shown in Table 1.

There are three groups of keys in Table 1. $s(i)$ is used to decide which group is selected to encrypt r_i, g_i, and b_i of the i-th pixel. So, it is realized that different plain images are encrypted by different key streams. The sequence $s(i)$ is generated by equations (14) and (15):

$$\text{key}_s(i) = \left(\text{abs}\left(\sum_{j=1}^{4} x_j(i)\right) - \text{floor}\left(\text{abs}\left(\sum_{j=1}^{4} x_j(i)\right)\right)\right) \times 10^{14}, \quad i = 1, 2, \ldots, mn, \tag{14}$$

$$s(i) = \begin{cases} \text{floor}\left(\sum_{j=2}^{mn}\left(r_j + g_j + b_j\right) \times \text{key}_s(i)\right) \bmod 3, & i = 1, \\ \text{floor}\left(\left(s^p(i-1) - \left(r_i + g_i + b_i\right)\right) \times \text{key}_s(i)\right) \bmod 3, & \\ \quad i = 2, \ldots, mn, & \end{cases} \tag{15}$$

where $x_j(i)$, $(j = 1, 2, \ldots, 4)$ are produced by fractional-order hyperchaotic system (4).

Step 3. After r_i, g_i, and b_i of three grayscale images are encrypted by equation (16), respectively, we can get the encrypted r_i', g_i', and b_i':

$$\begin{cases} r_i' = \left(\left(r_i + r_{i-1}'\right) \bmod 256\right) \oplus \text{key}_r(i), \\ g_i' = \left(\left(g_i + g_{i-1}'\right) \bmod 256\right) \oplus \text{key}_g(i), \quad i = 1, \ldots, mn, \\ b_i' = \left(\left(b_i + b_{i-1}'\right) \bmod 256\right) \oplus \text{key}_b(i), \end{cases} \tag{16}$$

where

$$\begin{cases} r_0' = \left(\sum_{j=1}^{mn} r_j + sk_1(1)\right) \bmod 256, \\ g_0' = \left(\sum_{j=1}^{mn} g_j + sk_2(1)\right) \bmod 256, \\ b_0' = \left(\sum_{j=1}^{mn} b_j + sk_3(1)\right) \bmod 256. \end{cases} \tag{17}$$

Step 4. Repeat the aforementioned steps appropriately. In the end, the encrypted color image I_E is created by

Table 1: The key selection table.

Key	0	1	2
$\text{key}_r(i)$	$sk_1(i) \oplus sk_2(i)$	$sk_1(i) \oplus sk_3(i)$	$sk_2(i) \oplus sk_5(i)$
$\text{key}_g(i)$	$sk_3(i) \oplus sk_5(i)$	$sk_4(i) \oplus sk_5(i)$	$sk_1(i) \oplus sk_4(i)$
$\text{key}_b(i)$	$sk_4(i) \oplus sk_6(i)$	$sk_2(i) \oplus sk_6(i)$	$sk_3(i) \oplus sk_6(i)$

the composition of the three encrypted grayscale images.

4.2. Design of the Decryption Algorithm

4.2.1. Decryption Algorithm

Step 1. Separate the encrypted image I_E into red, green, and blue grayscale images, and set r'_i, g'_i, and $b'_i (i = 1, 2, \ldots, mn)$ to represent the i-th pixel value of these grayscale images, respectively. The decryption begins from the back to the front, that is to say that the mn-th pixel is firstly decrypted.

Step 2. With the same initial values with the encryption process, the sequences $(y_1(i), y_2(i), y_3(i), y_4(i))$ are generated by fractional-order dynamic system (7). Next, it can be calculated that $s(mn) = 0$ by equation (15). Then, the keys $(\text{key}_r(mn), \text{key}_g(mn), \text{key}_b(mn))$ can be obtained by equation (13) and $s(mn) = 0$. Finally, we can get r_{mn}, g_{mn}, and b_{mn} after the following equation:

$$\begin{cases} r_i = \left(r'_i \oplus \text{key}_r(i) - r'_{i-1}\right) \bmod 256, \\ g_i = \left(g'_i \oplus \text{key}_g(i) - g'_{i-1}\right) \bmod 256, \\ b_i = \left(b'_i \oplus \text{key}_b(i) - b'_{i-1}\right) \bmod 256. \end{cases} \tag{18}$$

Step 3. With values of r_{mn}, g_{mn}, and b_{mn} and $s(mn) = 0$, the value of $s(mn-1)$ can be computed by equations (14) and (15). Then, the $(mn-1)$-th pixel can be decrypted. Similarly, it is finished until the values of r_1, g_1, and b_1 are decrypted.

Step 4. After repeating the above steps for the same rounds with the encryption process, the decrypted image I' is obtained.

4.2.2. Inverse Permutation Process

Step 1. According to the red, green, and blue components of the color image, the image I' is converted into a grayscale image with size of $m \times 3n$. Then, a binary matrix I'_b with size of $m \times 24n$ is obtained by each pixel of the grayscale image which is changed into an 8-bit array.

Step 2. Because the sum of all the elements with value of 1 in the binary matrix I'_b is equal to one of all the elements with value of 1 in the binary matrix P_b, the value of g is computed by the following equation:

$$g = \frac{\text{sum}(I'_b)}{mn}. \tag{19}$$

Step 3. With the same initial values as permutation process, the sequences $(x_1(i), x_2(i), x_3(i), x_4(i))$ are generated by system (4). Then, the keys key_h and key_v are computed by equations (8) and (9), respectively. Finally, the vectors h' and v' are obtained by equations (11) and (12) separately.

Step 4. According to the array vectors h' and v', the rows and columns of binary image I'_b are inversely permuted, respectively. The image I_b is obtained by this inverse permutation. We convert I_b with size of $m \times 24n$ into the plain color image I whose size is of $m \times n$. Thus, the decryption is achieved completely.

4.3. Experimental Result. The color image named pepper is selected as the plain images, whose size is 197×206. The initial values of fractional-order hyperchaotic system (4) and system (7) are $x_1(0) = 0.67185367890218$, $x_2(0) = 0.24566789543262$, $x_3(0) = 0.15492289843576$, $x_4(0) = 1.32854321678987$, $y_1(0) = 0.98165678567657$, $y_2(0) = 0.12345678901234$, $y_3(0) = 1.65432109876543$, and $y_4(0) = 0.57167689592916$. The experimental results are shown in Figure 6.

4.4. Performance and Security Analysis

4.4.1. Key Space and Sensitivity. In the encryption algorithm, the secret keys are the initial values of the two hyperchaotic systems, that is, $(x_1(0), x_2(0), x_3(0), x_4(0))$ and $(y_1(0), y_2(0), y_3(0), y_4(0))$. Because the maximum precision of these initial values is 10^{-14}, the total key space is that $(10^{14})^8 = 10^{112}$, which is much larger than 2^{100} [25]. Therefore, our algorithm can resist all kinds of brute force attacks.

For the key sensitive test, the tiny change 10^{-14} is selected as the error of these initial values, and it is shown in Table 2. Due to space limitations, only the changes of $x_1(0)$, $x_2(0)$, $y_3(0)$, and $y_4(0)$ were made. The experimental results are shown in Figure 7. It can be seen that these decrypted images are extremely similar to noise and absolutely different from the plain image, and those pixel distribution histograms are uniform. Moreover, we calculate the NPCR and UACI of the original image and recovered images (peppers) with different keys; it is shown in Table 3. It is easy to observe that NPCR is over 99%, and the UACI is close to 33%. It demonstrates that the recovered images with different keys are greatly different from their original form. Therefore, our algorithm is sensitive to the secret key.

4.4.2. χ^2 Test. We compute the χ^2 values of both plain image and encrypted image named Pepper, Flower, Yacht, and Baboon, whose sizes are all 197×206. It is shown in Table 4.

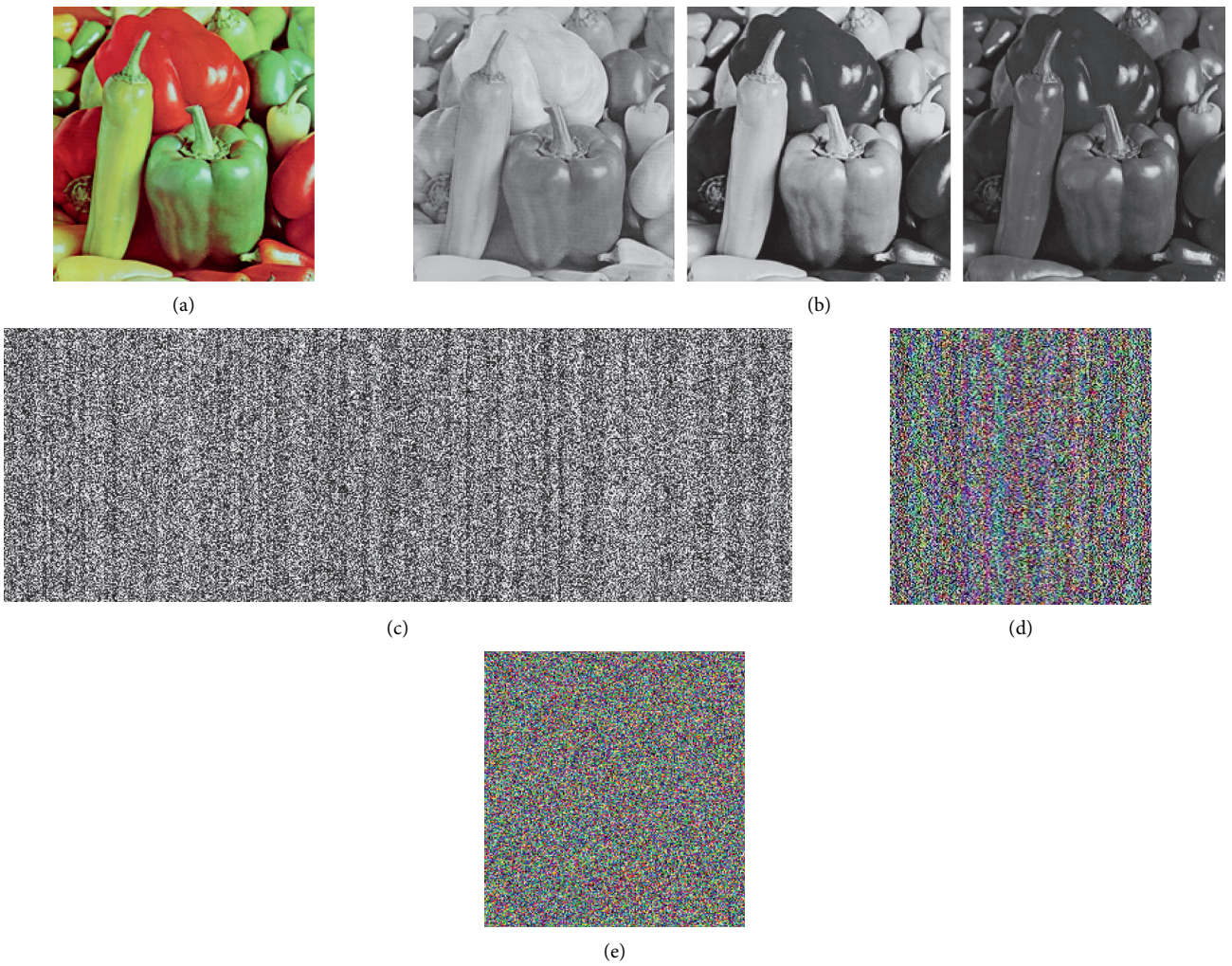

Figure 6: The encryption results of pepper image. (a) The original image. (b) The grayscale image of decomposing Figure 6(a). (c) The image of permuting Figure 6(b). (d) The result of composing Figure 6(c). (e) The encrypted image.

Table 2: The tiny change of secret keys.

Key	Original value	New value
$x_1(0)$	0.67185367890218	$0.67185367890218 + 10^{-14}$
$x_2(0)$	0.24566789543262	$0.24566789543262 - 10^{-14}$
$y_3(0)$	1.65432109876543	$1.65432109876543 + 10^{-14}$
$y_4(0)$	0.57167689592916	$0.57167689592916 - 10^{-14}$

Obviously, the χ^2 values of the ciphered images are far lower than those of the plain images and similar to the algorithm in [26, 27]; they are all within the effective interval [210.7918, 293.2478].

4.4.3. Statistical Analysis. From the plain image and encrypted image, 2500 pairs of adjacent pixels are randomly selected in horizontal, vertical, and diagonal directions, respectively. Then, we calculate the correlation coefficients of two adjacent pixels, which are shown in Table 5. From Table 5, it can be observed that the correlations of two adjacent pixels are close to 1 in the plain images, while the ones of the encrypted images are round 0 and similar to the algorithm in [28, 29]. Therefore, the encryption algorithm can eliminate the correlation of the adjacent pixels.

4.4.4. Information Entropy. We compute the information entropy of the encrypted images according to the red, green, and blue components of the color image, which is shown in Table 6. It can be seen that the information entropy of these ciphered images is all close to the value 8. So, it proves that the unpredictability of the encrypted images is very high.

4.4.5. Differential Attack. To test the differential attack, some color images are encrypted with altering a pixel in the plain images, respectively, and NPCR and UACI are calculated in Table 7. It can be found that the NPCR is over 99%, the UACI is over 33%, and similar to the algorithm in [28–30]. It indicates that our algorithm can resist the differential attack.

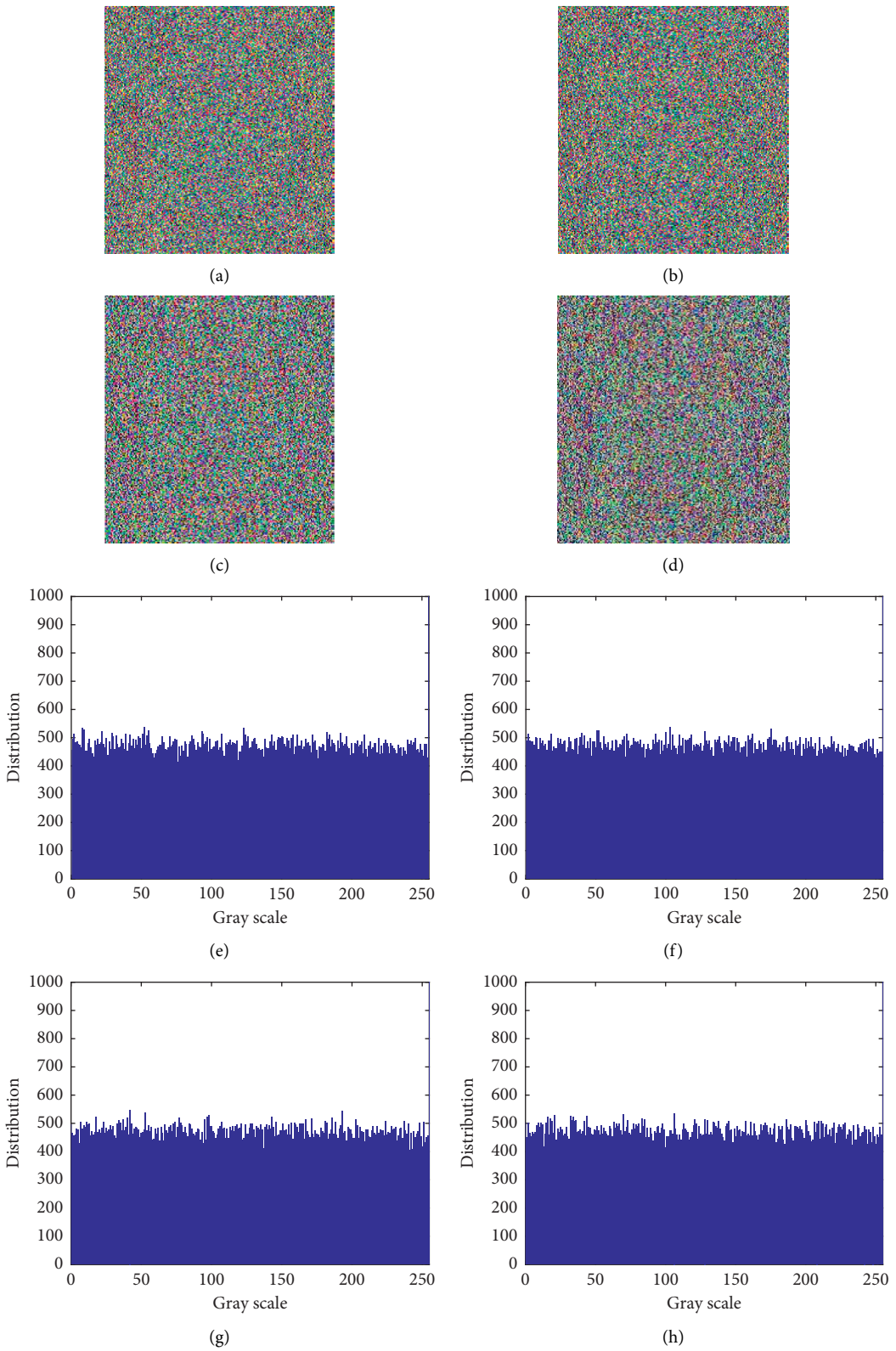

FIGURE 7: The decrypted images in tiny change of keys and their histograms. (a) $x_1(0) = 0.67185367890219$. (b) $x_2(0) = 0.24566789543261$. (c) $y_3(0) = 1.65432109876544$. (d) $y_4(0) = 0.57167689592915$. (e) The pixel distribution histogram of Figure 7(a). (f) The pixel distribution histogram of Figure 7(b). (g) The pixel distribution histogram of Figure 7(c). (h) The pixel distribution histogram of Figure 7(d).

Table 3: The NPCR and UACI of the original image and recovered image (peppers) with different keys.

Image	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
Recovered image with $x_1(0)$	99.4259	99.3569	99.4185	28.3860	32.9807	32.8930
Recovered image with $x_2(0)$	99.3421	99.3864	99.4061	28.4061	32.8305	32.7692
Recovered image with $y_3(0)$	99.3174	99.3618	99.4209	28.2771	32.8916	32.7201
Recovered image with $y_4(0)$	99.3544	99.2755	99.3544	28.1678	32.4912	32.7000

Table 4: The results of the χ^2 test.

χ^2	Plain image			Ciphered image		
	R	G	B	R	G	B
Pepper	35,300	32,679	64,067	258.8352	247.7227	208.7380
Flower	25,554	27,012	47,904	235.1820	250.1199	260.4022
Yacht	18,431	21,044	17,323	259.1406	271.4038	229.4794
Baboon	19,059	27,759	17,654	249.9811	237.2006	219.9287
Pepper in [26]	57,362	62,180	122,870	265.4625	269.3956	289.2321
Image 1 in [27]	—	—	—	230.8105	234.7070	250.3419
Image 2 in [27]	—	—	—	265.7558	286.3242	276.2754

Table 5: Correlation coefficients of the plain image and ciphered image.

Correlation	Horizontal	Vertical	Diagonal
Pepper	0.9373	0.9716	0.9478
Ciphered pepper	0.0021	0.0018	−0.0195
Flower	0.9414	0.9792	0.9769
Ciphered flower	0.0009	0.0173	−0.0194
Lena in [28] (R)	0.95409435	0.97692808	0.92946084
Lena in [28] (G)	0.93859702	0.96847242	0.91318153
Lena in [28] (B)	0.92230178	0.95144503	0.89275171
Ciphered lena in [28] (R)	0.00268849	0.00113425	0.00526812
Ciphered lena in [28] (G)	0.00979889	0.00302981	0.00038029
Ciphered lena in [28] (B)	0.00098796	0.00056287	0.00111043
Lena in [29]	0.9494	0.9667	0.9336
Ciphered lena in [29]	0.0054	0.0035	0.0016

Table 6: The information entropy of encrypted images.

Color image	Red	Green	Blue
Pepper	7.9875	7.9880	7.9876
Flower	7.9882	7.9881	7.9871
Yacht	7.9867	7.9883	7.9874
Baboon	7.9881	7.9882	7.9875

Table 7: The NPCR and UACI of ciphered images.

Image	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
Pepper	99.5762	99.6205	99.5762	33.2831	33.4199	33.5400
Flower	99.6772	99.7142	99.6550	33.4547	33.7477	33.3845
Yacht	99.5269	99.5810	99.5146	33.3787	33.4017	33.4997
Baboon	99.6550	99.6723	99.6747	33.3987	33.3903	33.3644
Lena in [28]	99.98779	99.98779	99.98779	50.17915	50.18009	25.19263
Lena in [29] (avg.)		99.5723			33.3159	
Lena in [30]	99.6231	99.6338	99.6170	33.4747	33.5683	33.3382

5. Conclusion

In this paper, the anticontrol of the fractional-order chaotic system is studied. We give the necessary conditions for the anticontrol of the fractional-order chaotic system. With the same parameters and fractional order, a 3D chaotic system is driven to two new 4D fractional-order hyperchaotic systems, respectively. We compute Lyapunov exponents and bifurcation diagrams of these new fractional dynamic systems.

Based on these two fractional-order hyperchaotic systems, a color image encryption algorithm is designed. In permutation process, the key is related to the plain image, and the key in encryption process is dynamically changing with different plain images and encrypted images. Therefore, our algorithm can resist the chosen plaintext (ciphertext) attacks and overcome the difficulty of key management in the "one time and one secret (one time one key)" scheme. In addition, the security analysis shows that our algorithm has better security. Therefore, it verifies the effectiveness of these fractional dynamic systems for image encryption.

In the future, we will further study on the anticontrol of the fractional-order chaotic system and identify the new chaotic system scientifically by the criteria from the work [31]. In image encryption, the fractional hyperchaotic system could be extended to a computational model for parallel image encryption algorithms.

Data Availability

No data were used to support this study.

Conflicts of Interest

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

Acknowledgments

This research was supported by the National Natural Science Foundation of China (nos. 61662073, 11701061, and 11501074) and the General Research Project of Liaoning Provincial Education Department of China (no. L2015023).

References

[1] G. Chen and D. Lai, "Feedback control of Lyapunov exponents for discrete-time dynamical systems," *International Journal of Bifurcation and Chaos*, vol. 6, no. 7, pp. 1341–1349, 1996.

[2] X. F. Wang, G. Chen, and X. Yu, "Anticontrol of chaos in continuous-time systems via time-delay feedback," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 10, no. 4, pp. 771–779, 2000.

[3] X. Wang, G. Chen, and K. Man, "Making a continuous-time minimum-phase system chaotic by using time-delay feedback," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 5, pp. 641–645, 2001.

[4] Y. Li, G. Chen, and K. S. Tang, "Controlling a unified chaotic system to hyperchaotic," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 52, no. 4, pp. 204–207, 2005.

[5] H. Xi, S. Yu, C. Zhang, and Y. Sun, "Generation and implementation of hyperchaotic chua system via state feedback control," *International Journal of Bifurcation and Chaos*, vol. 22, no. 5, p. 1250119, 2012.

[6] C. Shen, S. Yu, J. Lu, and G. Chen, "A systematic methodology for constructing hyperchaotic systems with multiple positive Lyapunov exponents and circuit implementation," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 3, pp. 854–864, 2014.

[7] C. Shen, S. Yu, J. Lü, and G. Chen, "Constructing hyperchaotic systems at will," *International Journal of Circuit Theory and Applications*, vol. 43, no. 12, pp. 2039–2056, 2015.

[8] H. Deng, T. Li, Q. Wang, and H. Li, "A fractional-order hyperchaotic system and its synchronization," *Chaos, Solitons & Fractals*, vol. 41, no. 2, pp. 962–969, 2009.

[9] J.-M. He and F.-Q. Chen, "A new fractional order hyperchaotic Rabinovich system and its dynamical behaviors," *International Journal of Non-Linear Mechanics*, vol. 95, pp. 73–81, 2017.

[10] Y. Gao, C. Liang, Q. Wu, and H. Yuan, "A new fractional-order hyperchaotic system and its modified projective synchronization," *Chaos, Solitons & Fractals*, vol. 76, pp. 190–204, 2015.

[11] C. Li and G. Chen, "Chaos and hyperchaos in the fractional-order Rössler equations," *Physica A: Statistical Mechanics and Its Applications*, vol. 341, pp. 55–61, 2004.

[12] A. Hajipour, M. Hajipour, and D. Baleanu, "On the adaptive sliding mode controller for a hyperchaotic fractional-order financial system," *Physica A: Statistical Mechanics and Its Applications*, vol. 497, pp. 139–153, 2018.

[13] X.-Y. Wang and J.-M. 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.

[14] L. Pan, W. Zhou, L. Zhou, and K. Sun, "Chaos synchronization between two different fractional-order hyperchaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 6, pp. 2628–2640, 2011.

[15] X. Wu, H. Wang, and H. Lu, "Modified generalized projective synchronization of a new fractional-order hyperchaotic system and its application to secure communication," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 3, pp. 1441–1450, 2012.

[16] A. M. A. El-Sayed, H. M. Nour, A. Elsaid, A. E. Matouk, and A. Elsonbaty, "Dynamical behaviors, circuit realization, chaos control, and synchronization of a new fractional order hyperchaotic system," *Applied Mathematical Modelling*, vol. 40, no. 5-6, pp. 3516–3534, 2016.

[17] 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.

[18] R. Montero-Canela, E. Zambrano-Serrano, E. I. Tamariz-Flores, J. M. Muñoz-Pacheco, and R. Torrealba-Meléndez, "Fractional chaos based-cryptosystem for generating encryption keys in Ad Hoc networks," *Ad Hoc Networks*, vol. 97, Article ID 102005, 2020.

[19] A. Akgul, C. Arslan, and B. Aricioglu, "Design of an interface for random number generators based on integer and fractional order chaotic systems," *Chaos Theory and Applications*, vol. 1, no. 1, pp. 1–18, 2019.

[20] G. Qi, G. Chen, S. Du, Z. Chen, and Z. Yuan, "Analysis of a new chaotic system," *Physica A: Statistical Mechanics and Its Applications*, vol. 352, no. 2-4, pp. 295–308, 2005.

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

[22] M. Caputo, "Linear models of dissipation whose Q is almost frequency independent," *The Geophysical Journal of the Royal Astronomical Society*, vol. 13, no. 5, pp. 529–539, 1967.

[23] D. Matignon, "Stability results for fractional differential equations with application to control processing," *Computational Engineering in System Application*, pp. 963–968, IMACS, Lille, France, 1996.

[24] K. Ramasubramanian and M. Sriram, "A comparative study of computation of Lyapunov spectra with different algorithms," *Physica D: Nonlinear Phenomena*, vol. 139, no. 1-2, pp. 72–86, 2000.

[25] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, FL, USA, 2006.

[26] H. Liu, Y. Zhang, A. Kadir, and Y. Xu, "Image encryption using complex hyper chaotic system by injecting impulse into parameters," *Applied Mathematics and Computation*, vol. 360, pp. 83–93, 2019.

[27] H. Liu, A. Kadir, and J. Liu, "Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system," *Optics and Lasers in Engineering*, vol. 122, pp. 123–133, 2019.

[28] A. G. Radwan, S. K. Abd-El-Hafiz, and S. H. AbdElHaleem, "Image encryption in the fractional-order domain," in *Proceedings of the 2012 International Conference on Engineering and Technology (ICET)*, IEEE, Cairo, Egypt, October 2012.

[29] T. Li, M. Yang, J. Wu, and X. Jing, "A novel image encryption algorithm based on a fractional-order hyperchaotic system and DNA computing," *Complexity*, vol. 2017, Article ID 9010251, 13 pages, 2017.

[30] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, pp. 104–112, 2015.

[31] J. C. Sprott, "A proposed standard for the publication of new chaotic systems," *International Journal of Bifurcation and Chaos*, vol. 21, no. 9, pp. 2391–2394, 2011.