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

1School of Information Engineering, Dalian University, Dalian 116622, China
2School 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

Copyright © 2020 Yujun Niu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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

\[
\begin{align*}
\dot{x} &= a(y - x) + yz, \\
\dot{y} &= cx - y - xz, \\
\dot{z} &= xy - bz,
\end{align*}
\]

(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

\[
\begin{align*}
\frac{d^{q_1}x}{dt^{q_1}} &= a(y - x) + yz, \\
\frac{d^{q_2}y}{dt^{q_2}} &= cx - y - xz, \\
\frac{d^{q_3}z}{dt^{q_3}} &= xy - bz,
\end{align*}
\]

(2)

where \(q_i\) is the fractional order, \(0 < q_i \leq 1 (i = 1, 2, 3).\) 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 equilibrium 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 \((\lambda_1, \lambda_2, \ldots, \lambda_n)\) of the Jacobian matrix of some equilibrium point satisfy

\[
|\arg(\lambda_i)| > \frac{\alpha \pi}{2}, \quad \alpha = \max(q_1, q_2, \ldots, q_n), \quad i = 1, 2, \ldots, n,
\]

(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 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 equilibriums \(S_0(-19.3091, -7.5418, 54.6094),\) 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 equilibriums \(S_1(19.3091, 7.5418, 54.6094)\) 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 equilibrium 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 \(x_i (i = 1, \ldots, 4).\) With the same parameters and fractional order, a new 4-dimensional fractional-order dynamic system is obtained by introducing a linear feedback control term \(\left(\frac{d^{q_i}x_i}{dt^{q_i}}\right) = -63x_2 + r_1x_4\) to the equation of system (2) as follows:

\[
\begin{align*}
\frac{d^{q_1}x_1}{dt^{q_1}} &= a(x_2 - x_1) + x_2x_3, \\
\frac{d^{q_2}x_2}{dt^{q_2}} &= cx_1 - x_2 - x_1x_3 + x_4, \\
\frac{d^{q_3}x_3}{dt^{q_3}} &= x_1x_2 - bx_3, \\
\frac{d^{q_4}x_4}{dt^{q_4}} &= -63x_1 + r_1x_4,
\end{align*}
\]

(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
\[
\mathbf{V} = \begin{bmatrix}
\frac{\partial \mathbf{x}_1}{\partial x_1} & \frac{\partial \mathbf{x}_1}{\partial x_2} & \frac{\partial \mathbf{x}_1}{\partial x_3} & \frac{\partial \mathbf{x}_1}{\partial x_4} \\
\frac{\partial \mathbf{x}_2}{\partial x_1} & \frac{\partial \mathbf{x}_2}{\partial x_2} & \frac{\partial \mathbf{x}_2}{\partial x_3} & \frac{\partial \mathbf{x}_2}{\partial x_4} \\
\frac{\partial \mathbf{x}_3}{\partial x_1} & \frac{\partial \mathbf{x}_3}{\partial x_2} & \frac{\partial \mathbf{x}_3}{\partial x_3} & \frac{\partial \mathbf{x}_3}{\partial x_4} \\
\frac{\partial \mathbf{x}_4}{\partial x_1} & \frac{\partial \mathbf{x}_4}{\partial x_2} & \frac{\partial \mathbf{x}_4}{\partial x_3} & \frac{\partial \mathbf{x}_4}{\partial x_4}
\end{bmatrix} = -\mathbf{a} - \mathbf{b} + r_1 = r_1 - 38.7 < 0
\]

(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 $S_0(0, 0, 0, 0), S_1(0.0487, 0.0088, 0.1508, 5.1141)$, 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:

\[
\mathbf{J} = \begin{bmatrix}
-a & a + 3x_2 & x_2 & 0 \\
2c - x_3 & -1 & -x_1 & 1 \\
x_2 & x_1 & -b & 0 \\
-63 & 0 & 0 & r_1
\end{bmatrix} = \begin{bmatrix}
-a & a & 0 & 0 \\
c & -1 & 0 & 1 \\
0 & 0 & -b & 0 \\
-63 & 0 & 0 & r_1
\end{bmatrix}
\]

(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 $\lambda_4 = -2.6666$. 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, $S_1(0.0487, 0.0088, 0.1508, 5.1141)$ 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 $-1.5 \leq r_1 \leq 2$, 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 $-1.05 \leq r_1 \leq 1.7$, fractional-order system (4) is hyperchaotic with satisfying $\lambda_1 > 0, \lambda_2 > 0, \lambda_3 = 0$, 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:

\[
\begin{aligned}
\frac{d^{\alpha}y_1}{d\tau^{\alpha}} &= a(y_2 - y_1) + y_2y_3, \\
\frac{d^{\alpha}y_2}{d\tau^{\alpha}} &= cy_1 - y_2y_3 + y_4, \\
\frac{d^{\alpha}y_3}{d\tau^{\alpha}} &= y_1y_2 - by_3, \\
\frac{d^{\alpha}y_4}{d\tau^{\alpha}} &= -y_1y_3 + r_2y_4,
\end{aligned}
\]

(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 $0.5 \leq r_2 \leq 2.5$, 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 $1.1 \leq r_2 \leq 1.95$, 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 permuted 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 $-1.5 \leq r_1 \leq 2$. (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 $0.5 \leq r_2 \leq 2.5$. (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 \(\text{key}_h\) and \(\text{key}_v\) are produced by equations (8) and (9), respectively:

\[
\text{key}_h(i) = \text{abs}(x_1(i) + x_2(i) \times g) \mod 256, \quad i = 1, 2, \ldots, m,
\]

\[
\text{key}_v(j) = \text{abs}(x_3(j) \times g + x_4(j)) \mod 256, \quad j = 1, 2, \ldots, 24n,
\]

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

\[
g = \frac{\text{sum}(P_b)}{mn},
\]

where \(\text{sum}(P_b)\) is the sum of all the elements with value of 1 in the matrix \(P_b\). Therefore, the key vectors \(\text{key}_h\) and \(\text{key}_v\) 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 \(P_c\):

\[
h'(i) = h(\text{floor}(\text{key}_h(i) \times n) \mod m), \quad i = 1, 2, \ldots, m,
\]

\[
v'(j) = v(\text{floor}(\text{key}_v(j) \times 24n) \mod j), \quad j = 1, 2, \ldots, 24n.
\]

4.1.2. Encryption Algorithm. In this stage, the permuted 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:

\[
sk_j(i) = (\text{abs}(y_u(i) + y_v(i))) - \text{floor}(\text{abs}(y_u(i) + y_v(i))) \times 10^{14} \mod 256, \quad j = 1, \ldots, 6,
\]

where \(u, v \in \{1, 2, 3, 4\}\) and \(u \neq v\). The encryption key sequences \((\text{key}_h(i), \text{key}_h(i), \text{key}_h(i), \text{key}_h(i))\) 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):

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

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

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 \(b'_i\):

\[
\begin{align*}
  r'_i & = \left( (r_i + r'_{i-1}) \mod 256 \right) \oplus \text{key}_r(i), \\
  g'_i & = \left( (g_i + g'_{i-1}) \mod 256 \right) \oplus \text{key}_g(i), \\
  b'_i & = \left( (b_i + b'_{i-1}) \mod 256 \right) \oplus \text{key}_b(i),
\end{align*}
\]

where

\[
\begin{align*}
  r'_0 & = \left( \sum_{j=1}^{mn} r_j + sk_1(1) \right) \mod 256, \\
  g'_0 & = \left( \sum_{j=1}^{mn} g_j + sk_2(1) \right) \mod 256, \\
  b'_0 & = \left( \sum_{j=1}^{mn} b_j + sk_3(1) \right) \mod 256.
\end{align*}
\]

Step 4. Repeat the aforementioned steps appropriately.

In the end, the encrypted color image \(I_E\) is created by
4.2. Design of the Decryption Algorithm

4.2.1. Decryption Algorithm

Step 1. Separate the encrypted image $I_b$ 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 $(key_h (mn), key_g (mn), key_b (mn))$ 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:

\[
\begin{cases}
    r_i = (r'_i \oplus key_r (i) - r'_{i-1}) \mod 256, \\
    g_i = (g'_i \oplus key_g (i) - g'_{i-1}) \mod 256, \\
    b_i = (b'_i \oplus key_b (i) - b'_{i-1}) \mod 256.
\end{cases}
\]

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:

\[ g = \frac{\sum (I'_b)}{mn} \]

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 $197 \times 206$. The initial values of fractional-order hyperchaotic system (4) and system (7) are $x_1 (0) = 0.67185367890218$, $x_2 (0) = 0.24566789543262$, $x_3 (0) = 0.15492289843576$, $x_4 (0) = 1.32854321678987$, $y_1 (0) = 0.9816576857657$, $y_2 (0) = 0.12345678901234$, $y_3 (0) = 1.65432109876543$, 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 $x_1 (0)$, $x_2 (0)$, $y_2 (0)$, 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. $\chi^2$ Test

We compute the $\chi^2$ values of both plain image and encrypted image named Pepper, Flower, Yacht, and Baboon, whose sizes are all $197 \times 206$. It is shown in Table 4.

---

Table 1: The key selection table.

<table>
<thead>
<tr>
<th>Key</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>key_0</td>
<td>$sk_0 (i) \oplus sk_1 (i)$</td>
<td>$sk_0 (i) \oplus sk_1 (i)$</td>
<td>$sk_0 (i) \oplus sk_1 (i)$</td>
</tr>
<tr>
<td>key_1</td>
<td>$sk_2 (i) \oplus sk_3 (i)$</td>
<td>$sk_2 (i) \oplus sk_3 (i)$</td>
<td>$sk_2 (i) \oplus sk_3 (i)$</td>
</tr>
<tr>
<td>key_2</td>
<td>$sk_4 (i) \oplus sk_5 (i)$</td>
<td>$sk_4 (i) \oplus sk_5 (i)$</td>
<td>$sk_4 (i) \oplus sk_5 (i)$</td>
</tr>
</tbody>
</table>

---

the composition of the three encrypted grayscale images.
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.

<table>
<thead>
<tr>
<th>Image</th>
<th>NPCR (%)</th>
<th>UACI (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Recovered image with $x_1(0)$</td>
<td>99.4259</td>
<td>99.3569</td>
</tr>
<tr>
<td>Recovered image with $x_2(0)$</td>
<td>99.3421</td>
<td>99.3864</td>
</tr>
<tr>
<td>Recovered image with $y_1(0)$</td>
<td>99.3174</td>
<td>99.3618</td>
</tr>
<tr>
<td>Recovered image with $y_2(0)$</td>
<td>99.3544</td>
<td>99.2755</td>
</tr>
</tbody>
</table>

### Table 4: The results of the $\chi^2$ test.

<table>
<thead>
<tr>
<th>$\chi^2$</th>
<th>Plain image</th>
<th>Ciphered image</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Pepper</td>
<td>35,300</td>
<td>32,679</td>
</tr>
<tr>
<td>Flower</td>
<td>25,554</td>
<td>27,012</td>
</tr>
<tr>
<td>Yacht</td>
<td>18,431</td>
<td>21,044</td>
</tr>
<tr>
<td>Baboon</td>
<td>19,059</td>
<td>27,759</td>
</tr>
<tr>
<td>Pepper in [26]</td>
<td>57,362</td>
<td>62,180</td>
</tr>
<tr>
<td>Image 1 in [27]</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Image 2 in [27]</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Correlation</th>
<th>Horizontal</th>
<th>Vertical</th>
<th>Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pepper</td>
<td>0.9373</td>
<td>0.9716</td>
<td>0.9478</td>
</tr>
<tr>
<td>Ciphered pepper</td>
<td>0.0021</td>
<td>0.0018</td>
<td>−0.0195</td>
</tr>
<tr>
<td>Flower</td>
<td>0.9414</td>
<td>0.9792</td>
<td>0.9769</td>
</tr>
<tr>
<td>Ciphered flower</td>
<td>0.0009</td>
<td>0.0173</td>
<td>−0.0194</td>
</tr>
<tr>
<td>Lena in [28] (R)</td>
<td>0.95409435</td>
<td>0.97692808</td>
<td>0.92946084</td>
</tr>
<tr>
<td>Lena in [28] (G)</td>
<td>0.93859702</td>
<td>0.96847242</td>
<td>0.91318153</td>
</tr>
<tr>
<td>Lena in [28] (B)</td>
<td>0.92230178</td>
<td>0.95144503</td>
<td>0.89275171</td>
</tr>
<tr>
<td>Ciphered lena in [28] (R)</td>
<td>0.00268849</td>
<td>0.00113425</td>
<td>0.00526812</td>
</tr>
<tr>
<td>Ciphered lena in [28] (G)</td>
<td>0.00979889</td>
<td>0.00302981</td>
<td>0.00038029</td>
</tr>
<tr>
<td>Ciphered lena in [28] (B)</td>
<td>0.00098796</td>
<td>0.00056287</td>
<td>0.0011043</td>
</tr>
<tr>
<td>Lena in [29]</td>
<td>0.9494</td>
<td>0.9667</td>
<td>0.9336</td>
</tr>
<tr>
<td>Ciphered lena in [29]</td>
<td>0.0054</td>
<td>0.0035</td>
<td>0.0016</td>
</tr>
</tbody>
</table>

### Table 6: The information entropy of encrypted images.

<table>
<thead>
<tr>
<th>Color image</th>
<th>Red</th>
<th>Green</th>
<th>Blue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pepper</td>
<td>7.9875</td>
<td>7.9880</td>
<td>7.9876</td>
</tr>
<tr>
<td>Flower</td>
<td>7.9882</td>
<td>7.9881</td>
<td>7.9871</td>
</tr>
<tr>
<td>Yacht</td>
<td>7.9887</td>
<td>7.9883</td>
<td>7.9874</td>
</tr>
<tr>
<td>Baboon</td>
<td>7.9881</td>
<td>7.9882</td>
<td>7.9875</td>
</tr>
</tbody>
</table>

### Table 7: The NPCR and UACI of ciphered images.

<table>
<thead>
<tr>
<th>Image</th>
<th>NPCR (%)</th>
<th>UACI (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Pepper</td>
<td>99.5762</td>
<td>99.6205</td>
</tr>
<tr>
<td>Flower</td>
<td>99.6772</td>
<td>99.7142</td>
</tr>
<tr>
<td>Yacht</td>
<td>99.5269</td>
<td>99.5810</td>
</tr>
<tr>
<td>Baboon</td>
<td>99.6550</td>
<td>99.6723</td>
</tr>
<tr>
<td>Lena in [29] (avg.)</td>
<td>99.5723</td>
<td>99.5723</td>
</tr>
</tbody>
</table>
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


