scientific reports

OPEN

A new image encryption scheme based on fractional-order hyperchaotic system and multiple image fusion

Xinyu Gao[1], Jiawu Yu[1✉], Santo Banerjee[2✉], Huizhen Yan[1] & Jun Mou[1✉]
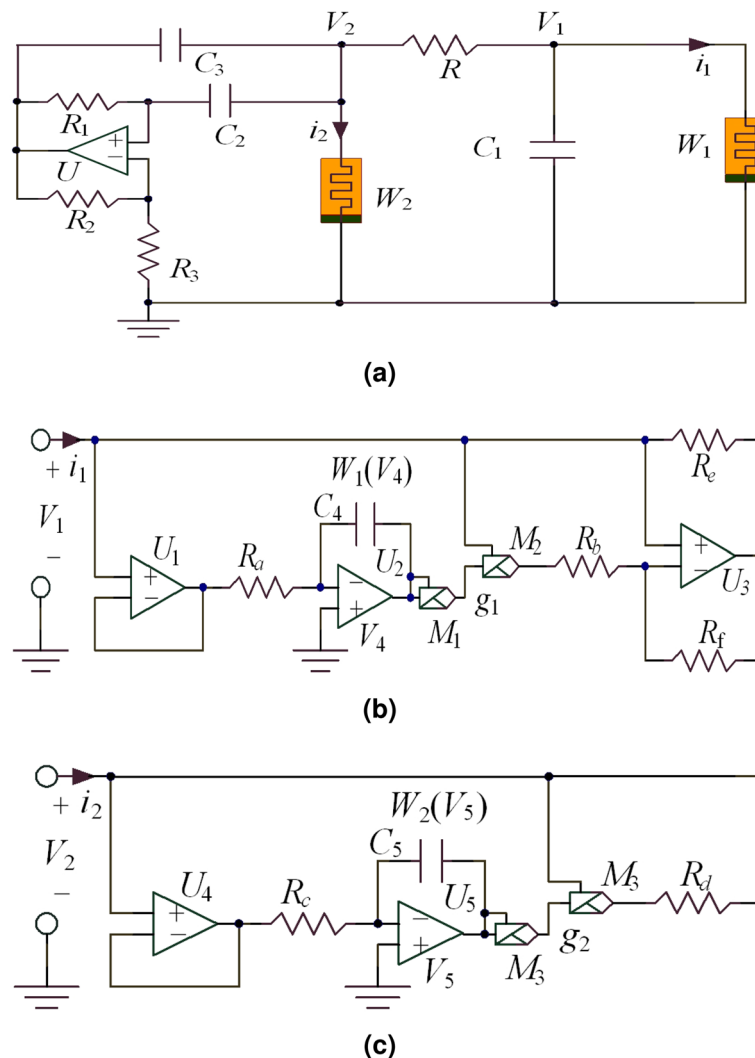
A multi-image encryption scheme based on the fractional-order hyperchaotic system is designed in this paper. The chaotic characteristics of this system are analyzed by the phase diagram, Lyapunov exponent and bifurcation diagram. According to the analyses results, an interesting image encryption algorithm is proposed. Multiple grayscale images are fused into a color image using different channels. Then, the color image is scrambled and diffused in order to obtain a more secure cipher image. The pixel confusion operation and diffusion operation are assisted by fractional hyperchaotic system. Experimental simulation and test results indicate that the devised multi-image encryption scheme can effectively encrypt multiple images, which increase the efficiency of image encryption and transmission, and have good security performance.

In the era of big data, picture information is widely spread on the network, and the security of picture information is also widely concerned[1]. Conventional encryption schemes such as AES, DES encrypt textual data and do not apply to the encryption of images[2–4]. New image encryption algorithms, especially chaos-based encryption algorithms, are under increasingly investigation. Lorentz discovered chaotic attractors in 1963, and in 1997, Fridrich first applied chaotic systems to digital image encryption[5–8]. Chaotic systems are widely used in image encryption and have become a hot research topic in the field of secure communication because of their sensitivity to initial values and irregular internal random motion in deterministic systems[1,9–16]. Compared with ordinary chaotic systems, hyperchaotic systems have more complex dynamics and greater sensitivity and are more suitable for image encryption[17–22]. The fractional-order chaotic system is also more secure because the key space is increased by adding system variables[2,23–28]. Therefore, in this encryption scheme, the fractional-order hyperchaotic system is used for image encryption.

The prerequisite for employing fractional-order chaotic systems is to be able to solve them out. Commonly used methods for solving fractional order chaotic systems are time domain-frequency domain solution algorithms, prediction-correction algorithms, and Adomian decomposition method(ADM)[29,30]. The ADM is widely used due to the advantages of fast convergence and high solution accuracy. However, in the case of conformable fractional calculus, the conformable ADM (CADM) is needed to obtain the digital solution of the chaotic system[31,32].

Another noteworthy point is that single-image encryption is fast but inefficient[21]. Multi-image encryption can encrypt two or more images at a time with the same computational complexity, which has increased the effectiveness of image encryption[33–37]. Many multi-image encryption schemes are already proposed by scholars. Combined with nonlinear fractional Merlin transform and discrete cosine transform, Pan et al. proposed an optical multi-image encryption scheme[38]. On this basis, Zhou et al. proposed a dual image encryption algorithm based on co-sparse representation and random pixel exchange[39]. Zhang et al. proposed a multi-image encryption scheme to encrypt the arbitrary number of images[37] and by using a DNA encoding encryption algorithm to accomplish encrypt multiple images simultaneously[35]. There also some scholars proposed the encryption schemes that can encrypt arbitrary size multiple images or a batch of images[40–43]. Huang et al. proposed a double-image encryption algorithm based on compression-sensing, which reduces data space while improving encryption efficiency[44]. These encryption schemes all use chaotic systems, which greatly improve the randomness of the encrypted image data and make the encryption schemes withstand a certain level of hacking[40,45]. However, some

[1]School of Information Science and Engineering, Dalian Polytechnic University, Dalian 116034, China. [2]Department of Mathematical Sciences, Giuseppe Luigi Lagrange, Politecnico di Torino, Corso Duca degli Abruzzi 24, Torino, Italy. ✉email: yujiawu_dlpu@sina.com; santoban@gmail.com; moujun@csu.edu.cn

Figure 1. Memristive circuit, (**a**) BPF memristive Chua's circuit, (**b**) equivalent circuit for the memristor W_1, (**c**) equivalent circuit for the memristor W_2.

of the encryption schemes still have the problem of weak security or lack of efficiency. For this reason, a new encryption scheme based on fractional-order hyperchaotic systems and multi-image fusion is proposed[46–51]. The application of fractional-order hyperchaotic system makes the pseudo-random sequence more complex and thus allows for a more secure encryption algorithm[52]. The fusion of multiple images allows image encryption efficiency to be improved.

The remaining part of the paper is arranged as the following. "Characteristic analysis of a fractional-order hyperchaotic system" section, the circuit and the dynamic analysis of chaotic system are given. The encryption algorithm which includes scrambling and diffusion is shown in "The complete encryption scheme" section. "Decryption scheme" section introduces the complete encryption and decryption scheme. "Performance analysis" section illustrates the simulation results and some security analyses. In the last section "Conclusion", this paper ends with concluding remarks.

Characteristic analysis of a fractional-order hyperchaotic system

Fractional-order memristive hyperchaotic circuit. A new two-memristor circuit based on band pass filter (BPF) and Chua's circuit is obtained as shown in Fig. 1a. The two equivalent circuits of two memristors W_1 and W_2 are shown in Fig. 1b, c.

For the Fig. 1b, V_1 and i_1 represent the input voltage and the input current, V_4 is the node voltage of the integrator U_2 output. Therefore, the memristor W_1 can be expressed as

$$\begin{cases} i_1 = W_1(V_4)V_1 = -\frac{1}{R_b}(1 - m_1 V_4{}^2)V_1 \\ \frac{dV_4}{dt} = f(V_1) = -\frac{1}{R_a C_4} \end{cases} \tag{1}$$

where, m_1 represent the total gain of multipliers M_1 and M_2. The fluxϕ_1(t) of the memristor W_1 is

2

$$\varphi_1(t) = \int_{-\infty}^{t} V_1(\tau)d(\tau) = -R_a C_4 V_4(t) \tag{2}$$

For the Fig. 1c, V_2 and i_2 represent the input voltage and the input current, V_5 means that the node voltage of the integrator U_5 output. Therefore, the memristor W_2 is expressed as

$$\begin{cases} i_2 = W_2(V_5)V_2 = -\frac{1}{R_d}(1 - m_2 V_5{}^2)V_2 \\ \frac{dV_5}{dt} = f(V_2) = -\frac{1}{R_c C_5} \end{cases} \tag{3}$$

where, m_2 represent the total gain of multipliers M_3 and M_4. The flux $\phi_2(t)$ of the memristor W_2 is

$$\varphi_2(t) = \int_{-\infty}^{t} V_2(\tau)d(\tau) = -R_c C_5 V_5(t) \tag{4}$$

Chaotic system. According to the Kirchhoff's circuit laws, current-voltage relation of capacitors and memristor model, we get the they mathematical model is

$$\begin{cases} \frac{dV_1}{dt} = -\frac{1}{RC_1}(V_1 - V_2) + \frac{1}{R_b C_1}(1 - m_1 V_4{}^2)V_1 \\ \frac{dV_2}{dt} = -\frac{1}{RC_2}(V_1 - V_2) + \frac{1}{R_d C_1}(1 - m_2 V_5{}^2)V_2 - \frac{2s+1}{(s+1)R_1 C_2}V_3 \\ \frac{dV_3}{dt} = -\frac{s+1}{RC_3}(V_1 - V_2) + \frac{s+1}{R_d C_3}(1 - m_2 V_5{}^2)V_2 - \frac{2}{R_1 C_3}V_3 \\ \frac{dV_4}{dt} = -\frac{1}{R_a C_4}V_1 \\ \frac{dV_5}{dt} = -\frac{1}{R_c C_5}V_2 \end{cases} \tag{5}$$

where, $s = R_3/R_2$.

For the Eq. (5), introducing the new variables and scaling the circuit parameters as

$$\begin{cases} x = V_1, y = V_2, z = V_3, w = V_4, u = V_5 \\ C = C_2 = C_3, R_a C_4 = R_c C_5 \\ c = \frac{C}{C_1}, e = \frac{RC}{R_b C_1}, g = \frac{R}{R_d}, n = \frac{R}{R_1}, p = \frac{RC}{R_a C_4} \end{cases} \tag{6}$$

According to Eq. (6), the Eq. (5) becomes to

$$\begin{cases} \dot{x} = -c(x - y) + e(1 - m_1 w^2)x \\ \dot{y} = -s(x - y) + sg(1 - m_2 u^2)y - (2s + 1)/(s + 1)nz \\ \dot{z} = -(s + 1)(x - y) + (s + 1)g(1 - m_2 u^2)y - 2nz \\ \dot{w} = -px \\ \dot{u} = -py \end{cases} \tag{7}$$

Based on Eq. (7), the fractional-order memristive hyperchaotic circuit system is denoted by

$$\begin{cases} {}^*D_{t_0}^q x = -c(x - y) + e(1 - m_1 w^2)x \\ {}^*D_{t_0}^q y = -s(x - y) + sg(1 - m_2 u^2)y - (2s + 1)/(s + 1)nz \\ {}^*D_{t_0}^q z = -(s + 1)(x - y) + (s + 1)g(1 - m_2 u^2)y - 2nz \\ {}^*D_{t_0}^q w = -px \\ {}^*D_{t_0}^q u = -py \end{cases} \tag{8}$$

where, q is order of the equation.

According to the CADM[43] algorithm, the linear and nonlinear terms of the fractional-order system are obtained as follows

$$\begin{bmatrix} Lx \\ Ly \\ Lz \\ Lw \\ Lu \end{bmatrix} = \begin{bmatrix} (e - c)x + cy \\ -sx + sy(g + 1) - (2s + 1)/(s + 1)nz \\ -(s + 1)x + (s + 1)y(g + 1) - 2nz \\ -px \\ -py \end{bmatrix}, \begin{bmatrix} Nx \\ Ny \\ Nz \\ Nw \\ Nu \end{bmatrix} = \begin{bmatrix} -em_1 w^2 x \\ -sgm_2 u^2 y \\ -(s + 1)gm_2 u^2 y \\ 0 \\ 0 \end{bmatrix} \tag{9}$$

The before five Adomian polynomials for the nonlinear parts $-cm_1 w_2$, $-sgm_2$, $-u_2$ and $-(s+1)gm_2 u_2$ are

$$
\begin{cases}
A^0_{-cm_1x(w)^2} = -cm_1x^0(w^0)^2 \\
A^1_{-cm_1x(w)^2} = -cm_1x^1(w^0)^2 - 2cm_1x^1w^1w^0 \\
A^2_{-cm_1x(w)^2} = -cm_1x^2(w^0)^2 - 2cm_1x^1w^1w^0 - 2cm_1x^1w^2w^0 - cm_1x^0(w^1)^2 \\
A^3_{-cm_1x(w)^2} = -cm_1x^3(w^0)^2 - 2cm_1x^2w^1w^0 - 2cm_1x^0w^3w^0 - 2cm_1x^0w^2w^1 \\
\qquad\qquad\; -2cm_1x^1w^2w^0 - cm_1x^1(w^1)^2 \\
A^4_{-cm_1x(w)^2} = -cm_1x^4(w^0)^2 - 2cm_1x^3w^1w^0 - 2cm_1x^2w^0w^2 - 2cm_1x^1w^2w^1 \\
\qquad\qquad\; -2cm_1x^1w^3w^0 - 2cm_1x^0w^4w^0 - 2cm_1x^0w^3w^0 - 2cm_1x^2(w^1)^2 \\
\qquad\qquad\; -2cm_1x^0(w^2)^2
\end{cases}
\tag{10}
$$

$$
\begin{cases}
A^0_{-sgm_2y(u)^2} = -sgm_2y^0(u^0)^2 \\
A^1_{-sgm_2y(u)^2} = -sgm_2y^1(u^0)^2 - 2sgm_2y^1u^1u^0 \\
A^2_{-sgm_2y(u)^2} = -sgm_2y^2(u^0)^2 - 2sgm_2y^1u^1u^0 - 2sgm_2y^1u^2u^0 - sgm_2y^0(u^1)^2 \\
A^3_{-sgm_2y(u)^2} = -sgm_2y^3(u^0)^2 - 2sgm_2y^2u^0u^1 - 2sgm_2y^0u^3u^0 - 2sgm_2y^0u^2u^1 \\
\qquad\qquad\; -2sgm_2y^1u^2u^0 - sgm_2y^1(u^1)^2 \\
A^4_{-sgm_2y(u)^2} = -sgm_2y^4(u^0)^2 - 2sgm_2y^3u^0u^1 - 2sgm_2y^2u^0u^2 - 2sgm_2y^1u^2u^1 \\
\qquad\qquad\; -2sgm_2y^1u^3u^0 - 2sgm_2y^0u^4u^0 - 2sgm_2y^0u^3u^0 - 2sgm_2y^2(u^1)^2 \\
\qquad\qquad\; -sgm_2y^0(u^2)^2
\end{cases}
\tag{11}
$$

$$
\begin{cases}
A^0_{-(s+1)gm_2y(u)^2} = -(s+1)gm_2y^0(u^0)^2 \\
A^1_{-(s+1)gm_2y(u)^2} = -(s+1)gm_2y^1(u^0)^2 - 2(s+1)gm_2y^1u^1u^0 \\
A^2_{-(s+1)gm_2y(u)^2} = -(s+1)gm_2y^2(u^0)^2 - 2(s+1)gm_2y^1u^1u^0 - 2(s+1)gm_2y^1u^2u^0 - (s+1)gm_2y^0(u^1)^2 \\
A^3_{-(s+1)gm_2y(u)^2} = -(s+1)gm_2y^3(u^0)^2 - 2(s+1)gm_2y^2u^0u^1 - 2(s+1)gm_2y^0u^3u^0 - 2(s+1)gm_2y^0u^2u^1 \\
\qquad\qquad\; -2(s+1)gm_2y^1u^2u^0 - (s+1)gm_2y^1(u^1)^2 \\
A^4_{-(s+1)gm_2y(u)^2} = -(s+1)gm_2y^4(u^0)^2 - 2(s+1)gm_2y^3u^0u^1 - 2(s+1)gm_2y^2u^0u^2 - 2(s+1)gm_2y^1u^2u^1 \\
\qquad\qquad\; -2(s+1)gm_2y^1u^3u^0 - 2(s+1)gm_2y^0u^4u^0 - 2(s+1)gm_2y^0u^3u^0 - 2(s+1)gm_2y^2(u^1)^2 \\
\qquad\qquad\; -(s+1)gm_2y^0(u^2)^2
\end{cases}
\tag{12}
$$

If the initial conditions are set as $x0$, $y0$, $z0$, $w0$, $u0$, then the first term is

$$
\begin{cases}
x^0 = x(t_0) \\
y^0 = y(t_0) \\
z^0 = w(t_0) \\
w^0 = w(t_0) \\
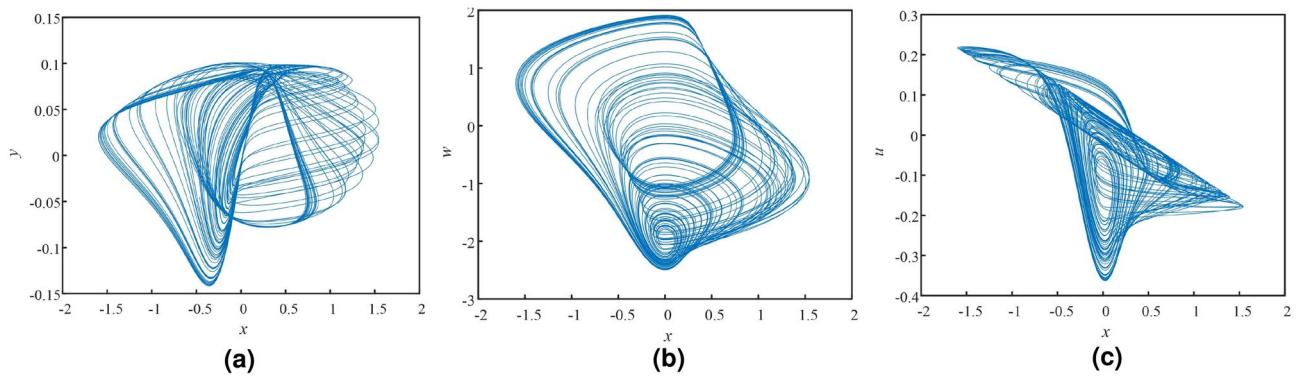u^0 = u(t_0)
\end{cases}
\tag{13}
$$

Let

$$
\begin{cases}
c^0_1 = x^0 \\
c^0_2 = y^0 \\
c^0_3 = w^0 \\
c^0_4 = w^0 \\
c^0_5 = u^0
\end{cases}
\tag{14}
$$

We can get the coefficients of other term as follows

$$
\begin{cases}
c^1_1 = -c(c^0_1 - c^0_2) + ec^0_1 - em_1(c^0_1(c^0_4)^2) \\
c^1_2 = -s(c^0_1 - c^0_2) + sgc^0_2 - scm_2(c^0_2(c^0_5)^2) - \frac{2s+1}{s+1}nc^0_3 \\
c^1_3 = -(s+1)(c^0_1 - c^0_2) + (s+1)gc^0_2 - (s+1)gm_2(c^0_2(c^0_5)^2) - 2nc^0_3 \\
c^1_4 = -pc^0_1 \\
c^1_5 = -pc^0_2
\end{cases}
\tag{15}
$$

$$
\begin{cases}
c^2_1 = -c(c^1_1 - c^1_2) + ec^1_1 - em_1(c^1_1(c^0_4)^2 + 2c^0_1c^1_4c^0_4) \\
c^2_2 = -s(c^1_1 - c^1_2) + sgc^1_2 - scm_2(c^1_2(c^0_5)^2 + 2c^0_2c^1_5c^0_5) - \frac{2s+1}{s+1}nc^1_3 \\
c^2_3 = -(s+1)(c^1_1 - c^1_2) + (s+1)gc^1_2 - (s+1)gm_2(c^1_2(c^0_5)^2 + 2c^0_2c^1_5c^0_5) - 2nc^1_3 \\
c^2_4 = -pc^1_1 \\
c^2_5 = -pc^1_2
\end{cases}
\tag{16}
$$

Figure 2. Phase diagrams of fractional-order hyperchaotic system, (**a**) x–y plan, (**b**) x–w plan, (**c**) x–u plan.

$$
\begin{cases}
c_1^3 = -c(c_1^2 - c_2^2) + ec_1^2 - em_1(c_1^2(c_4^0)^2) - em_1(4c_1^1 c_4^1 c_4^0 + 2c_1^0 c_4^2 c_4^0 + 4c_4^0(c_4^1)^2) \\
c_2^3 = -s(c_1^2 - c_2^2) + sgc_2^2 - scm_2(c_2^2(c_5^0)^2) - sgm_2(4c_2^1 c_5^1 c_5^0 + 4c_2^0(c_5^1)^2) - \frac{2s+1}{s+1} nc_3^2 \\
c_3^3 = -(s+1)(c_1^2 - c_2^2) + (s+1)gc_2^2 - (s+1)gm_2(c_2^2(c_5^0)^2) - (s+1)gm_2 - (4c_2^1 c_5^1 c_5^0 \\
\qquad + 4c_2^0(c_5^1)^2 + 2c_2^0 c_5^2 c_5^0)2nc_3^2 \\
c_4^3 = -pc_1^2 \\
c_5^3 = -pc_2^2
\end{cases}
\tag{17}
$$

$$
\begin{cases}
c_1^4 = -c(c_1^3 - c_2^3) + ec_1^3 - em_1(c_1^3(c_4^0)^2 + 6c_1^2 c_4^0 c_4^1) \\
\qquad - em_1(6(c_1^1 c_4^2 c_4^0 + c_1^0 c_4^1 c_4^2 - c_1^1(c_4^1)^2) - 2c_1^0 c_4^3 c_4^0) \\
c_2^4 = -s(c_1^3 - c_2^3) + sgc_2^3 - scm_2(c_2^3(c_5^0)^2 + 6c_2^2 c_5^0 c_5^1) \\
\qquad - sgm_2(6(c_2^1 c_5^2 c_5^0 + c_2^0 c_5^1 c_5^2 - 2c_2^0 c_5^3 c_5^0) - 2c_2^0 c_5^3 c_5^0) - \frac{2s+1}{s+1} nc_3^3 \\
c_3^4 = -(s+1)(c_1^3 - c_2^3) + (s+1)gc_2^3 - (s+1)gm_2(c_2^3(c_5^0)^2 + 6c_2^2 c_5^0 c_5^1) \\
\qquad - (s+1)gm_2(6(c_2^1 c_5^2 c_5^0 + c_2^0 c_5^1 c_5^2 - c_2^1(c_5^1)^2) + 2c_2^0 c_5^3 c_5^0) - 2nc_3^3 \\
c_4^4 = -pc_1^3 \\
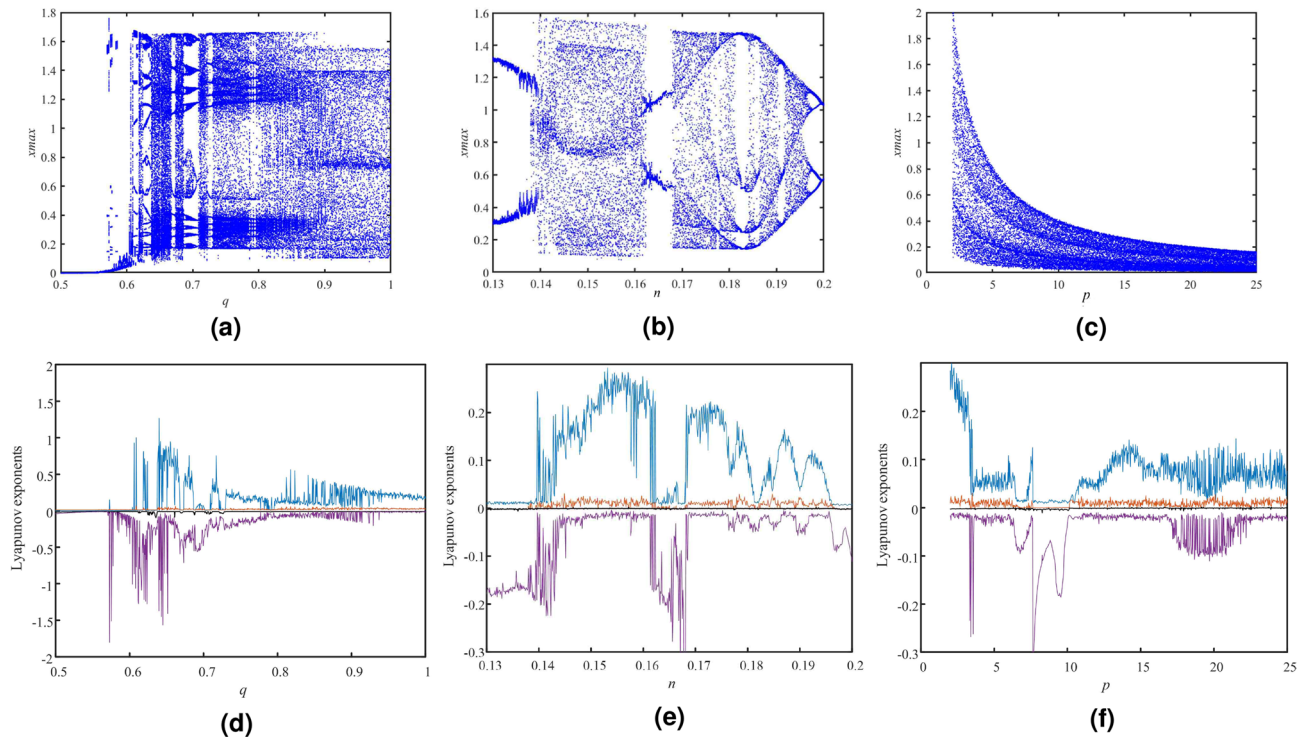c_5^4 = -pc_2^3
\end{cases}
\tag{18}
$$

The CADM solution of the fractional-order memristive hyperchaotic circuit system is

$$
x_j(t) = \sum_{i=0}^{4} c_j^i \frac{(t - t_0)^{iq}}{i! q^i}
\tag{19}
$$

where $j = 1, 2, 3, 4, 5$.

Deploying step size $h = 0.01$, $c = 20$, $e = 150/7$, $g = 15$, $n = 0.15$, $p = 3$, $s = 0.05$, $m_1 = m_2 = 0.1$, $q = 0.97$, the starting value are $[x\ y\ z\ w\ u] = [0.1\ 0\ 0\ 0\ 0]$ for the Eq. (8), the phase diagrams with different planes are shown in Figure 2. The attractor trajectories of the fractional-order hyperchaotic system are distributed over a wide area. The bifurcation diagrams (BDs) andu Lyapunov exponent spectrums (LES) are presented in Figure 3 so that we can study the sensitivity of the system with the varying parameter. We severally fix $q \in (0.5, 1)$, $n \in (0.13, 0.2)$, $p \in (2, 25)$ and other parameters are set as above. The fifth Lyapunov exponent is not shown in Fig. 3d–f, because it is much less than 0. From Fig. 3d, when $q \in (0.5, 0.61)$, there is no Lyapunov exponent greater than 0. With the increase of q, the Lyapunov exponent greater than 0 appears, and the system appears chaotic state. In between there are alternating periodic states and chaotic states appearing. When $n \in (0.13, 0.2)$ and $p \in (2, 25)$, the changes of Lyapunov exponent spectrum and bifurcation diagram are also consistent. It can be known that the dynamical characteristics of the fractional-order chaotic system is variegated so that the proposed chaotic system is suitable for cryptosystem.

Equilibrium stability. Qualitative analysis is an effective method to analyze chaos, and the calculation and analysis of the equilibrium point of chaotic system is an important part of the qualitative analysis of chaos mechanism. Continuous fractional-order system is used, so it is essential to find the equilibrium point of the corresponding integer order system to analyze its stability, and then deduce from the integer order to the fractional order. The solution of the differential equation gives the equilibrium point $O(x_{(e)}^0, y_{(e)}^0, z_{(e)}^0, w_{(e)}^0, u_{(e)}^0) = [0, 0, 0, \alpha, \beta]$, and α and β on behalf of arbitrary value. For the sake of analysis, if $\alpha = 1$ and $\beta = 1$, then the equilibrium point $O_1(x_{(e)}^0, y_{(e)}^0, z_{(e)}^0, w_{(e)}^0, u_{(e)}^0) = [0, 0, 0, 1, 1]$. Other system parameters are set in accordance with "Chaotic

Figure 3. Bifurcation diagrams and Lyapunov exponent spectrums, (**a**) BD, $q \in (0.5, 1)$, (**b**) BD, $n \in (0.13, 0.2)$, (**c**) BD, $p \in (2, 25)$, (**d**) LES, $q \in (0.5, 1)$, (**e**) LES, $n \in (0.13, 0.2)$, (**f**) LES, $p \in (2, 25)$.

Figure 4. Hardware connection diagram.

system" section, and the Jacobian matrix J and its corresponding characteristic equation and eigenvalue can be obtained as follows:

$$J = \begin{bmatrix} -0.7143 & 20.0000 & 0 & 0 & 0 \\ -0.0500 & 0.7250 & -0.1571 & 0 & 0 \\ -1.0500 & 15.2250 & -0.3000 & 0 & 0 \\ -3.0000 & 0 & 0 & 0 & 0 \\ 0 & -3.0000 & 0 & 0 & 0 \end{bmatrix} \tag{20}$$

$$\lambda^2(\lambda^3 + 0.2893\lambda^2 + 3\lambda - 1.4464) = 0 \tag{21}$$

$$\lambda_1 = 0, \lambda_2 = 0, \lambda_3 = -0.3703 + 1.7517i, \lambda_4 = -0.3703 - 1.7517i, \lambda_5 = 0.4512 \tag{22}$$
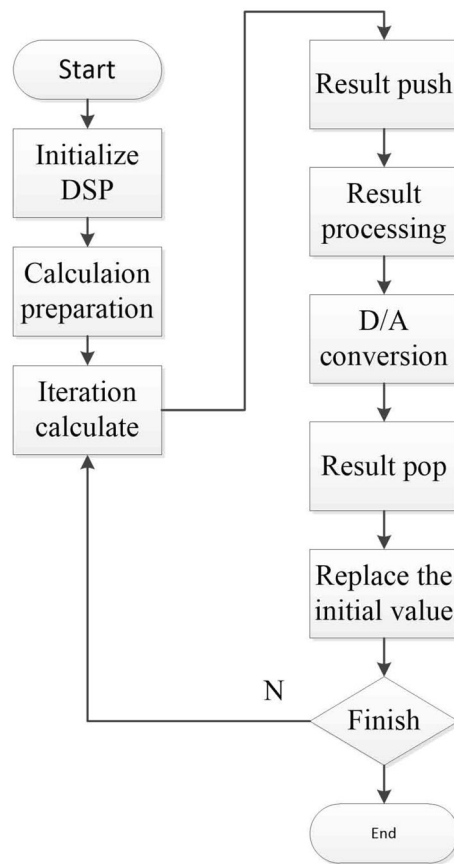
therefore, this equilibrium point is the saddle coke equilibrium point of index 1. Homoclinic and heteroclinic orbits can be formed between saddle points or saddle focal points, which is the key to chaos.

According to the fractional order stability theorem, the system is stable when the system order q satisfies Eq. (23), and it is unstable when the system order q satisfies Eq. (24). Because of Eq. (25), when $q \in (0.8764, 1)$, the system is not stable.

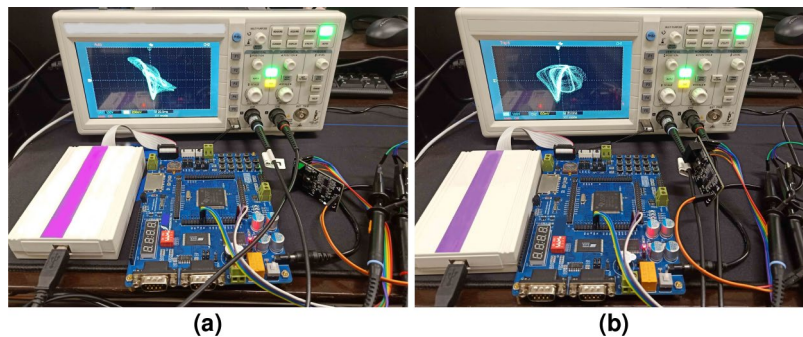$$0 \leq q \leq \min_{i=1,2,\dots,5} | arg(\lambda_i) | \tag{23}$$

$$\frac{2}{\pi} \min_{i=1,2,\dots,5} | arg(\lambda_i) | \leq q \leq 1 \tag{24}$$
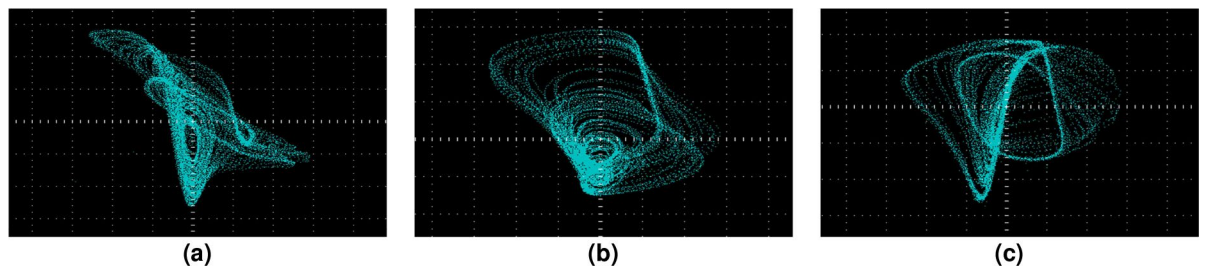
$$| arg(\lambda_3, 4) | = 1.3625 \tag{25}$$
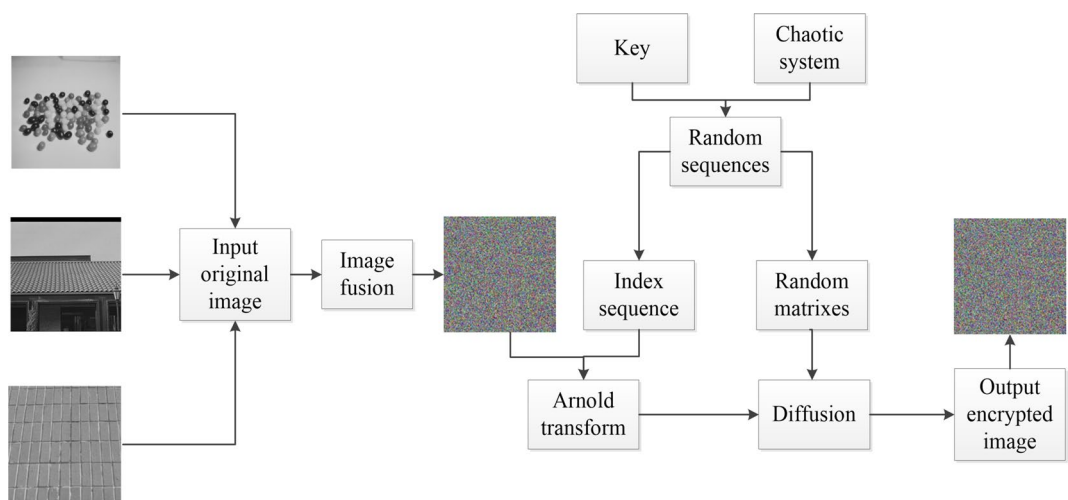
Figure 5. Program flow diagram.

Figure 6. DSP experimental platform construction diagram.

Figure 7. The phase diagrams captured by oscilloscope, (**a**) x–y plan, (**b**) x–w plan, (**c**) x–u plan.

System parameter	$c, e, g, n, p, s, m_1, m_2$	20, 150/7, 15, 0.15, 3, 0.05, 0.1, 0.1
System initial value	x, y, z, w, u	0.1, 0, 0, 0, 0
Order	q	0.97
Iteration step size	h	0.01

Table 1. Parameter configuration.

Figure 8. Encryption scheme.

Implementation of DSP technology. The hardware realization of chaos system can show the possibility of applying chaos from theory to practice. Therefore, DSP experimental platform is built. Through SPI connected to the D/A converter, the final output sequence displayed by the oscilloscope. Hardware connection diagram, program flow diagram and experimental platform construction diagram are shown in the Figs. 4, 5 and 6. Parameter configuration is shown in Table 1. The chaotic phase diagram collected in the oscilloscope is shown in Fig. 7. The output of the oscilloscope is visually consistent with the Fig. 2. This shows that the fractional-order system used can be successfully built on the DSP experimental platform.

The complete encryption scheme

The images combine encryption algorithm based on the principle of color image channels. This is the main discussion point of this section. The process of the proposed encryption scheme is shown in Fig. 8. Firstly, three pictures need to be pre-processed. And then, the pictures are merged and encrypted. Finally, the cipher image is acquired by the image is rotated 180 degrees. The detailed process is described in the following.

Image fusion. In the step of image fusion, the encrypted gray image can be processed into a color image. The processed image is already visually meaningless.

Step 1: Control parameters and initial values of fractional-order hyperchaotic system are immobilized. The iteration time can be ascertained according to the need.

Step 2: The chaotic sequences X, Y, Z, W, U can be got from the fractional-order hyperchaotic system based on the Eq (8). The five chaotic sequences are pseudo-random. Simultaneous quantitative operations are performed.

Step 3: Read in three pictures and deal them with bitwise exclusive-OR operation. The bitwise exclusive-OR method is:

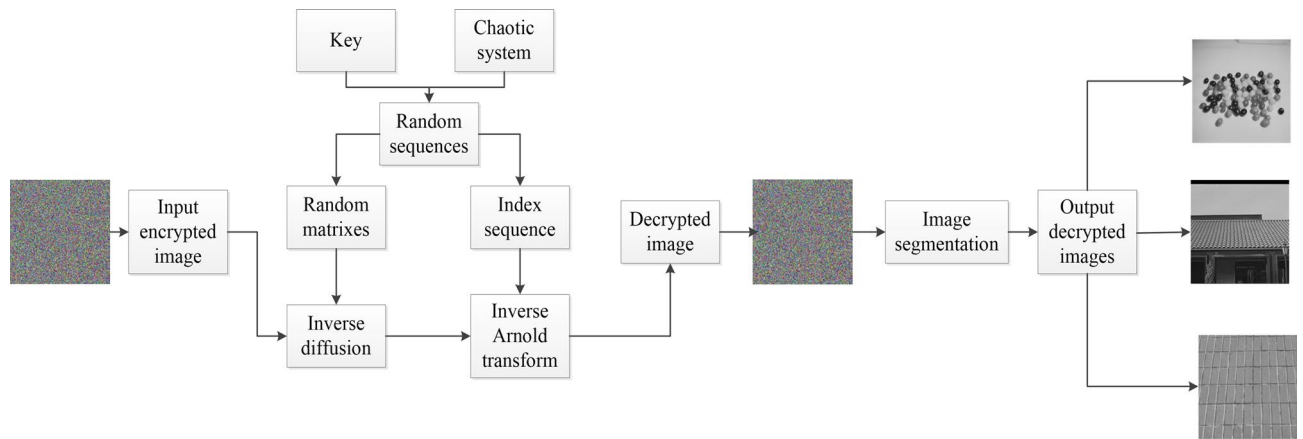$$\begin{cases} I1 = I1 \oplus I2 \oplus X \\ I2 = I2 \oplus I3 \oplus Y \\ I3 = I3 \oplus Z \end{cases} \tag{26}$$

Step 4: Merge three images into one colorful image according to the principles of R, G and B.

Step 5: Finally, the resulting output image I3 is used as the input image for the scrambling operation.

Scrambling algorithm. Arnold transform is a frequently-used method to scramble the location of the pixels. The process of Arnold transformation is depicted as the following.

Step 1: It is the same as step one and step two of the scrambling algorithm in "Image fusion" section.

Step 2: Two sequences a_1 and b_1 are acquired from quantized random sequences. From this, index sequence q is generated by addition and modulus through the use of a_1 and b_1.

Figure 9. Decryption scheme.

$$\begin{cases} a_1 = X(30000 + 1 : 30000 + M \times H) \\ b_1 = Y(30000 + 1 : 30000 + M \times H) \\ q = (b_1 + a_1. \times (1 : M \times H))\%(M \times H) + 1 \end{cases} \tag{27}$$

M and H are length and width of the original images and $(b_1+a_1.(1:MH))\%(MH))$ means that chaotic sequence a_1 is multiplied by the corresponding increasing sequence 1 to MH,then add it to b_1, and finally take the remainder for MH.

Step 3: Every pixel of each of the three images went through. After that, using index sequence can get a rough-and-tumble image by scrambling severally.

Step 4: Three vectors of three images pixels can be got and shaped into matrixes.

Diffusion algorithm. The operation that the pixels position of an image is unchanged and the pixels values are changed is called diffusion. Idiographic diffusion algorithm processes are as follows.

Step 1: It is the same as step one and step two of the scrambling algorithm in "Image fusion" section.

Step 2: The scrambled image is reused as the source image. The pixel which is located (1, 1) is disposed of.

$$\begin{cases} C1(1, 1) = A1(1, 1) \oplus X(1, 1) \oplus U(1, 1) \\ C2(1, 1) = A2(1, 1) \oplus X(1, 1) \oplus U(1, 1) \\ C3(1, 1) = A3(1, 1) \oplus X(1, 1) \oplus U(1, 1) \end{cases} \tag{28}$$

where $A1 \oplus X$ is the operation of bitwise exclusive-OR between $A1$ and X. $A1$ on behalf of the first scrambled image, $C1$ represents the image which has been diffused. In addition, $A2$, $A3$, $C2$, $C3$ are corresponding with the second image and third image severally.

Step 3: The first row of per image is diffused by

$$\begin{cases} C1(1, j) = A1(1, j) \oplus X(1, j) \oplus C1(1, j - 1) \\ C2(1, j) = A2(1, j) \oplus X(1, j) \oplus C2(1, j - 1) \\ C3(1, j) = A3(1, j) \oplus X(1, j) \oplus C3(1, j - 1) \end{cases} \tag{29}$$

where j is the number of columns from 2 to end.

Step 4: The first column of per image is diffused by

$$\begin{cases} C1(i, 1) = A1(i, 1) \oplus X(i, 1) \oplus C1(i - 1, 1) \\ C2(i, 1) = A2(i, 1) \oplus X(i, 1) \oplus C2(i - 1, 1) \\ C2(i, 1) = A3(i, 1) \oplus X(i, 1) \oplus C3(i - 1, 1) \end{cases} \tag{30}$$

where i is the number of rows from 2 to end.

Step 5: For the rest of the pixels, operate on them in a row by

$$\begin{cases} C1(i, j) = A1(i, j) \oplus X(i, j) \oplus C1(i - 1, j) \oplus C1(i, j - 1) \\ C2(i, j) = A2(i, j) \oplus X(i, j) \oplus C2(i - 1, j) \oplus C2(i, j - 1) \\ C2(i, j) = A3(i, j) \oplus X(i, j) \oplus C3(i - 1, j) \oplus C3(i, j - 1) \end{cases} \tag{31}$$

three images which are diffused can be obtained.

Step 6: The image which is diffused is rotated 180 degrees.

Decryption scheme

The algorithm for decryption is the reverse operation of the encryption algorithm, the corresponding flowchart is shown in Figure 9. The decryption result is that we can get three undamaged pictures. The detailed algorithm comprises inverse diffusion, inverse Arnold transform and picture segmentation. Some detailed steps are described as follows.

Step 1: As described in step one to two of scrambling algorithm "Image fusion", there are five quantized sequences.

Step 2: The encrypted image is separated into three gray images. Rotate three images 180 degrees, respectively.

Step 3: According to the following Eq. (32)

$$\begin{cases} D1(1,1) = C1(1,1) \oplus X(1,1) \oplus U(1,1) \\ D2(1,1) = C2(1,1) \oplus X(1,1) \oplus U(1,1) \\ D3(1,1) = C3(1,1) \oplus X(1,1) \oplus U(1,1) \end{cases} \tag{32}$$

where C and D represent cipher image and inverse diffused image.

Step 4: The first row of the three figures is treated with inverse diffusion.

$$\begin{cases} D1(1,j) = C1(1,j) \oplus X(1,j) \oplus C1(1,j-1) \\ D2(1,j) = C2(1,j) \oplus X(1,j) \oplus C2(1,j-1) \\ D3(1,j) = C3(1,j) \oplus X(1,j) \oplus C3(1,j-1) \end{cases} \tag{33}$$

Step 5: The first column of three pictures is handled by inverse diffusion.

$$\begin{cases} D1(i,1) = C1(i,1) \oplus X(i,1) \oplus C1(i-1,1) \\ D2(i,1) = C2(i,1) \oplus X(i,1) \oplus C2(i-1,1) \\ D2(i,1) = C2(i,1) \oplus X(i,1) \oplus C3(i-1,1) \end{cases} \tag{34}$$

Step 6: For the rest of the pixels, operate on them in a row by

$$\begin{cases} D1(i,j) = C1(i,j) \oplus X(i,j) \oplus C1(i-1,j) \oplus C1(i,j-1) \\ D2(i,j) = C2(i,j) \oplus X(i,j) \oplus C2(i-1,j) \oplus C2(i,j-1) \\ D2(i,j) = C3(i,j) \oplus X(i,j) \oplus C3(i-1,j) \oplus C3(i,j-1) \end{cases} \tag{35}$$

Step 7: Three sequences a_1, b_1 and q are acquired the same as "Image fusion" section. Then, the inverse Arnold transform is carried out by

$$\begin{cases} t1 = Q1(i); Q1(i) = Q1(q(i)); Q1(q(i)) = t1 \\ t2 = Q2(i); Q2(i) = Q2(q(i)); Q2(q(i)) = t2 \\ t3 = Q3(i); Q3(i) = Q3(q(i)); Q3(q(i)) = t3 \end{cases} \tag{36}$$

three vectors of three images pixels are obtained and shaped into matrixes which include Q_1, Q_2, Q_3.

Step 8: The inverse operation of step two in "Decryption scheme" section follows in

$$\begin{cases} Q3 = Q3 \oplus Z \\ Q2 = Q2 \oplus Q3 \oplus Y \\ Q1 = Q1 \oplus Q2 \oplus X \end{cases} \tag{37}$$

at this moment, the decrypted images including Q_1, Q_2 and Q_3 are acquired.
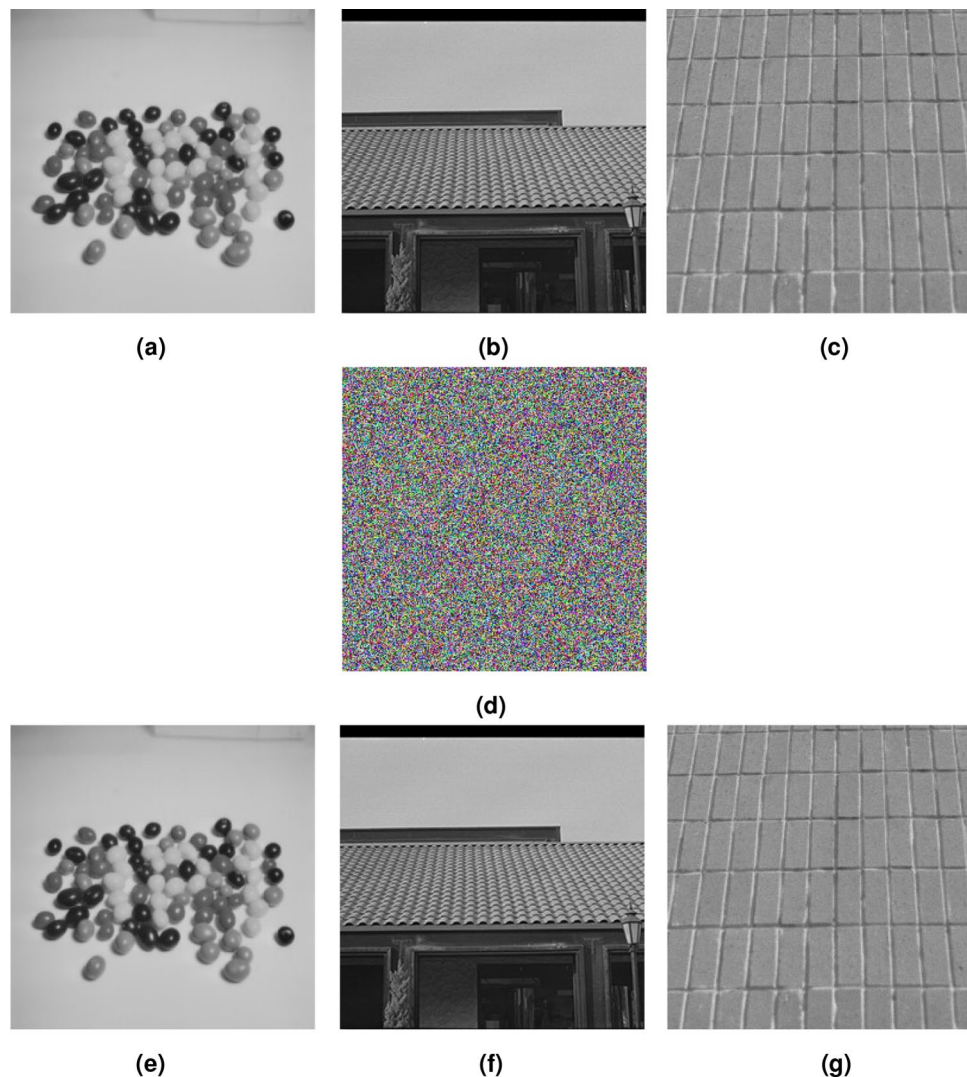
Performance analysis

Simulations results. To verify the effectiveness of the presented encryption algorithm, the designed image encryption scheme is tested. Deploying step size $h = 0.01$, $c = 20$, $e = 150/7$, $g = 15$, $n = 0.15$, $p = 3$, $s = 0.05$, $m_1 = m_2 = 0.1$, $q = 0.97$, starting value is $[x\ y\ z\ w\ u] = [0.1\ 0\ 0\ 0\ 0]$. Original image Candy, House and Texture in size 256–256 are encrypted and decrypted simultaneously. The simulation results of proposed image encryption and decryption algorithm are shown in Fig. 10. Where original images (OI) are Fig. 10a–c, cipher image (CI) is displayed in Fig. 10d, the corresponding decryption images (DI) are Fig. 10e–g. As we can see from Fig. 10, the cipher image is visually completely different from plaintext images. The cipher image is almost noisy and is in color. Therefore, the proposed algorithm can encrypt and decrypt images efficiently.

Key space. The key space of an encryption algorithm should be large enough to resist brute force attacks. This algorithm has fourteen control parameters. The system parameters c and e change 10^{-14}, g and p change 10^{-15}, n and n change 10^{-16}, m_1, m_2 and q change 10^{-17}, the system initial values change 10^{-17}. So, the key space of the proposed scheme is more than 2^{750}, it is much bigger than 2^{100}, which is regarded as the minimum value of key space. Data from other literature are given in Table 2 for reference[53–57]. So, the proposed can stand up to brute force attack.

Key sensitivity. The image cryptosystem has strong sensitivity if the two cipher images have conspicuous difference. On the contrary, the image cryptosystem is insensitive. A well cryptosystem should have high key sensitivity.

To analyze key sensitivity, the key sensitivity test is done. In the simulation, plain images are encrypted by the slightly altered keys and decrypted by the correct keys. The decrypted images are shown in Fig. 11. Because of the difference in parameter values, sensitivity scales are also different. Via testing one by one, the sensitivity of every parameter can be obtained. From Fig. 11 and the sensitivity of every parameter, the proposed algorithm has highly key sensitivity.

Histogram. Histogram is a statistic of gray level distribution in gray image. This index can reflect the relationship between the gray level and the frequency. Before encryption, the histogram of the original image is

Figure 10. Encrypted and decrypted results, (**a**) OI, Candy, (**b**) OI, House, (**c**) OI, Texture, (**d**) CI, (**e**) DI, Candy, (**f**) DI, House, (**g**) DI, Texture.

Our algorithm	Ref.[53]	Ref.[54]	Ref.[55]	Ref.[56]	Ref.[57]
2^{750}	2^{213}	2^{580}	2^{497}	2^{374}	2^{399}

Table 2. Key space of different algorithms.

variational. In contrast, the histogram of cipher image is uniform distribution. From Fig. 12, the difference of histogram between original images and cipher images is obvious. The cardinality test can be used to quantitatively analyze the ability of the encryption scheme to resist statistical attacks, and for the cardinality test results are shown in Table 3. The proposed encryption algorithms pass the cardinality test when the significance levels are 0.01, 0.05, and 0.1, respectively. This also shows that the cipher image obtained by the encryption scheme are approximately uniformly distributed[44,58].

Correlation of adjacent pixels. Usually, plain images have a strong correlation between adjacent pixels. A good encryption algorithm should generate cipher images with low correlation. In this way, the encryption scheme can hide the original image information. The correlation of adjacent pixels is defined by:
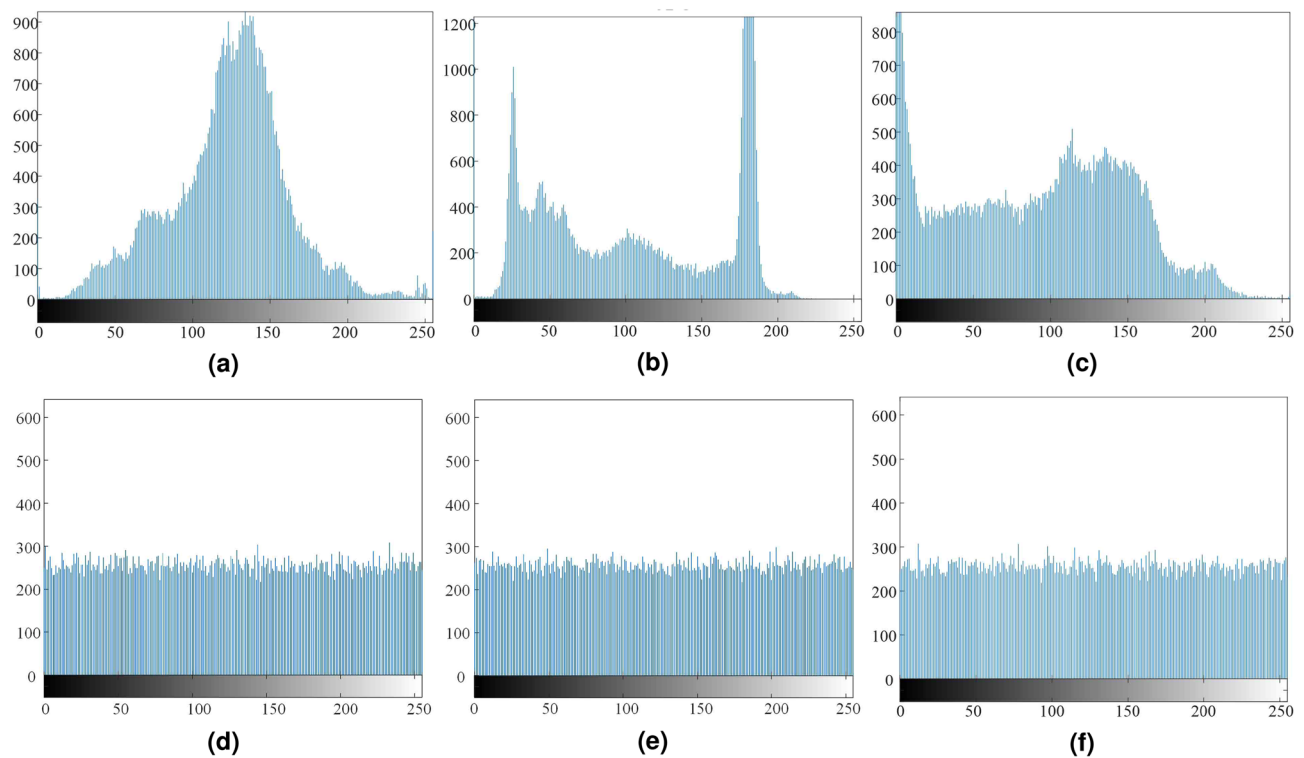
$$r_{x,y} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}} \tag{38}$$

Figure 11. Decrypted results about key sensitivity test, (**a**) Candy, $c = 20+1^{-14}$, (**b**) House, $c = 20+10^{-14}$, (**c**) Texture, $c = 20+10^{-14}$, (**d**) Candy, $g = 15+10^{-15}$, (**e**)House, $g = 15+10^{-15}$, (**f**) Texture, $g = 15+10^{-15}$, (**g**) Candy, $q = 0.97+10^{-16}$, (**h**) House, $q = 0.97+10^{-16}$, (**i**) Texture, $q = 0.97+10^{-16}$, (**j**) Candy, $m_1 = 0.1+10^{-17}$, (**k**) House, $m_1 = 0.1+10^{-17}$, (**l**) Texture, $m_1 = 0.1+10^{-17}$.

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \tag{39}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \tag{40}$$

Figure 12. Histogram test, (**a**) OI, Candy, (**b**) OI, House, (**c**) OI, Texture, (**d**) CI, Candy, (**e**) CI, House, (**f**) CI, Texture.

The model name	χ^2-value (plaintext)	χ^2-value (Cipher)	Critical value		
			$\chi^2_{0.1}$ (255)	$\chi^2_{0.05}$ (255)	$\chi^2_{0.01}$ (255)
Candy (256×256)	49346.0625	243.5469	Pass	Pass	Pass
House (256×256)	72970.4609	228.0781	Pass	Pass	Pass
Texture (256×256)	83678.7734	249.1224	Pass	Pass	Pass

Table 3. The table of χ^2-value for different objects.

where E(x) and D(x) are the expectation and variance of the variable x, y, r_x, y is the correlation coefficient between adjacent pixels x and y.
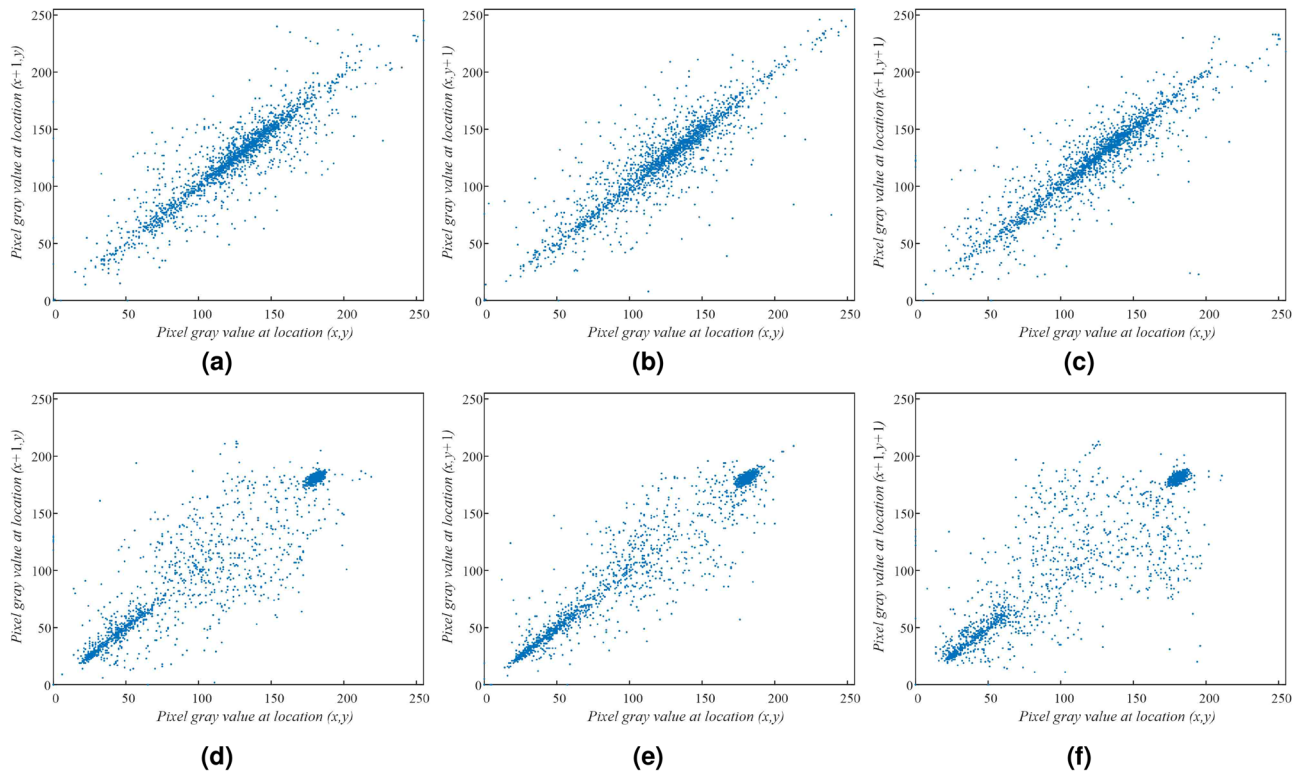
For testing the correlation of adjacent pixels, we select 1000 pairs adjacent pixels randomly from original images and their corresponding cipher images to analyze. The correlation and correlation coefficients calculated by using the Eq. (38) are shown in Figs. 13 and 14 and Table 4. Results from other literature are also listed in Table 4[59-61]. From Figs. 13 and 14, the adjacent values of plain image pixels all lie near a straight line with slope 1, there is a high correlation between two adjacent pixels. The pixel values of cipher images are carpeted with the whole region, that is to say a low correlation between adjacent pixels. The results in Table 4 also indicate that the correlation coefficients between the adjacent pixels of the original images in horizontal, vertical and diagonal (H, V and D) directions are large. The correlation coefficients of the encrypted image in corresponding orientations are decreased significantly. The encryption algorithm proposed can effectively against statistical attacks.

Information entropy. Information entropy can be used to describe the uncertainty of picture information and to measure its randomness. For an image, the more homogeneous the gray values distribute, the bigger the information entropy is. The picture information has a strong randomness when the information entropy is close to 8. Information entropy is computed by:

$$H(m) = -\sum_{i=1}^{255} P(x_i) log_2 P(x_i) \tag{41}$$

where $P(x_i)$ is the probability of gray value x_i.

Information entropies of original images and cipher images are listed in Table 5. The information entropies of cipher images are more than 7.997 and close to 8. From Table 5, the information entropy of our scheme and

Figure 13. Correlation of adjacent pixels, (**a**–**c**) OI, Candy, (**d**–**f**) OI, House.

others in Refs.[33,41,60,62] are given, a conclusion that the proposed algorithm can generate cipher images with strong randomness can be drawn.

Differential attack. The performance of anti-differential attack depends on the sensitivity to plaintext and is usually measured by the number of pixels change rate (NPCR) and the unified average changing intensity (UACI). NPCR and UACI are calculated by:

$$NPCR(P_1, P_2) = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} | Sign(P_1(i,j) - P_2(i,j)) | \times 100\% \tag{42}$$

$$UACI(P_1, P_2) = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{| P_1(i,j) - P_2(i,j) |}{255 - 0} \times 100\% \tag{43}$$
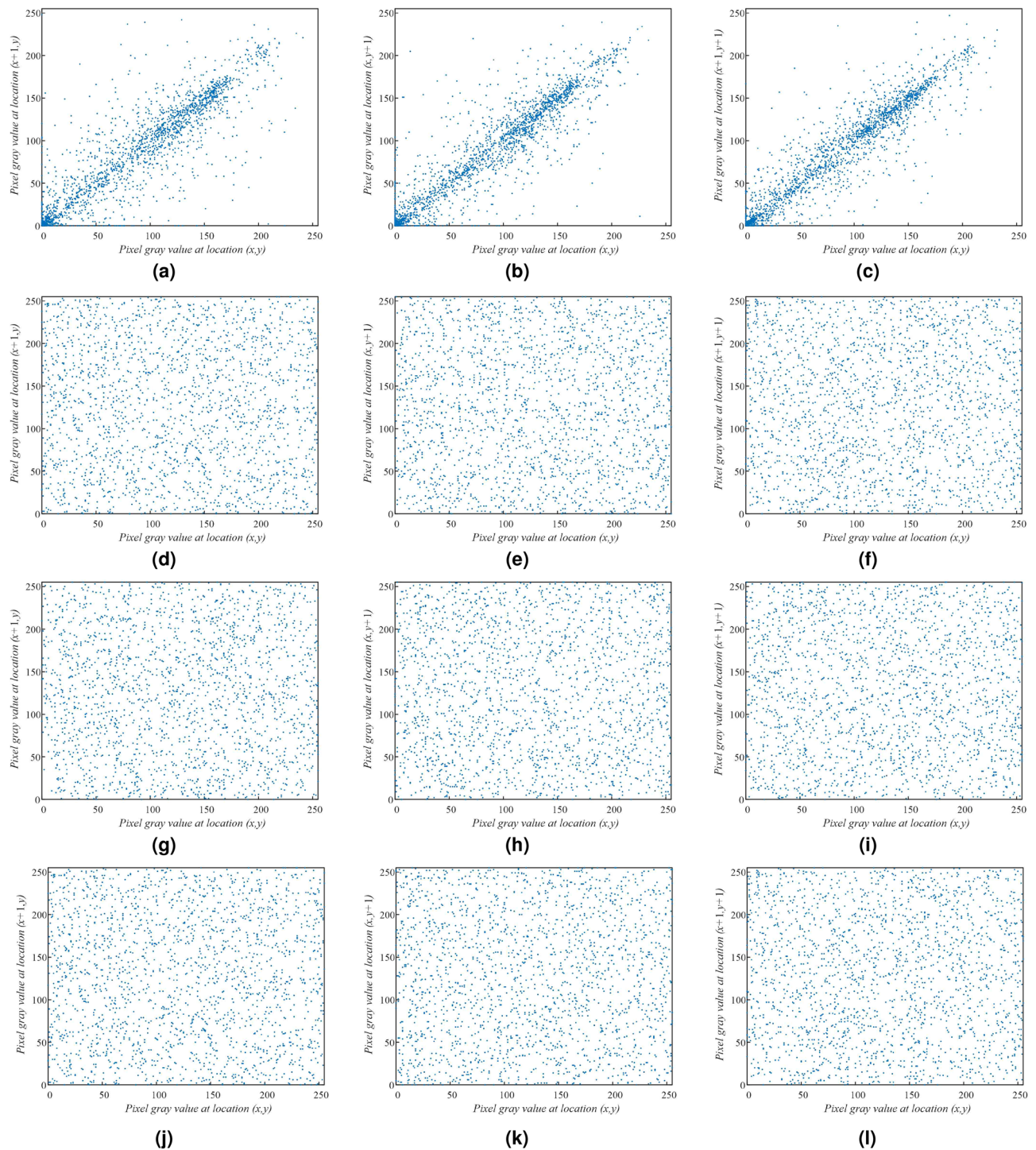
where P_1 on behalf of cipher image and P_2 is the cipher image which plain image pixel value has changed.

Due to the arbitrariness of position, the theoretical values of NPCR and UACI are 99.6094% and 33.4635% respectively. The NPCR and UACI values in the simulation test should be close to expectation. Via simulation test, the results of the proposed algorithm are presented as Table 6. From the Table 6, the results are closed to theoretical expectations and it will get an almost completely different image if the gray value of the image is changed slightly. Moreover, we list the average values of NPCR and UACI in other literature which is shown in Table 7[10,17,27,63]. Results indicate that our algorithm can resist differential attack effectively.

Robustness. When transmitted over a channel, the cipher image will be influenced by a variety of interference and attacks. A good encryption algorithm should make images have robustness for external interference. Noise attack and cropping attack testing experiments were carried out to test the robustness of the encryption algorithm.

Noise attack. In the process of data transmission, cipher image will be contaminated by noise. For testing the resistance performance of encryption algorithm to noise, Salt and Pepper noise (SPN), Gaussian noise (GN) are added to the cipher image and the decrypted results are shown in Fig. 15. It is observed that the decrypted images still have noise, but the main information can be recovered. So, a certain level of noise attack can be tolerated by the encryption algorithm.

Cropping attack. Cipher image may be destroyed while it is in the process of transmission and results in data loss. The cropping attack test is carried out to illustrate the performance of the proposed encryption algorithm

Figure 14. Correlation of adjacent pixels, (**a**–**c**) OI, Texture, (**d**–**f**) CI, Candy, (**g**–**i**) CI, House, (**j**–**l**) CI, Texture.

to resist cropping attack. The simulation results are shown in Fig. 16, while encrypted image lose 6.25% data, decrypted images which include Candy, House and Texture are Figure 16a. While encrypted image 12.5% data are cropped, decrypted images are shown in Fig. 16b. While encrypted image 25% data are removed, the results of decryption are shown in Fig. 16c. We can see that though the encrypted image loses 6.25%, 12.5% or 25% data, the main information in the decrypted images can still be identified. Simulation results demonstrate that the proposed algorithm has a certain ability to resist cropping attack.

Time analysis. Time complexity is an important aspect to measure the efficiency of the encryption algorithm,for three images 'Candy', 'House' and 'Texture', the running time for encryption and decryption is shown in Table 8 and compared with other encryption schemes as shown in Table 9. From the Table 9, it can be seen that the encryption scheme has a better performance in terms of running rate[47,64–67].

Encryption algorithm	Image	Direction	Plain image	Cipher image
Our scheme	Candy	H	0.9718	0.0005
		V	0.9743	0.0009
		D	0.9506	0.0018
	House	H	0.9254	0.0009
		V	0.9083	0.0036
		D	0.9314	0.0042
	Texture	H	0.9706	0.0045
		V	0.9503	0.0028
		D	0.9465	0.0010
Ref.[60]	Image	H	0.9724	0.0118
		V	0.9455	−0.0173
		D	0.9214	0.0080
Ref.[59]	Image	H	0.9724	−0.0048
		V	0.9455	−0.0112
		D	0.9214	−0.0125
Ref.[61]	Image	H	0.9724	0.0070
		V	0.9455	−0.0102
		D	0.9214	0.0030

Table 4. Correlation coefficient pixels.

Encryption algorithm	Image	Image size	Original image	Cipher image
Our scheme	Candy	256256	7.3456	7.9973
	House	256256	7.1235	7.9975
	Texture	256256	7.0384	7.9976
Ref.[60]	Airplane	256256	–	7.9971
Ref.[62]	Baboon	256256	7.1273	7.9974
Ref.[62]	Average	256256	7.4127	7.9973
Ref.[33]	Average	256256	7.3446	7.9970
Ref.[41]	Average	256256	7.6560	7.9969

Table 5. Information entropy of original images and cipher images.

Image	Candy	House	Texture	Average
NPCR (%)	99.5986	99.6232	99.5853	99.6024
UACI (%)	33.5052	33.4633	33.5240	33.4975

Table 6. The results of differential attack test.

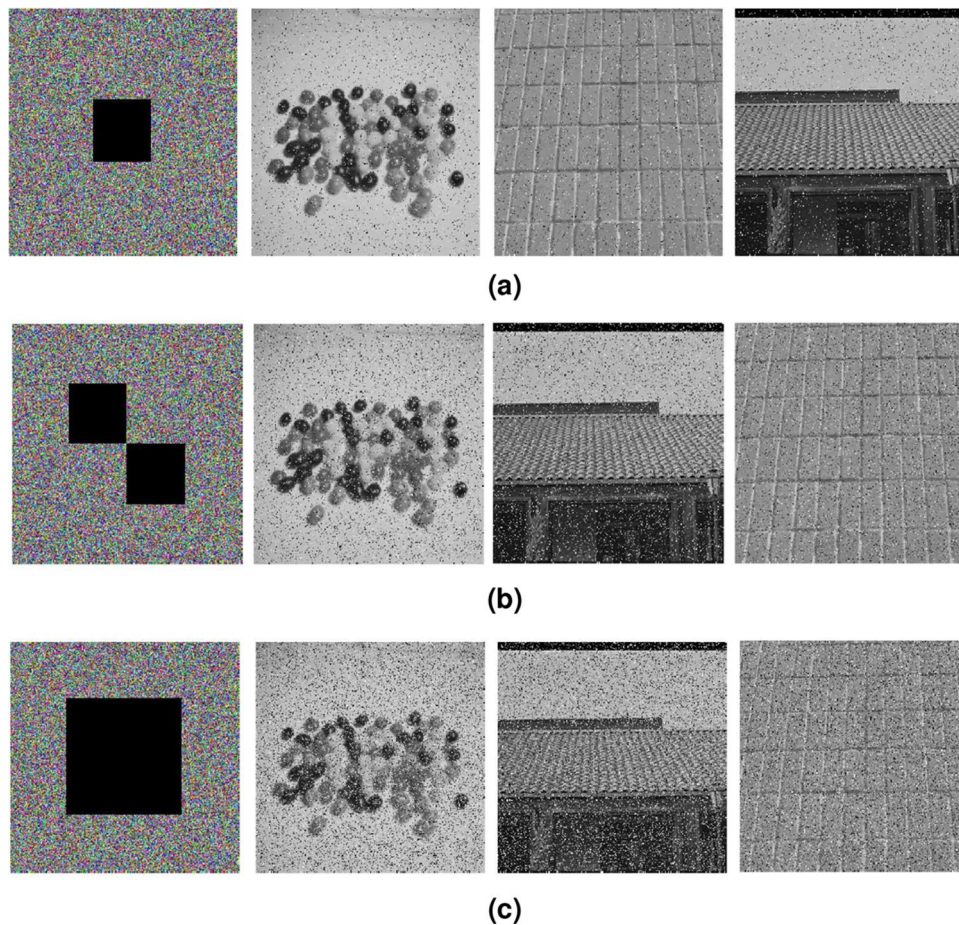|	Our algorithm	Ref.[10]	Ref.[17]	Ref.[63]	Ref.[27]
NPCR (%) (average)	99.6024	99.610	99.6117	99.6082	99.5582
UACI (%) (average)	33.4975	33.462	33.6694	33.3391	33.3844

Table 7. NPCR and UACI values of different algorithms.

Figure 15. Decrypted images with various noise, (**a**) SPN, 0.05, (**b**) SPN, 0.07, (**c**) GN, 0.0001.

Conclusion

In this paper, a multiple image encryption scheme based on fractional-order hyperchaotic system is presented. The phase diagram, bifurcation diagram, Lyapunov exponent spectrum and equilibrium point are analyzed in detail. The analysis results show that the fractional-order hyperchaotic system has complex dynamical characteristics and it is suitable for image security encryption. The fractional-order hyperchaotic system is implemented on the DSP platform and the results are the same as simulation results. It provides the possibility of realizing secure communication with fractional-order hyperchaotic systems. By using the proposed algorithm, multiple images are encrypted twice, it not only improves the encryption efficiency, but also improves the security of image transmission. The key space, key sensitivity, histogram, correlation, information entropy and robustness are analyzed, the results indicate that it can withstand brute attack, statistical attack, a certain degree of noise pollution and cropping attack effectively. It shows that the encryption algorithm has a great encryption effect. Hence, the proposed image encryption scheme has research significance and application value.

Figure 16. Cropping attack test, (**a**) 6.25% data loss, encrypted image and decrypted images, (**b**) 12.5% data loss, encrypted image and decrypted images, (**c**) 25% data loss, encrypted image and decrypted images.

Round	1 (s)	2 (s)	3 (s)	4 (s)	5 (s)	6 (s)	Average (s)	Speed (Mb/s)
Encryption	0.0382	0.0404	0.0459	0.0441	0.0467	0.0426	0.0430	4.4967
Decryption	0.0326	0.0272	0.0360	0.0366	0.0602	0.0464	0.0399	4.8461

Table 8. Running time of the proposed algorithm.

Algorithm	Ours	Ref.[47]	Ref.[64]	Ref.[65]
Encryption	0.0430	0.4400	1.1737	0.3356
Decryption	0.0399	–	–	1.5216

Table 9. Running time of the different algorithm.

Data availability
The test images used in this paper are from the SIPI image database and are used for scientific research only, not for other purposes, and without copyright disputes.

References
1. Hua, Z., Zhou, Y. & Huang, H. Cosine-transform-based chaotic system for image encryption. *Information Sciences* **480**, 403–419. https://doi.org/10.1016/j.ins.2018.12.048 (2019).

2. Chai, X., Fu, X., Gan, Z., Lu, Y. & Chen, Y. A color image cryptosystem based on dynamic dna encryption and chaos. *Signal Processing* **155**, 44–62. https://doi.org/10.1016/j.sigpro.2018.09.029 (2019).

3. Chai, X. *et al.* Combining improved genetic algorithm and matrix semi-tensor product (stp) in color image encryption. *Signal Processing* **183**, 108041. https://doi.org/10.1016/j.sigpro.2021.108041 (2021).

4. Chai, X. *et al.* Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. *Signal Processing* **176**, 107684. https://doi.org/10.1016/j.sigpro.2020.107684 (2020).

5. Fridrich, J. Image encryption based on chaotic maps. In *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation*, https://doi.org/10.1109/ICSMC.1997.638097.

6. Brindha, M. & Gounden, N. A. A chaos based image encryption and lossless compression algorithm using hash table and chinese remainder theorem. *Applied Soft Computing* **40**, 379–390. https://doi.org/10.1016/j.asoc.2015.09.055 (2016).

7. Wang, X. Y. *et al.* A novel color image encryption scheme using dna permutation based on the lorenz system. *Multimedia Tools and Applications* **77**, 6243–6265. https://doi.org/10.1007/s11042-017-4534-z (2018).

8. Li, X., Mou, J., Xiong, L., Wang, Z. & Xu, J. Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption. *Optics & Laser Technology* **140**, 107074. https://doi.org/10.1016/j.optlastec.2021.107074 (2021).

9. Hu, T., Liu, Y., Gong, L. H., Guo, S. F. & Yuan, H. M. Chaotic image cryptosystem using dna deletion and dna insertion. *Signal Processing* **134**, 234–243. https://doi.org/10.1016/j.sigpro.2016.12.008 (2017).

10. Bashir, Z., Rashid, T. & Zafar, S. Hyperchaotic dynamical system based image encryption scheme with time-varying delays. *Pacific Science Review A Natural Science & Engineering* **18**, 254–260. https://doi.org/10.1016/j.psra.2016.11.003 (2016).

11. Masood, F., Ahmad, J., Shah, S. A., Sajjad, S. & Hussain, I. A novel hybrid secure image encryption based on julia set of fractals and 3d lorenz chaotic map. *Entropy* **22**, 274. https://doi.org/10.3390/e22030274 (2020).

12. Niyat, A. Y. & Moattar, M. H. Color image encryption based on hybrid chaotic system and dna sequences. *Multimedia Tools and Applications* **79**, 1497–1518. https://doi.org/10.1007/s11042-019-08247-z (2020).

13. Wu, X., Wang, K., Wang, X., Kan, H. & Kurths, J. Color image dna encryption using nca map-based cml and one-time keys. *Signal Processing* **148**, 272–287. https://doi.org/10.1016/j.sigpro.2018.02.028 (2018).

14. Niu, Y., Sun, X., Zhang, C. & Liu, H. Anticontrol of a fractional-order chaotic system and its application in color image encryption. *Mathematical Problems in Engineering* **1–12**, 2020. https://doi.org/10.1155/2020/6795964 (2020).

15. Zhang, L. Y. *et al.* On the security of a class of diffusion mechanisms for image encryption. *IEEE Transactions on Cybernetics* **PP**, 1–13, https://doi.org/10.1109/TCYB.2017.2682561 (2015).

16. Weng, S., Shi, Y. Q., Hong, W. & Yao, Y. Dynamic improved pixel value ordering reversible data hiding. *Information Sciences* **489**, 136–154. https://doi.org/10.1016/j.ins.2019.03.032 (2019).

17. Abbasi, A. A., Mazinani, M. & Hosseini, R. Chaotic evolutionary-based image encryption using rna codons and amino acid truth table. *Optics & Laser Technology* **132**, 106465. https://doi.org/10.1016/j.optlastec.2020.106465 (2020).

18. Bao, B. *et al.* Two-memristor-based chua's hyperchaotic circuit with plane equilibrium and its extreme multistability. *Nonlinear Dynamics* **89**, 1157–1171. https://doi.org/10.1007/s11071-017-3507-0 (2017).

19. Zhang, W., Yu, H., Zhao, Y. L. & Zhu, Z. L. Image encryption based on three-dimensional bit matrix permutation. *Signal Processing* **118**, 36–50. https://doi.org/10.1016/j.sigpro.2015.06.008 (2016).

20. Annaby, M. H., Rushdi, M. A. & Nehary, E. A. Image encryption via discrete fractional fourier-type transforms generated by random matrices. *Signal Processing Image Communication* **49**, 25–46. https://doi.org/10.1016/j.image.2016.09.006 (2016).

21. Lia, C., Lina, D., LuB, J. & Feng, H. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. *IEEE Multimedia* **25**, 46–56. https://doi.org/10.1109/MMUL.2018.2873472 (2019).

22. Zhang, X., Zhao, Z. & Wang, J. Chaotic image encryption based on circular substitution box and key stream buffer. *SIGNAL PROCESSING-IMAGE COMMUNICATION* **29**, 902–913. https://doi.org/10.1016/j.image.2014.06.012 (2014).

23. Ba Nsal, R., Gupta, S. & Sharma, G. An innovative image encryption scheme based on chaotic map and vigenre scheme. *Multimedia Tools & Applications* **76**, 1–34. https://doi.org/10.1007/s11042-016-3926-9 (2016).

24. Hu, T., Ye, L., Gong, L. H. & Ouyang, C. J. An image encryption scheme combining chaos with cycle operation for dna sequences. *Nonlinear Dynamics* **87**, 1–16. https://doi.org/10.1007/s11071-016-3024-6 (2016).

25. Manjit, K. & Vijay, K. Adaptive differential evolution based lorenz chaotic system for image encryption. *ARABIAN JOURNAL FOR SCIENCE AND ENGINEERING* **1–18**, https://doi.org/10.1007/s13369-018-3355-3 (2018).

26. Sheela, *et al.* Image encryption based on modified henon map using hybrid chaotic shift transform. *Multimedia tools and applications* **77**, 25223–25251. https://doi.org/10.1007/s11042-018-5782-2 (2018).

27. Zhang, Y. Q. & Wang, X. Y. A new image encryption algorithm based on non-adjacent coupled map lattices. *Applied Soft Computing* **26**, 10–20. https://doi.org/10.1016/j.asoc.2014.09.039 (2015).

28. Chai, X. *et al.* An efficient approach for encrypting double color images into a visually meaningful cipher image using 2d compressive sensing. *Information Sciences* **556**, 305–340. https://doi.org/10.1016/j.ins.2020.10.007 (2021).

29. He, S., Sun, K., Mei, X., Yan, B. & Xu, S. Numerical analysis of a fractional-order chaotic system based on conformable fractional-order derivative. *European Physical Journal Plus* **132**, 36. https://doi.org/10.1140/epjp/i2017-11306-3 (2017).

30. Ma, C., Mou, J., Li, P. & Liu, T. Dynamic analysis of a new two-dimensional map in three forms: integer-order, fractional-order and improper fractional-order. *The European Physical Journal Special Topics* **1–13**, https://doi.org/10.1140/epjs/s11734-021-00133-w (2021).

31. He, S., Sun, K. & Wang, H. Dynamics and synchronization of conformable fractional-order hyperchaotic systems using the homotopy analysis method. *Communications in Nonlinear Science and Numerical Simulation* **73**, 146–164. https://doi.org/10.1016/j.cnsns.2019.02.007 (2019).

32. Liu, T., Yan, H., Banerjee, S. & Mou, J. A fractional-order chaotic system with hidden attractor and self-excited attractor and its dsp implementation. *Chaos, Solitons & Fractals* **145**, 110791. https://doi.org/10.1016/j.chaos.2021.110791 (2021).

33. Patro, K. & Acharya, B. A novel multi-dimensional multiple image encryption technique. *Multimedia Tools and Applications* **79**, https://doi.org/10.1007/s11042-019-08470-8 (2020).

34. Enayatifar, R., Guimaraes, F. G. & Siarry, P. Index-based permutation-diffusion in multiple-image encryption using dna sequence. *Optics and Lasers in Engineering* **115**, 131–140. https://doi.org/10.1016/j.optlaseng.2018.11.017 (2019).

35. Zhang, X. & Wang, X. Multiple-image encryption algorithm based on dna encoding and chaotic system. *Multimedia Tools and Applications* **78**, 7841–7869. https://doi.org/10.1007/s11042-018-6496-1 (2019).

36. Karawia, A. A. Encryption algorithm of multiple-image using mixed image elements and two dimensional chaotic economic map. *Entropy* **20**, 801. https://doi.org/10.3390/e20100801 (2018).

37. Zhang, X. & Wang, X. Multiple-image encryption algorithm based on mixed image element and permutation. *Computers & Electrical Engineering* **62**, 6–16. https://doi.org/10.1016/j.compeleceng.2016.12.025 (2017).

38. Pan, S. M., Wen, R. H., Zhou, Z. H. & Zhou, N. R. Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional mellin transform. *Multimedia Tools & Applications* **76**, 2933–2953. https://doi.org/10.1007/s11042-015-3209-x (2017).

39. Zhou, N., Jiang, H., Gong, L. & Xie, X. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. *Optics & Lasers in Engineering* **110**, 72–79. https://doi.org/10.1016/j.optlaseng.2018.05.014 (2018).

40. Vaish, A. & Kumar, M. Color image encryption using msvd, dwt and arnold transform in fractional fourier domain. *Optik - International Journal for Light and Electron Optics* **145**, https://doi.org/10.1016/j.ijleo.2017.07.041 (2017).

41. Hanif, M., Naqvi, R. A., Abbas, S., Khan, M. A. & Iqbal, N. A novel and efficient 3d multiple images encryption scheme based on chaotic systems and swapping operations. *IEEE Access* **PP**, 1–1, https://doi.org/10.1109/ACCESS.2020.3004536 (2020).

42. Sher, K. J. & Jawad, A. Chaos based efficient selective image encryption. *Multidimensional Systems and Signal Processing* **30**, 943–961. https://doi.org/10.1007/s11045-018-0589-x (2019).

43. Ma, X. *et al.* A novel simple chaotic circuit based on memristor-memcapacitor. *Nonlinear Dynamics* **100**, 2859–2876. https://doi.org/10.1007/s11071-020-05601-x (2020).

44. Huang, W., Jiang, D., An, Y., Liu, L. & Wang, X. A novel double-image encryption algorithm based on rossler hyperchaotic system and compressive sensing. *IEEE Access* **PP**, 41704–41716, https://doi.org/10.1109/ACCESS.2021.3065453 (2021).

45. Mzt, A. & Xw, B. A new fractional one dimensional chaotic map and its application in high-speed image encryption. *Information Sciences* **550**, 13–26. https://doi.org/10.1016/j.ins.2020.10.048 (2020).

46. Xdc, A., Ying, W. A., Jw, A. & Qhw, B. Asymmetric color cryptosystem based on compressed sensing and equal modulus decomposition in discrete fractional random transform domain. *Optics and Lasers in Engineering* **121**, 143–149. https://doi.org/10.1016/j.optlaseng.2019.04.004 (2019).

47. Chai, X., Zheng, X., Gan, Z. & Chen, Y. Exploiting plaintext-related mechanism for secure color image encryption. *Neural Computing and Applications* **32**, 8065–8088. https://doi.org/10.1007/s00521-019-04312-8 (2019).

48. Iqbal, N., Abbas, S., Khan, A., Alyas, T. & Ahmad, A. An rgb image encryption scheme using chaotic systems, 15-puzzle problem and dna computing. *IEEE Access* **PP**, 1–1, https://doi.org/10.1109/ACCESS.2019.2956389 (2019).

49. Zhu, C. & Sun, K. Cryptanalyzing and improving a novel color image encryption algorithm using rt-enhanced chaotic tent maps. *IEEE Access* **1–1**, https://doi.org/10.1109/ACCESS.2018.2817600 (2018).

50. Wu, X., Wang, K., Wang, X. & Kan, H. Lossless chaotic color image cryptosystem based on dna encryption and entropy. *Nonlinear Dynamics* **90**, 855–875. https://doi.org/10.1007/s11071-017-3698-4 (2017).

51. Yang, F., Mou, J., Ma, C. & Cao, Y. Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. *Optics and Lasers in Engineering* **129**, https://doi.org/10.1016/j.optlaseng.2020.106031 (2020).

52. Liu, T., Banerjee, S., Yan, H. & Mou, J. Dynamical analysis of the improper fractional-order 2d-sclmm and its dsp implementation. *The European Physical Journal Plus* **136**, 506. https://doi.org/10.1140/epjp/s13360-021-01503-y (2021).

53. Mohamed, ElKamchouchi & Moussa. A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial dna sequences. *Entropy* **22**, 158, https://doi.org/10.3390/e22020158 (2020).

54. Ouyang, X., Luo, Y., Liu, J., Cao, L. & Liu, Y. A color image encryption method based on memristive hyperchaotic system and dna encryption. *International Journal of Modern Physics B* **34**, 2050014. https://doi.org/10.1142/S0217979220500149 (2020).

55. Xingyuan *et al.* A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and dna level - sciencedirect. *Optics and Lasers in Engineering* **125**, 105851–105851, https://doi.org/10.1016/j.optlaseng.2019.105851.

56. Chen, L. P., Yin, H., Yuan, L. G., Lopes, A. M. & Wu, R. A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and dna sequence operations. *Frontiers of Information Technology & Electronic Engineering* **21**, 866–879. https://doi.org/10.1631/FITEE.1900709 (2020).

57. Zhou, M. & Wang, C. A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. *Signal Processing* **171**, 107484–107507. https://doi.org/10.1016/j.sigpro.2020.107484 (2020).

58. Liu, L., Jiang, D., Wang, X., Zhang, L. & Rong, X. A dynamic triple-image encryption scheme based on chaos, s-box and image compressing. *IEEE Access* **8**, 210382–210399. https://doi.org/10.1109/ACCESS.2020.3039891 (2020).

59. Belazi, A., El-Latif, A. A. A. & Belghith, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing* **128**, 155–170. https://doi.org/10.1016/j.optlaseng.2019.105851 (2016).

60. Farah, M., Farah, A. & Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynamics* **99**, 1–24. https://doi.org/10.1007/s11071-019-05413-8 (2020).

61. Chai, X., Zhang, J., Gan, Z. & Zhang, Y. Medical image encryption algorithm based on latin square and memristive chaotic system. *Multimedia Tools and Applications*https://doi.org/10.1007/s11042-019-08168-x *(2019).*

62. Wang, X., Liu, L. & Zhang, Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Optics and Lasers in Engineering* **66**, 10–18. https://doi.org/10.1016/j.optlaseng.2014.08.005 (2015).

63. Cao, C., Sun, K. & Liu, W. A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map. *Signal Processing* **143**, 122–133. https://doi.org/10.1016/j.sigpro.2017.08.020 (2017).

64. Chai, X., Zhang, J., Gan, Z. & Zhang, Y. Medical image encryption algorithm based on latin square and memristive chaotic system. *Multimedia Tools and Applications* **78**, 1–35. https://doi.org/10.1007/s11042-019-08168-x (2019).

65. Chai, X., Wu, H., Gan, Z., Zhang, Y. & Nixon, K. W. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic lsb embedding. *Optics and Lasers in Engineering* **124**, 105837–105855. https://doi.org/10.1016/j.optlaseng.2019.105837 (2020).

66. Liu, L., Jiang, D., Wang, X., Rong, X. & Zhang, R. 2d logistic-adjusted-chebyshev map for visual color image encryption. *Journal of Information Security and Applications* **60**, 102854. https://doi.org/10.1016/j.jisa.2021.102854 (2021).

67. Jiang, D., Liu, L., Wang, X. & Rong, X. Image encryption algorithm for crowd data based on a new hyperchaotic system and bernstein polynomial. *IET Image Processing* **1–20**, https://doi.org/10.1049/ipr2.12237 (2021).

Acknowledgements

Author contributions

X.G. designed and carried out experiments, data analyzed and manuscript wrote. J.Y., B.S., H.Y. and J.M. made the theoretical guidance for this paper.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to J.Y., S.B. or J.M.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.