A New Image Encryption Scheme based on Fractional-order Hyperchaotic System and Multiple Image Fusion

Xinyu Gao
Dalian polytechnic University
Jiawu Yu (yujiawu_dlpu@sina.com)
Dalian polytechnic University
Huizhen Yan
Dalian polytechnic University
Jun Mou
Dalian polytechnic University

Research Article

Keywords: Multi-image encryption, Fractional-order hyperchaotic system, Cryptoanalysis

Posted Date: May 24th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-494660/v1

Version of Record: A version of this preprint was published at Scientific Reports on August 3rd, 2021. See the published version at https://doi.org/10.1038/s41598-021-94748-7.

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

Xinyu Gao[a], Jiawu Yu*[a], Huizhen Yan[a] and Jun Mou[a]

[a]*School of Information Science and Engineering, Dalian polytechnic University, Dalian 116034, China , Corresponding author: yujiawu_ dlpu@sina.com , these authors contributed equally to this work*

Abstract

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.

Keywords: Multi-image encryption; Fractional-order hyperchaotic system; Cryptoanalysis

1 Introduction

In the era of big data, picture information is widely spread on the network, and the security of picture information is also widely concerned[22]. Conventional encryption schemes such as AES, DES encrypt textual data and do not apply to the encryption of images [10]. 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 [16, 8, 39]. 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 [22, 20, 6, 27, 31, 42, 30, 46, 40]. Compared with ordinary chaotic systems, hyperchaotic systems have more complex dynamics and greater sensitivity and are more suitable for image encryption [2, 5, 47, 3, 25, 50]. The fractional-order chaotic system is also more secure because the key space is increased by adding system variables [10, 4, 21, 26, 35, 51]. 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) [18]. 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 [19].

Another noteworthy point is that single-image encryption is fast but inefficient [25]. 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 [34, 14, 49, 24, 48]. 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 [33]. On this basis, Zhou et al. proposed a dual image encryption algorithm based on co-sparse representation and random pixel exchange [53]. Zhang et al. proposed a multi-image encryption scheme to encrypt the arbitrary number of images [48] and by using a DNA encoding encryption algorithm to accomplish encrypt multiple images simultaneously [49]. There also some scholars proposed the encryption schemes that can encrypt arbitrary size multiple images or a batch of images [37, 17, 36, 1]. 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 [29, 37]. However, some 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 [43, 12, 23, 54, 41, 45]. The application of fractional-order hyperchaotic system makes the pseudo-random sequence more complex and thus allows for a more secure encryption algorithm. The fusion of multiple images allows image encryption efficiency to be improved.

The remaining part of the paper is arranged as the following. Section 2, the circuit and the dynamic analysis of chaotic system are given. The encryption algorithm which includes scrambling and diffusion is shown in section 3. Section 4 introduces the complete encryption and decryption scheme. Section 5 illustrates the simulation results and some security analyses. In the last section 6, this paper ends with concluding remarks.

2 Characteristic analysis of a fractional-order hyperchaotic system

2.1 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.1 (a). The two equivalent circuits of two memristors W_1 and W_2 are shown in Fig.1 (b) and (c).

For the Fig.1 (b), 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

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

For the Fig.1 (c), 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 andM_4. The fluxϕ_2(t) of the memristor W_2 is

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

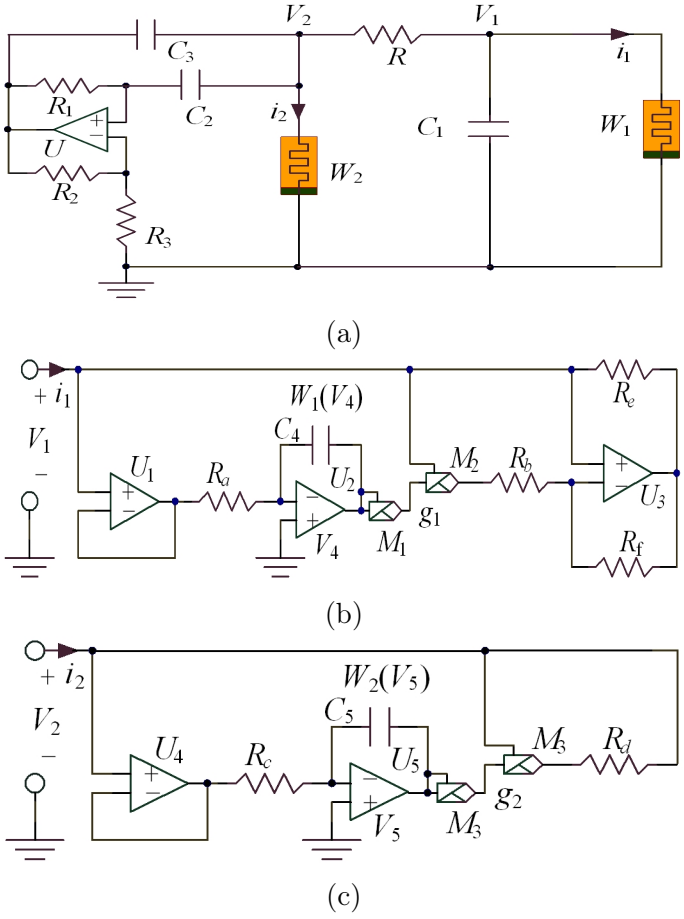


Figure 1: Memristive circuit, (a) BPF memristive Chua's circuit, (b) equivalent circuit for the memristor W_1, (c) equivalent circuit for the memristor W_2

2.2 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

$$\begin{cases} \dot{x} = -c(x-y) + e(1-m_1w^2)x \\ \dot{y} = -s(x-y) + sg(1-m_2u^2)y - (2s+1)/(s+1)nz \\ \dot{z} = -(s+1)(x-y) + (s+1)g(1-m_2u^2)y - 2nz \\ \dot{w} = -px \\ \dot{u} = -py \end{cases} \tag{7}$$

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

$$\begin{cases} {}^*D_{t_0}^q x = -c(x-y) + e(1-m_1w^2)x \\ {}^*D_{t_0}^q y = -s(x-y) + sg(1-m_2u^2)y - (2s+1)/(s+1)nz \\ {}^*D_{t_0}^q z = -(s+1)(x-y) + (s+1)g(1-m_2u^2)y - 2nz \\ {}^*D_{t_0}^q w = -px \\ {}^*D_{t_0}^q u = -py \end{cases} \tag{8}$$

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

$$\begin{bmatrix} Lx \\ Ly \\ Lz \\ Lw \\ Lu \end{bmatrix} = \begin{bmatrix} (e-c)x + cy \\ -sx + sy(g+1) - (2s+1)/(s+1)nz \\ -(s+1)x + (s+1)y(g+1) - 2nz \\ -px \\ -py \end{bmatrix}, \begin{bmatrix} Nx \\ Ny \\ Nz \\ Nw \\ Nu \end{bmatrix} = \begin{bmatrix} -em_1w^2x \\ -sgm_2u^2y \\ -(s+1)gm_2u^2y \\ 0 \\ 0 \end{bmatrix} \tag{9}$$

The before five Adomian polynomials for the nonlinear parts -cm_1w_2, -sgm_2, -u_2 and -$(s+1)gm_2u_2$ are

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

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

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

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

$$\begin{cases} c_1^0 = x^0 \\ c_2^0 = y^0 \\ c_3^0 = w^0 \\ c_4^0 = w^0 \\ c_5^0 = u^0 \end{cases} \tag{14}$$

We can get the coefficients of other term as follows

$$\begin{cases} c_1^1 = & -c(c_1^0 - c_2^0) + ec_1^0 - em_1(c_1^0(c_4^0)^2) \\ c_2^1 = & -s(c_1^0 - c_2^0) + sgc_2^0 - scm_2(c_2^0(c_5^0)^2) - \frac{2s+1}{s+1}nc_3^0 \\ c_3^1 = & -(s+1)(c_1^0 - c_2^0) + (s+1)gc_2^0 - (s+1)gm_2(c_2^0(c_5^0)^2) - 2nc_3^0 \\ c_4^1 = & -pc_1^0 \\ c_5^1 = & -pc_2^0 \end{cases} \tag{15}$$

$$\begin{cases} c_1^2 = & -c(c_1^1 - c_2^1) + ec_1^1 - em_1(c_1^1(c_4^0)^2 + 2c_1^0c_4^1c_4^0) \\ c_2^2 = & -s(c_1^1 - c_2^1) + sgc_2^1 - scm_2(c_2^1(c_5^0)^2 + 2c_2^0c_5^1c_5^0) - \frac{2s+1}{s+1}nc_3^1 \\ c_3^2 = & -(s+1)(c_1^1 - c_2^1) + (s+1)gc_2^1 - (s+1)gm_2(c_2^1(c_5^0)^2 + 2c_2^0c_5^1c_5^0) - 2nc_3^1 \\ c_4^2 = & -pc_1^1 \\ c_5^2 = & -pc_2^1 \end{cases} \tag{16}$$

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

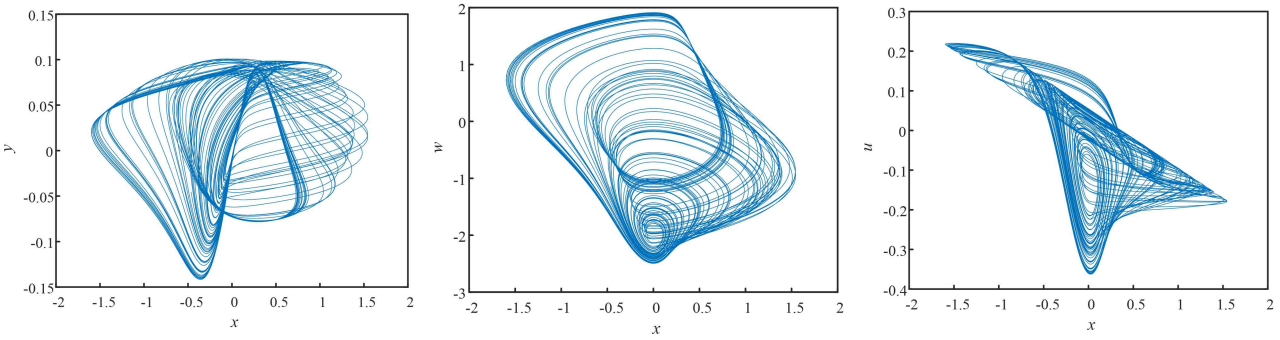
$$\begin{cases} c_1^4 = & -c(c_1^3 - c_2^3) + ec_1^3 - em_1(c_1^3(c_4^0)^2 + 6c_1^2c_4^0c_4^1) \\ & -em_1(6(c_1^1c_4^2c_4^0 + c_1^0c_4^1c_4^2 - c_1^1(c_4^1)^2) - 2c_1^0c_4^3c_4^0) \\ c_2^4 = & -s(c_1^3 - c_2^3) + sgc_2^3 - scm_2(c_2^3(c_5^0)^2 + 6c_2^2c_5^0c_5^1) \\ & -sgm_2(6(c_2^1c_5^2c_5^0 + c_2^0c_5^1c_5^2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

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

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

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 Fig.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 Fig.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.3 (d), (e), (f), because it is much less than 0. From Fig.3(d), 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 [25,44,45].



(a) (b) (c)

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

2.3 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

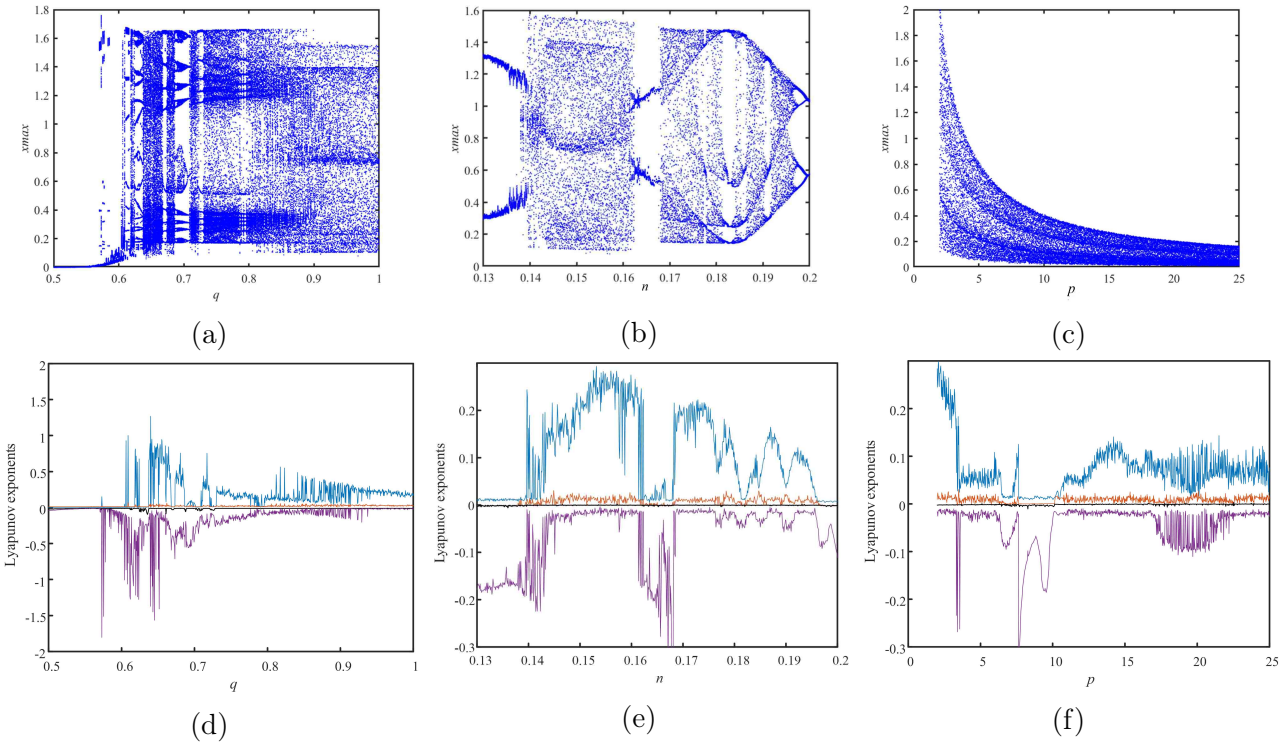


Figure 3: Bifurcation diagrams and Lyapunov exponent spectrums, (a) BD, $q\in(0.5,1)$, (b) BD, $n\in(0.13,0.2)$, (c) BD, $p\in(2,25)$, (d) LES, $q\in(0.5,1)$, (e) LES, $n\in(0.13,0.2)$, (f) LES, $p\in(2,25)$

fractional order. The solution of the differential equation gives the equilibrium point $O(x^0_{(e)}, y^0_{(e)}, z^0_{(e)}, w^0_{(e)}, u^0_{(e)})=[0, 0, 0, \alpha, \beta]$, and α and β on behalf of arbitrary value. For the sake of analysis, if $\alpha=1$ and $\beta=1$, then the equilibrium point $O_1(x^0_{(e)}, y^0_{(e)}, z^0_{(e)}, w^0_{(e)}, u^0_{(e)})=[0, 0, 0, 1, 1]$. Other system parameters are set in accordance with section 2.2, 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.

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

$$\frac{2}{\pi} \min_{i=1,2,\cdots,5} | \, arg(\lambda_i) \, | \le q \le 1 \tag{24}$$

$$| \, arg(\lambda_3, 4) \, | = 1.3625 \tag{25}$$

2.4 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 based on chip F28335 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 Fig.4, 5, 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.

Figure 4: Hardware connection diagram

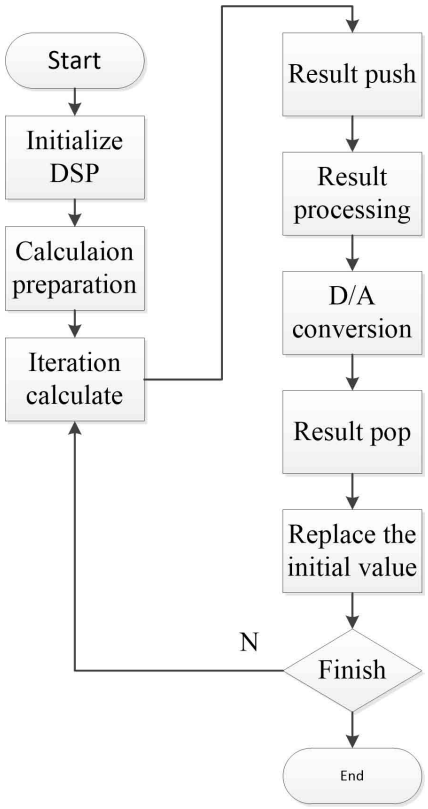


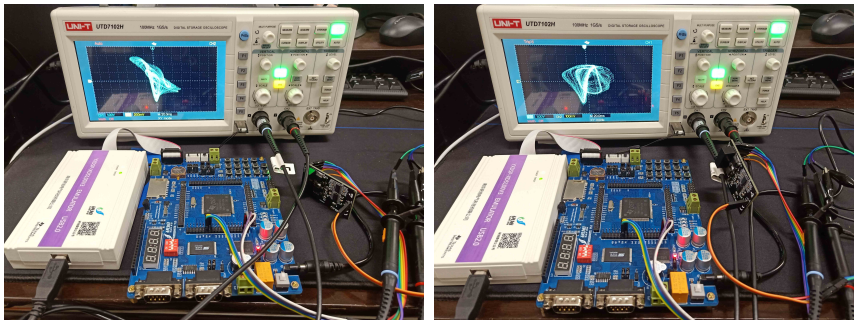
Figure 5: Program flow diagram

Table 1: Parameter configuration

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

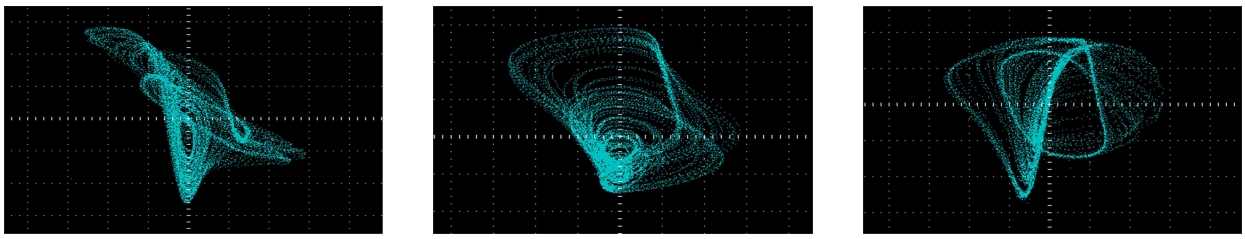
3 The complete encryption scheme

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



(a) (b)

Figure 6: DSP experimental platform construction diagram



(a) (b) (c)

Figure 7: The phase diagrams captured by oscilloscope, (a) x-y plan, (b) x-w plan, (c) x-u plan

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.

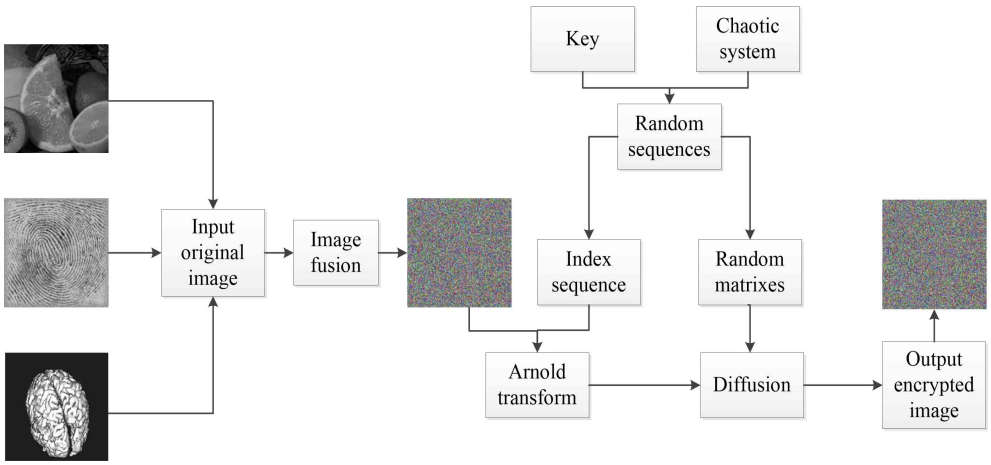


Figure 8: Encryption Scheme

3.1 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.

3.2 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 section 3.1.

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.

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

M and H are length and width of the original images and $(b_1 + a_1. \times (1{:}M \times H)\%(M \times H))$ means the operation of taking the remainder.

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.

3.3 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 section 3.1.

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.

4 Decryption scheme

The algorithm for decryption is the reverse operation of the encryption algorithm, the corresponding flowchart is shown in Fig.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.

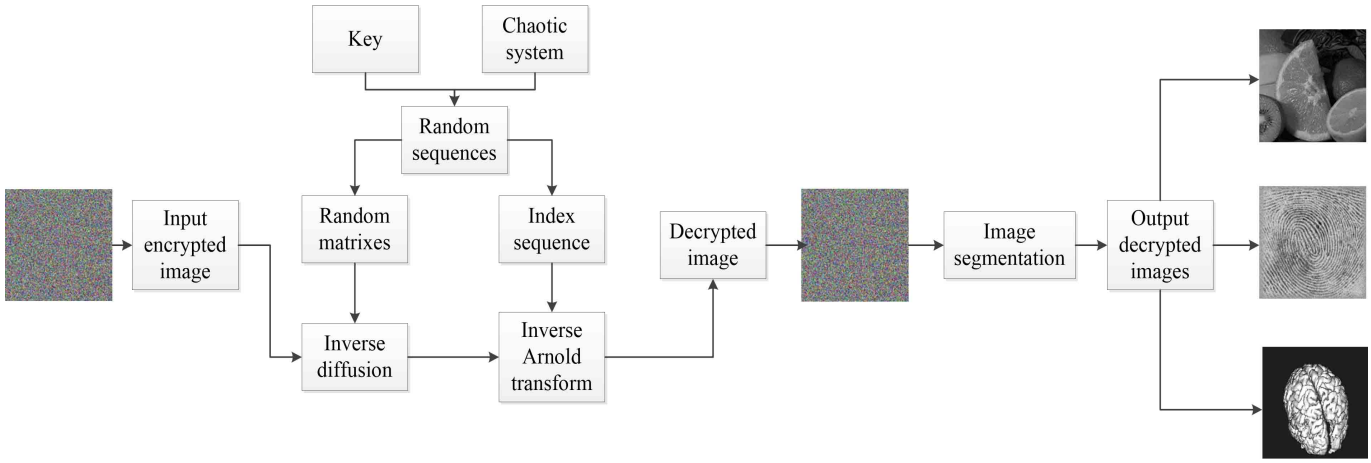


Figure 9: Decryption scheme

Step 1: As described in step one to two of scrambling algorithm section 3.1, 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 section 3.1. 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 section 4.1 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.

5 Performance analysis

5.1 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 fruits, finger and brain in size 256×256 are encrypted and decrypted simultaneously. The simulation results of proposed image encryption and decryption algorithm are shown in Fig.6. Where original images (OI) are Fig.10 (a), (b) and (c), cipher image (CI) is displayed in Fig.10 (d), the corresponding decryption images (DI) are Fig.10 (e), (f) and (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.

5.2 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 [28, 32, 44, 13, 52]. So, the proposed can stand up to brute force attack.

Table 2: Key space of different algorithms

Our algorithm	Ref.[28]	Ref.[32]	Ref.[44]	Ref.[13]	Ref.[52]
2^{750}	2^{213}	2^{580}	2^{497}	2^{374}	2^{399}

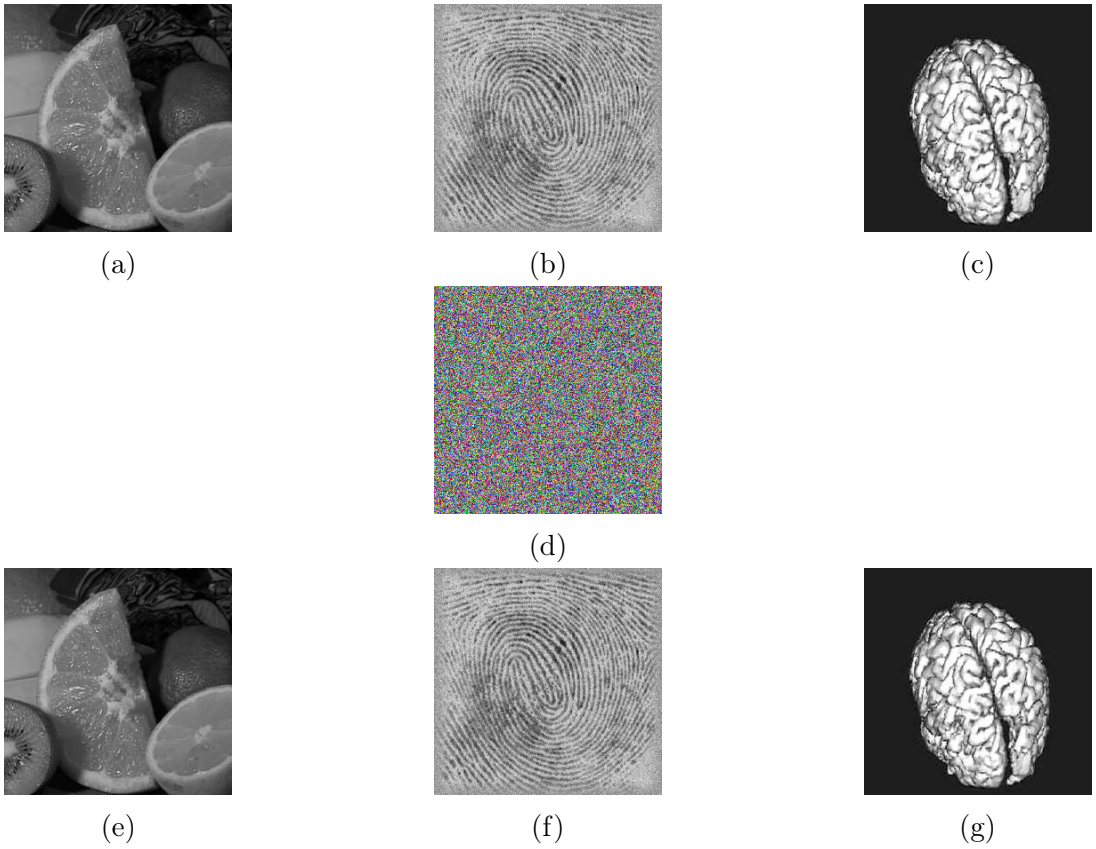


Figure 10: Encrypted and decrypted results, (a) OI, fruits, (b)OI, finger, (c)OI, brain, (d)CI, (e)DI, fruits, (f)DI, finger, (g)DI, brain

5.3 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.

5.4 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 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.

5.5 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:

$$r_{x,y} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}} \tag{38}$$

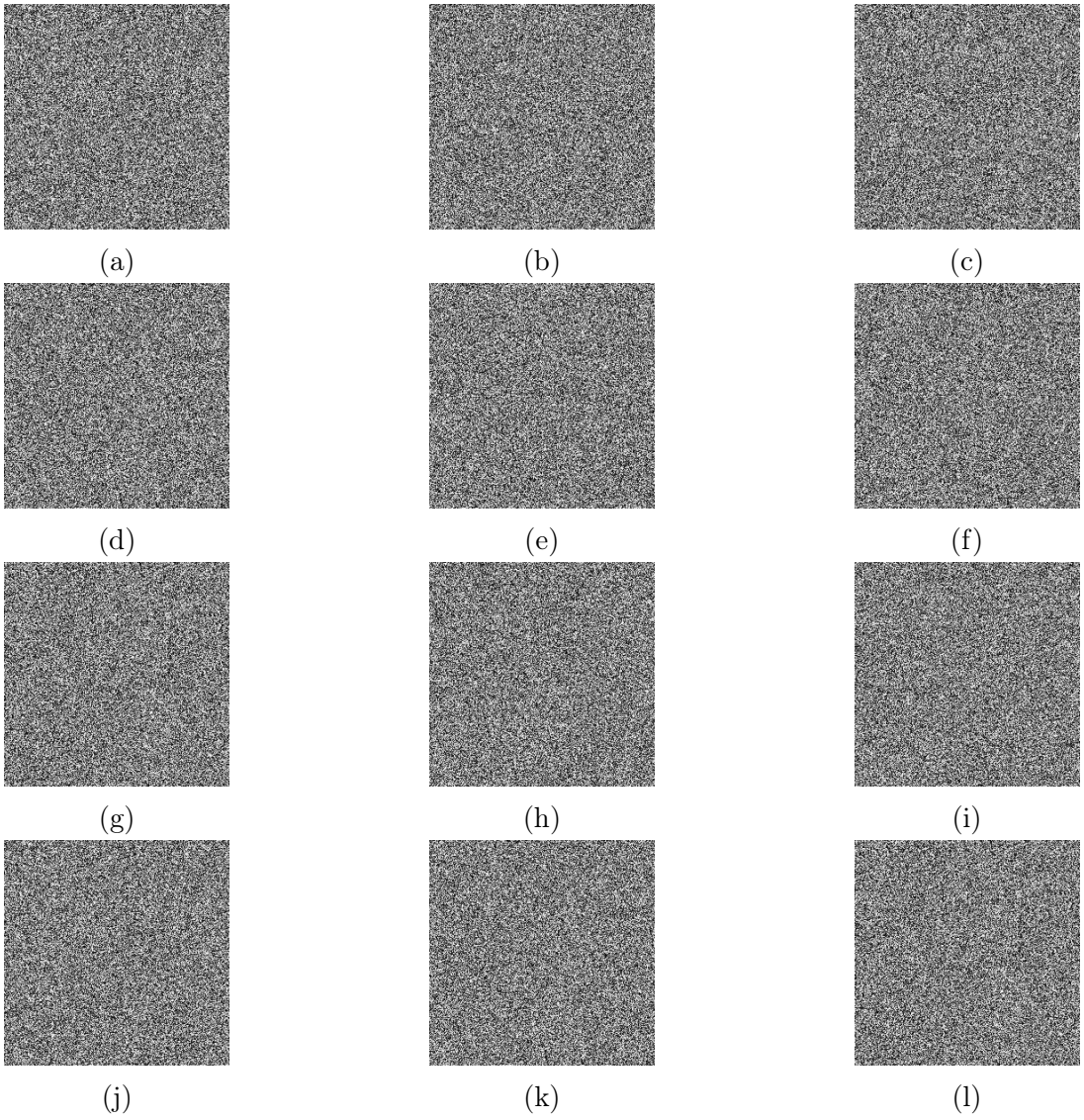


Figure 11: Decrypted results about key sensitivity test, (a)fruits, c=20+1^{-14}, (b)finger, c=20+10^{-14}, (c)brain, c=20+10^{-14}, (d)fruits, g=15+10^{-15}, (e)finger, g=15+10^{-15}, (f)brain, g=15+10^{-15}, (g)fruits, q=0.97+10^{-16}, (h)finger, q=0.97+10^{-16}, (i)brain, q=0.97+10^{-16}, (j)fruits,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

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

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

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 or 5000 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 Fig.13 and Table 3. Results from other literature are also listed in Table 3 [7, 15, 11]. From Fig.13, 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 3 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

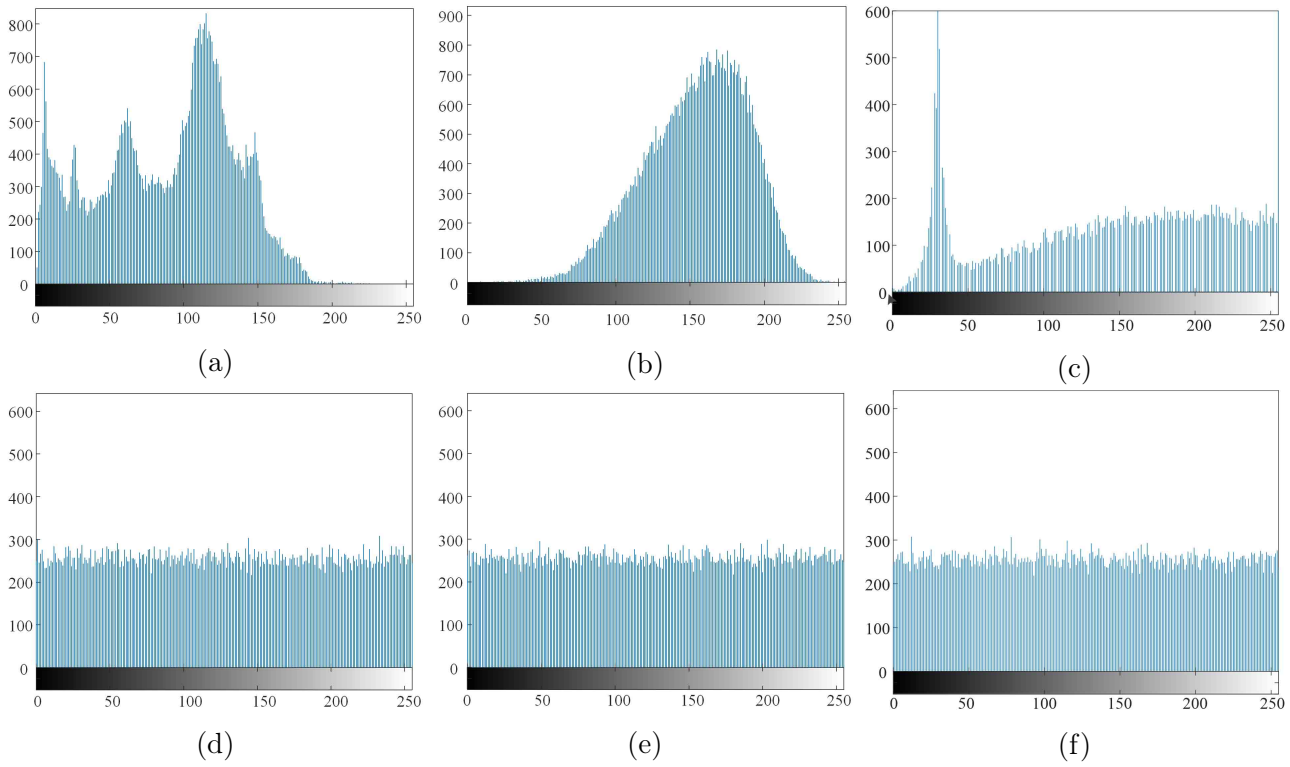


Figure 12: Histogram test, (a)OI, fruits, (b)OI, finger, (c)OI, brain, (d)CI, fruits, (e)CI, finger, (f)CI, brain

correlation coefficients of the encrypted image in corresponding orientations are decreased significantly. The encryption algorithm proposed can effectively against statistical attacks.

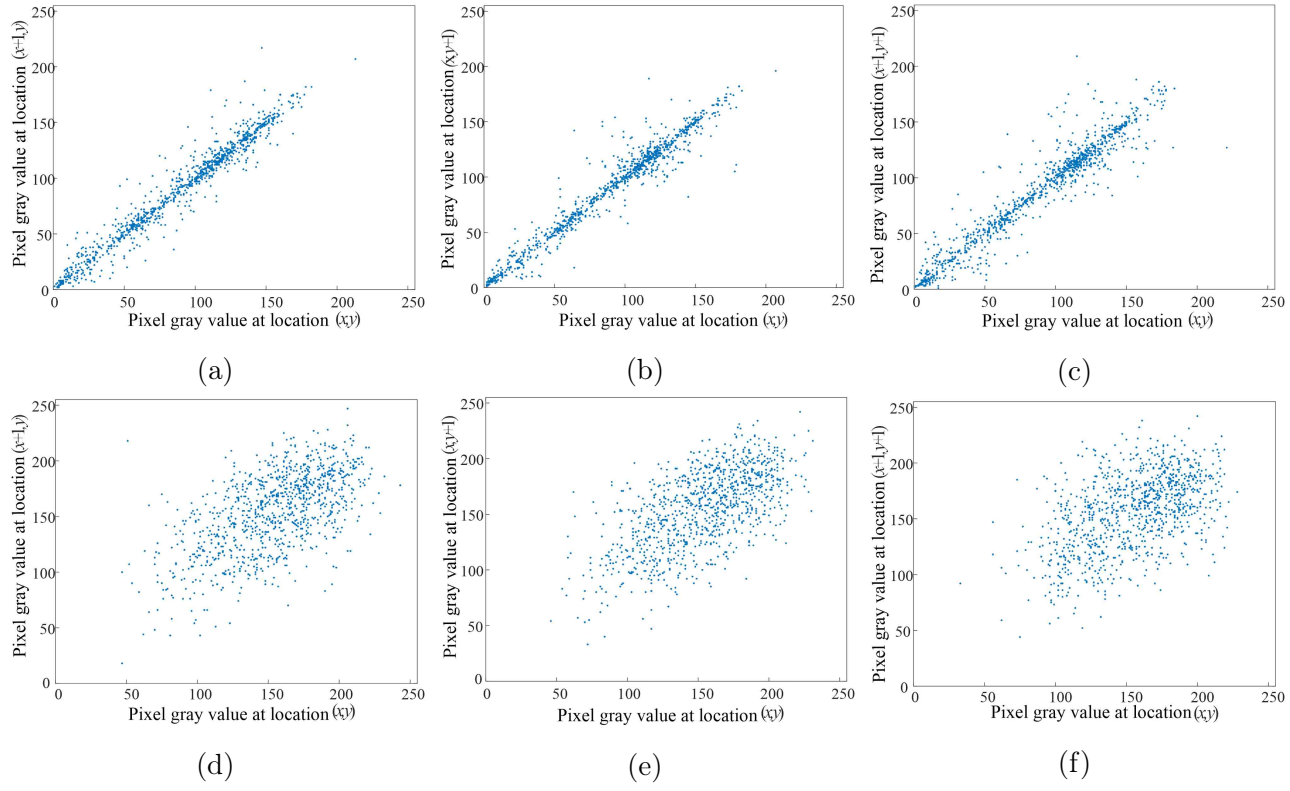


Figure 13a: Correlation of adjacent pixels, (a-c)OI, fruits, (d-f)OI, finger, (g-i)OI,brain, (j-l)CI, fruits, (m-o)CI, finger, (p-r)CI, brain

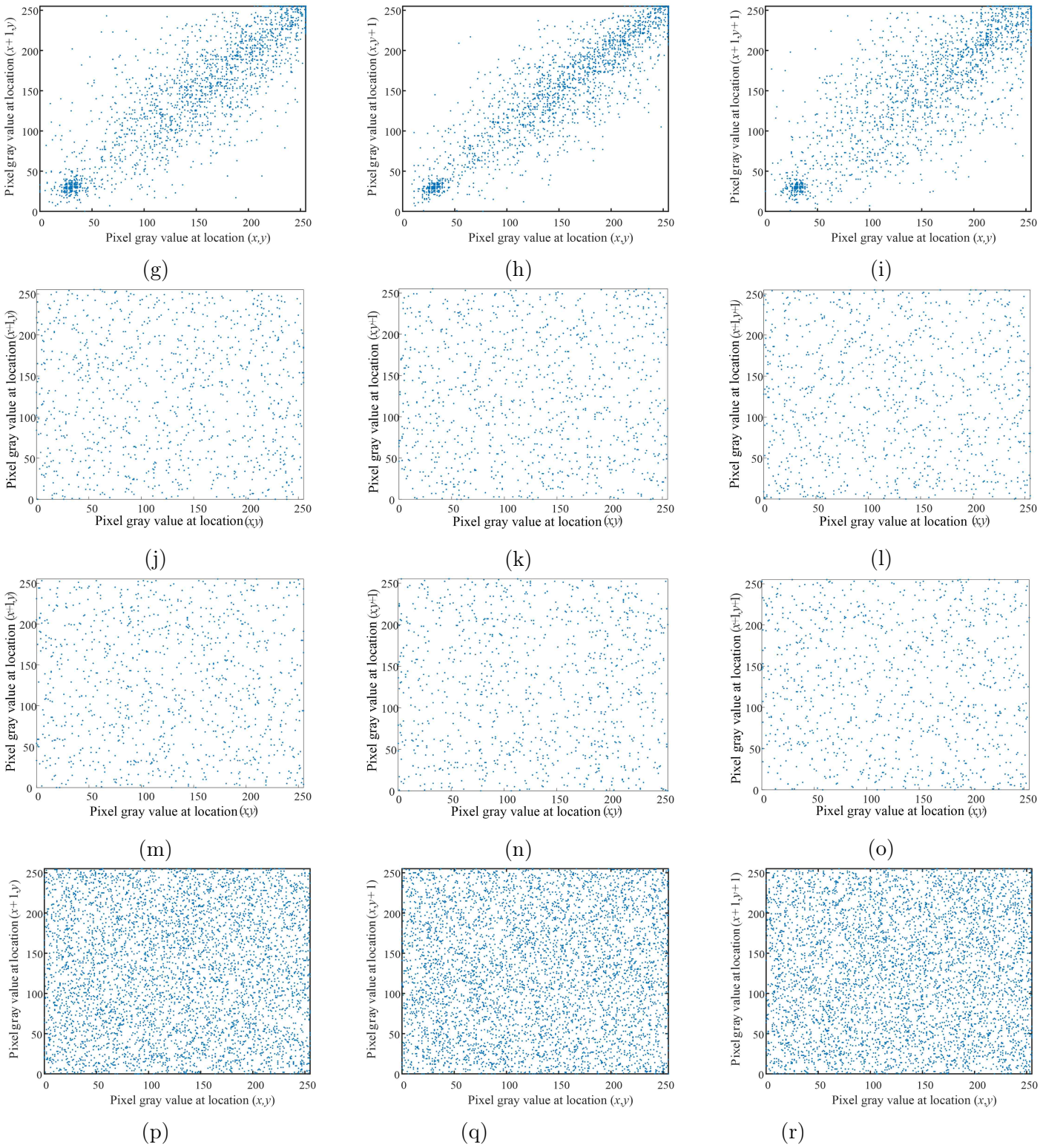


Figure 13b: Correlation of adjacent pixels, (a-c)OI, fruits, (d-f)OI, finger, (g-i)OI, brain, (j-l)CI, fruits, (m-o)CI, finger, (p-r)CI, brain

Table 3: Correlation coefficient pixels

Encryption algorithm	Image	Direction	Plain image	Cipher image
Our scheme	Fruits	H	0.9719	0.0006
		V	0.9736	0.0001
		D	0.9508	0.0023
	Finger	H	0.6161	0.0009
		V	0.5583	0.0058
		D	0.5103	0.0054
	Brain	H	0.9708	0.0055
		V	0.9550	0.0029
		D	0.9326	-0.0009
Ref.[15]	Image	H	0.9724	0.0118
		V	0.9455	-0.0173
		D	0.9214	0.0080
Ref.[7]	Image	H	0.9724	-0.0048
		V	0.9455	-0.0112
		D	0.9214	-0.0125
Ref.[11]	Image	H	0.9724	0.0070
		V	0.9455	-0.0102
		D	0.9214	0.0030

5.6 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 $\mathrm{P}(x_i)$ is the probability of gray value x_i.

Information entropies of original images and cipher images are listed in Table 4. The information entropies of cipher images are more than 7.997 and close to 8. From Table 4, the information entropy of our scheme and others in Refs. [34, 17, 15, 38] are given, a conclusion that the proposed algorithm can generate cipher images with strong randomness can be drawn.

Table 4: Information entropy of original images and cipher images

Encryption algorithm	Image	Image size	Original image	Cipher image
Our scheme	Fruits	256×256	7.3406	7.9972
	Finger	256×256	7.1075	7.9977
	Brain	256×256	4.1514	7.9974
Ref.[15]	Airplane	256×256	-	7.9971
Ref.[38]	Baboon	256×256	7.1273	7.9974
Ref.[38]	Average	256×256	7.4127	7.9973
Ref.[34]	Average	256×256	7.3446	7.9970
Ref.[17]	Average	256×256	7.6560	7.9969

5.7 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:

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

$$UACI(P_1, P_2) = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\mid P_1(i,j) - P_2(i,j) \mid}{255 - 0} \times 100\% \tag{43}$$

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 5. From the Table 5, 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 6 [6, 2, 51, 9]. Results indicate that our algorithm can resist differential attack effectively.

Table 5: The results of differential attack test

Image	Fruits	Finger	Brain	Average
NPCR(%)	99.5987	99.6231	99.5850	99.6023
UACI(%)	33.5054	33.4632	33.5239	33.4975

Table 6: NPCR and UACI values of different algorithms

	Our algorithm	Ref.[6]	Ref.[2]	Ref.[9]	Ref.[51]
NPCR(%)(average)	99.6023	99.610	99.6117	99.6082	99.5582
UACI(%)(average)	33.4975	33.462	33.6694	33.3391	33.3844

5.8 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.

5.8.1 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.14. 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.

5.8.2 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 to resist cropping attack. The simulation results are shown in Fig.15, while encrypted image lose 6.25%

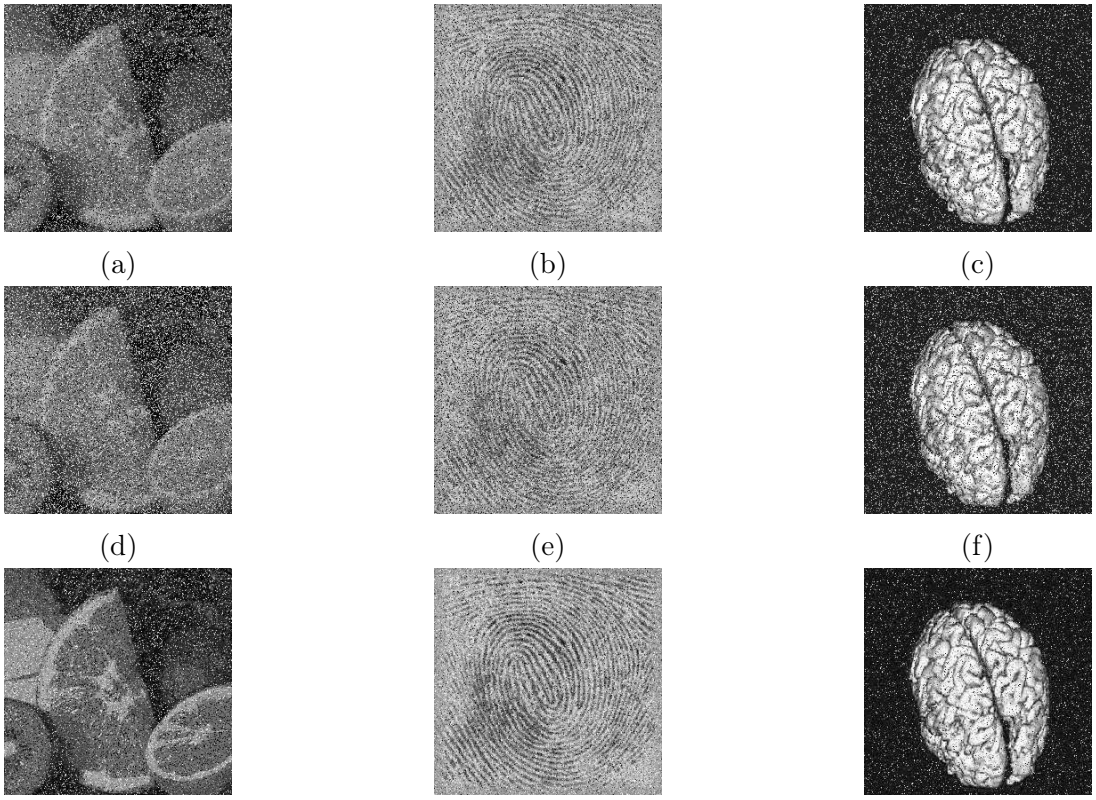


Figure 14: Decrypted images with various noise, (a-c) SPN, 0.05, (d-f) SPN, 0.07, (g-i)GN, 0.0001

data, decrypted images which include fruits, finger and brain are Fig.15 (a-d). While encrypted image 12.5% data are cropped, decrypted images are shown in Fig.15 (e-h). While encrypted image 25% data are removed, the results of decryption are shown in Fig.15 (i-l). 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.

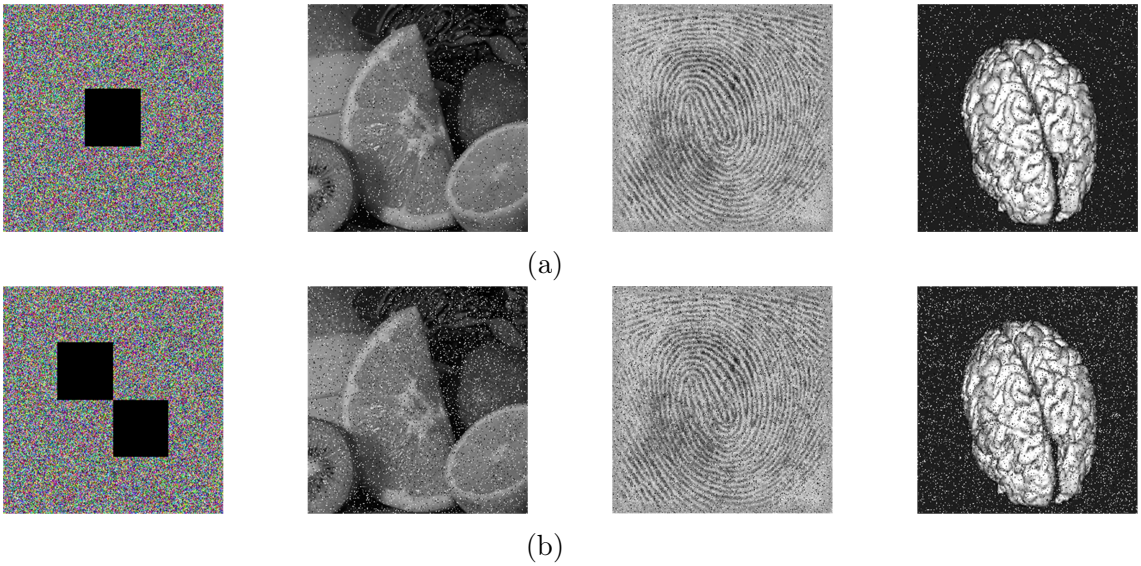
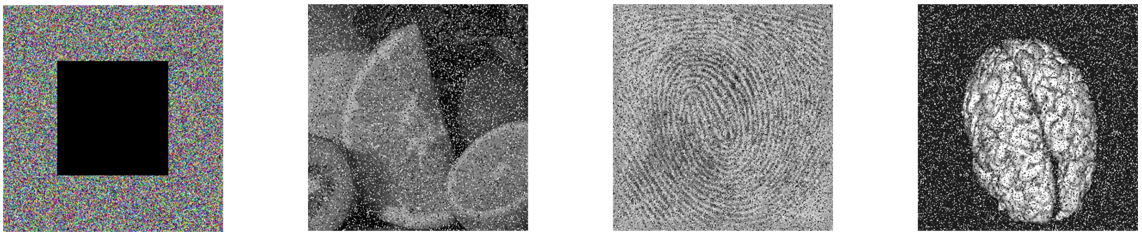


Figure 15a: Cropping attack test, (a) 6.25% data loss, encrypted image and decrypted images, (b) 12.5% data loss, encrypted image and decrypted images, (c) 25% data loss, encrypted image and decrypted images



(c)

Figure 15b: 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

6 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.

Acknowledgements

This work was supported by Provincial Natural Science Foundation of Liaoning (Grant Nos. 2020-MS-274); National Natural Science Foundation of China (Grant Nos. 62061014).

Author contributions

Xinyu Gao designed and carried out experiments, data analyzed and manuscript wrote. Jiawu Yu, Huizhen Yan and Jun Mou made the theoretical guidance for this paper.

Conflicts of Interest

No conflicts of interests about the publication by all authors.

References

[1] A novel simple chaotic circuit based on memristor–memcapacitor. *Nonlinear Dynamics*, 100(5), 2020.

[2] A. A. Abbasi, M. Mazinani, and R. Hosseini. Chaotic evolutionary-based image encryption using rna codons and amino acid truth table. *Optics & Laser Technology*, 132(12):106465, 2020.

[3] M. H. Annaby, M. A. Rushdi, and E. A. Nehary. Image encryption via discrete fractional fourier-type transforms generated by random matrices. *Signal Processing Image Communication*, 49:25–46, 2016.

[4] R. Ba Nsal, S. Gupta, and G. Sharma. An innovative image encryption scheme based on chaotic map and vigenère scheme. *Multimedia Tools & Applications*, 76(15):1–34, 2016.

[5] B. Bao, T. Jiang, G. Wang, P. Jin, H. Bao, and M. Chen. Two-memristor-based chua's hyperchaotic circuit with plane equilibrium and its extreme multistability. *Nonlinear Dynamics*, 2017.

[6] Z. Bashir, T. Rashid, and S. Zafar. Hyperchaotic dynamical system based image encryption scheme with time-varying delays. *Pacific Science Review A Natural Science & Engineering*, 18(3):254–260, 2016.

[7] Akram Belazi, Ahmed A. Abd El-Latif, and Safya Belghith. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, 128(Nov.):155–170, 2016.

[8] M. Brindha and N Ammasai Gounden. A chaos based image encryption and lossless compression algorithm using hash table and chinese remainder theorem. *Applied Soft Computing*, 40:379–390, 2016.

[9] C. Cao, K. Sun, and W. Liu. A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map. *Signal Processing*, 143(FEB.):122–133, 2017.

[10] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen. A color image cryptosystem based on dynamic dna encryption and chaos. *Signal Processing*, 155(FEB.):44–62, 2019.

[11] X. Chai, J. Zhang, Z. Gan, and Y. Zhang. Medical image encryption algorithm based on latin square and memristive chaotic system. *Multimedia Tools and Applications*, (21), 2019.

[12] X. Chai, X. Zheng, Z. Gan, and Y. Chen. Exploiting plaintext-related mechanism for secure color image encryption. *Neural Computing and Applications*, (1), 2019.

[13] L. P. Chen, H. Yin, L. G. Yuan, A. M. Lopes, and RC Wu. 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(6):866–879, 2020.

[14] R. Enayatifar, F. G. Guimaraes, and P. Siarry. Index-based permutation-diffusion in multiple-image encryption using dna sequence. *Optics and Lasers in Engineering*, 115(APR.):131–140, 2019.

[15] Mab Farah, A. Farah, and T. Farah. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynamics*, 99(1):1–24, 2020.

[16] J. Fridrich. Image encryption based on chaotic maps. In *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation.*

[17] M. Hanif, R. A. Naqvi, S. Abbas, M. A. Khan, and N. Iqbal. A novel and efficient 3d multiple images encryption scheme based on chaotic systems and swapping operations. *IEEE Access*, PP(99):1–1, 2020.

[18] S. He, K. Sun, X. Mei, B. Yan, and S. Xu. Numerical analysis of a fractional-order chaotic system based on conformable fractional-order derivative. *European Physical Journal Plus*, 132(1):36, 2017.

[19] S. He, K. Sun, and H. Wang. Dynamics and synchronization of conformable fractional-order hyperchaotic systems using the homotopy analysis method. *Communications in Nonlinear Science and Numerical Simulation*, 2019.

[20] T. Hu, Y. Liu, L. H. Gong, S. F. Guo, and H. M. Yuan. Chaotic image cryptosystem using dna deletion and dna insertion. *Signal Processing*, 134(may):234–243, 2017.

[21] T. Hu, L. Ye, L. H. Gong, and C. J. Ouyang. An image encryption scheme combining chaos with cycle operation for dna sequences. *Nonlinear Dynamics*, 87(1):1–16, 2016.

[22] Z. Hua, Y Zhou, and H. Huang. Cosine-transform-based chaotic system for image encryption. *Information Sciences*, 480:403–419, 2019.

[23] N. Iqbal, S. Abbas, A. Khan, T. Alyas, and A. Ahmad. An rgb image encryption scheme using chaotic systems, 15-puzzle problem and dna computing. *IEEE Access*, PP(99):1–1, 2019.

[24] A A Karawia. Encryption algorithm of multiple-image using mixed image elements and two dimensional chaotic economic map. *Entropy*, 20(10):801, 2018.

[25] C. Lia, D. Lina, J Lu¨B, and H. Feng. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. *IEEE Multimedia*, 25(4):46–56, 2019.

[26] K. Manjit and K. Vijay. Adaptive differential evolution based lorenz chaotic system for image encryption. *ARABIAN JOURNAL FOR SCIENCE AND ENGINEERING*, pages 1–18, 2018.

[27] F. Masood, J. Ahmad, S. A. Shah, S. Sajjad, and I. Hussain. A novel hybrid secure image encryption based on julia set of fractals and 3d lorenz chaotic map. *Entropy*, 22(3):274, 2020.

[28] Mohamed, ElKamchouchi, and Moussa. A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial dna sequences. *Entropy*, 22(2):158, 2020.

[29] A Mzt and B Xw. A new fractional one dimensional chaotic map and its application in high-speed image encryption. *Information Sciences*, 2020.

[30] Y. Niu, X Sun, C. Zhang, and H. Liu. Anticontrol of a fractional-order chaotic system and its application in color image encryption. *Mathematical Problems in Engineering*, 2020, 2020.

[31] A. Y. Niyat and M. H. Moattar. Color image encryption based on hybrid chaotic system and dna sequences. *Multimedia Tools and Applications*, 79(1):1497–1518, 2020.

[32] X Ouyang, Y. Luo, J. Liu, L. Cao, and Y. Liu. A color image encryption method based on memristive hyperchaotic system and dna encryption. *International Journal of Modern Physics B*, 34(4):2050014, 2020.

[33] S. M. Pan, R. H. Wen, Z. H. Zhou, and N. R. Zhou. Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional mellin transform. *Multimedia Tools & Applications*, 76(2):2933–2953, 2017.

[34] Kak Patro and B. Acharya. A novel multi-dimensional multiple image encryption technique. *Multimedia Tools and Applications*, 79(5), 2020.

[35] Sheela, S., J., Suresh, K., V., Tandur, and Deepaknath. Image encryption based on modified henon map using hybrid chaotic shift transform. *Multimedia tools and applications*, 77(19):25223–25251, 2018.

[36] K. J. Sher and A. Jawad. Chaos based efficient selective image encryption. *Multidimensional Systems and Signal Processing*, 2019.

[37] A. Vaish and M. Kumar. Color image encryption using msvd, dwt and arnold transform in fractional fourier domain. *Optik - International Journal for Light and Electron Optics*, 145, 2017.

[38] X. Wang, L. Liu, and Y. Zhang. A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Optics and Lasers in Engineering*, 66:10–18, 2015.

[39] X. Y. Wang, P. Li, Y. Q. Zhang, L. Y. Liu, H. Zhang, and X. Wang. A novel color image encryption scheme using dna permutation based on the lorenz system. *Multimedia Tools and Applications*, 2018.

[40] S. Weng, Y. Q. Shi, W. Hong, and Y. Yao. Dynamic improved pixel value ordering reversible data hiding. *Information Sciences*, 489:136–154, 2019.

[41] X. Wu, K. Wang, X. Wang, and H. Kan. Lossless chaotic color image cryptosystem based on dna encryption and entropy. *Nonlinear Dynamics*, 2017.

[42] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths. Color image dna encryption using nca map-based cml and one-time keys. *Signal Processing*, 148(jul.):272–287, 2018.

[43] A Xdc, W. A. Ying, A Jw, and B Qhw. 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, 2019.

[44] Xingyuan, Wang, Yu, Wang, Xiaoqiang, Zhu, Chao, and Luo. 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(C):105851–105851.

[45] F. Yang, J. Mou, C. Ma, and Y. Cao. Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. *Optics and Lasers in Engineering*, 129.

[46] L. Y. Zhang, Y. Liu, F Pareschi, Y. Zhang, K. W. Wong, R. Rovatti, and G. Setti. On the security of a class of diffusion mechanisms for image encryption. *IEEE Transactions on Cybernetics*, PP(99):1–13, 2015.

[47] W. Zhang, H. Yu, Y. L. Zhao, and Z. L. Zhu. Image encryption based on three-dimensional bit matrix permutation. *Signal Processing*, 118:36–50, 2016.

[48] X. Zhang and X. Wang. Multiple-image encryption algorithm based on mixed image element and permutation. *Computers & Electrical Engineering*, 62(MAY):6–16, 2017.

[49] X. Zhang and X. Wang. Multiple-image encryption algorithm based on dna encoding and chaotic system. *Multimedia Tools and Applications*, 78(6):7841–7869, 2019.

[50] X. Zhang, Z. Zhao, and J. Wang. Chaotic image encryption based on circular substitution box and key stream buffer. *SIGNAL PROCESSING-IMAGE COMMUNICATION*, 29(8):902–913, 2014.

[51] Y. Q. Zhang and X. Y. Wang. A new image encryption algorithm based on non-adjacent coupled map lattices. *Applied Soft Computing*, 26:10–20, 2015.

[52] M. Zhou and C. Wang. A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. *Signal Processing*, 171:107484–, 2020.

[53] Nanrun Zhou, Hao Jiang, Lihua Gong, and Xinwen Xie. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. *Optics & Lasers in Engineering*, 110(NOV.):72–79, 2018.

[54] C. Zhu and K. Sun. Cryptanalyzing and improving a novel color image encryption algorithm using rt-enhanced chaotic tent maps. *IEEE Access*, pages 1–1, 2018.

Figures

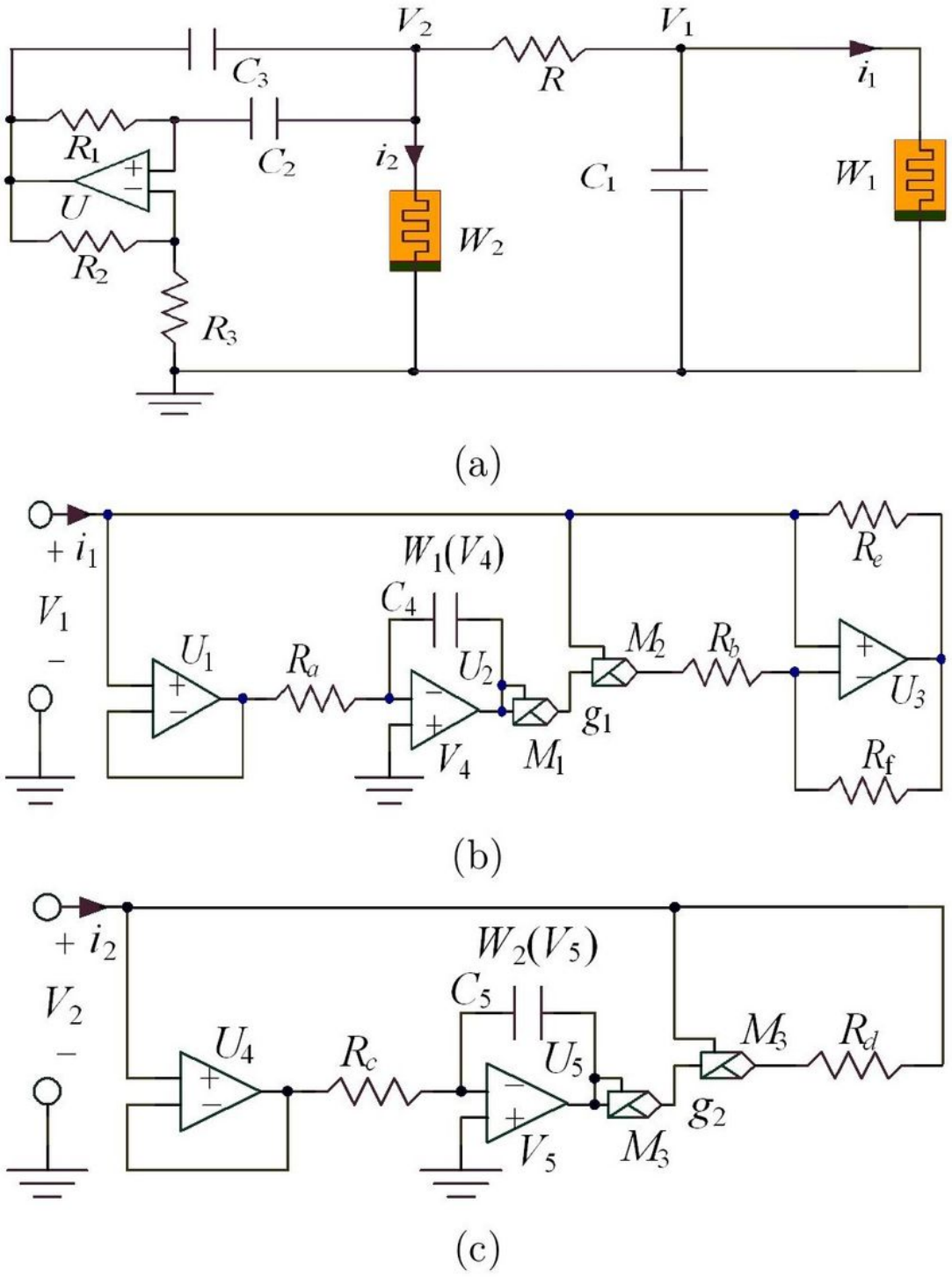


Figure 1

Please see the Manuscript PDF file for the complete figure caption

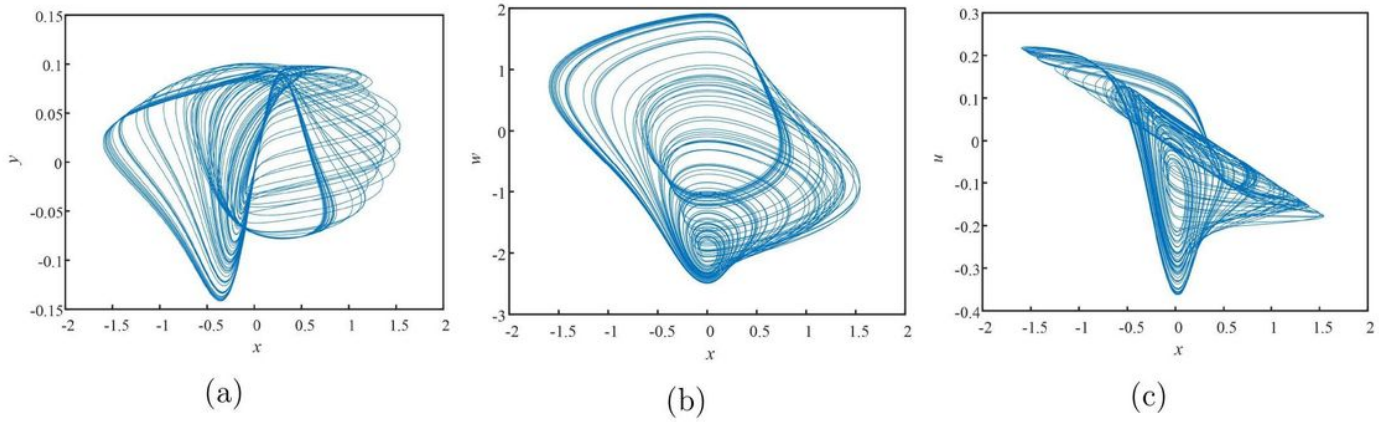


Figure 2

Please see the Manuscript PDF file for the complete figure caption

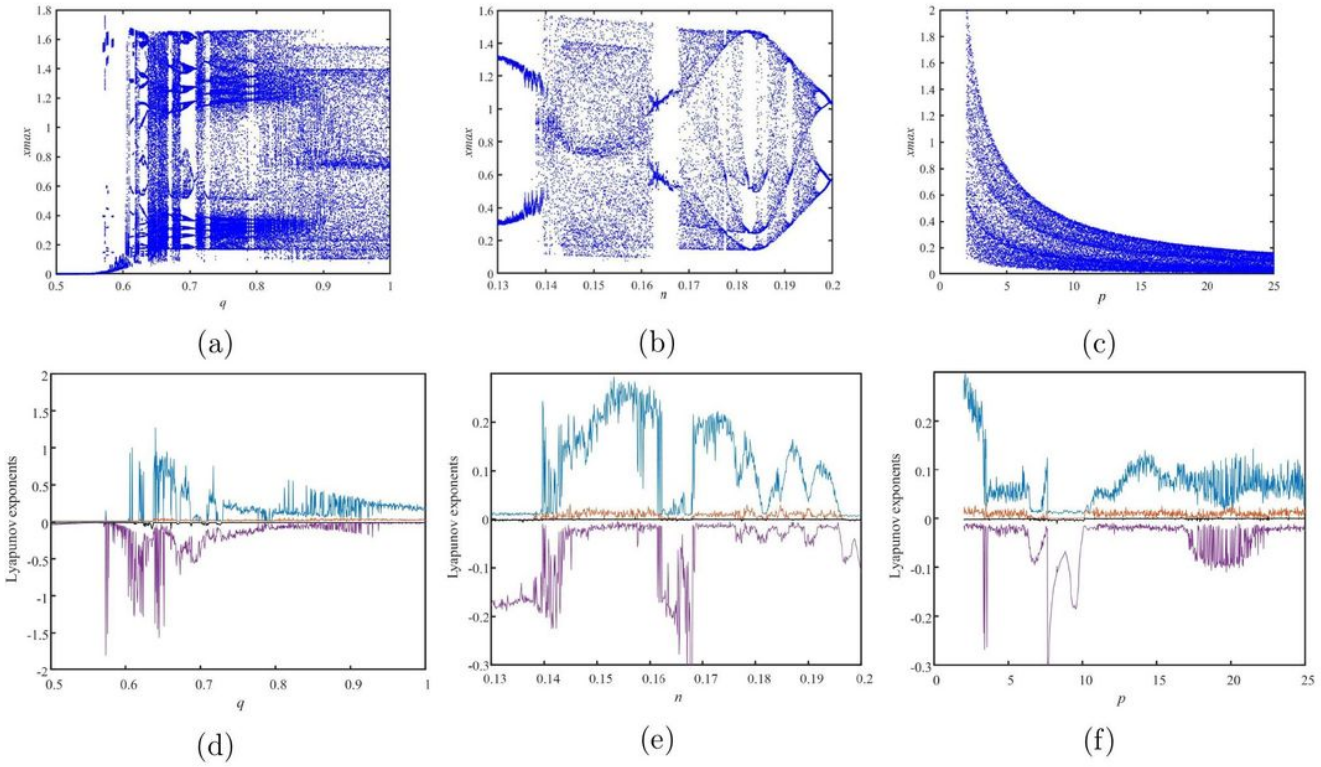


Figure 3

Please see the Manuscript PDF file for the complete figure caption

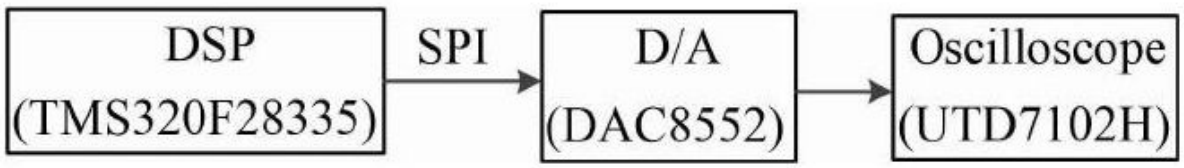


Figure 4

Please see the Manuscript PDF file for the complete figure caption

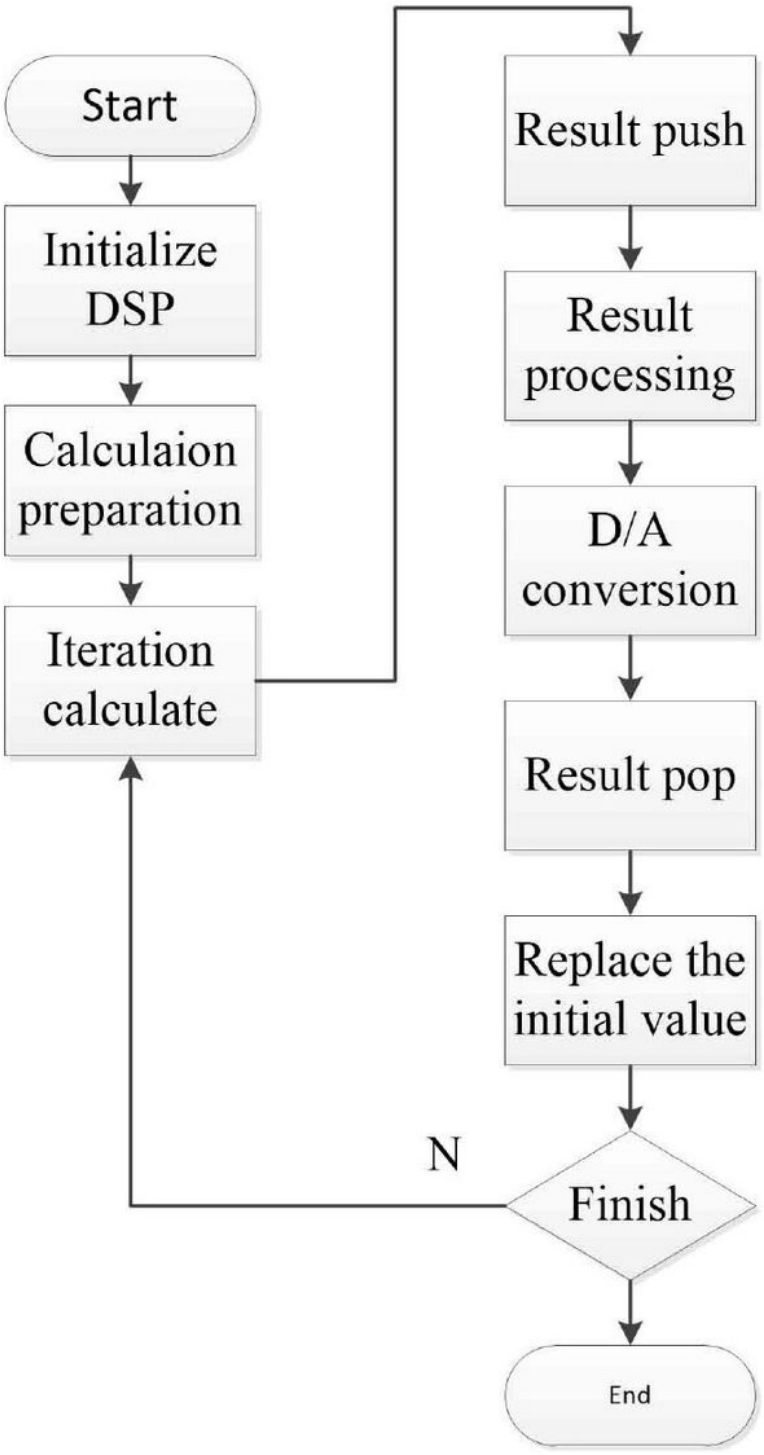


Figure 5

Please see the Manuscript PDF file for the complete figure caption

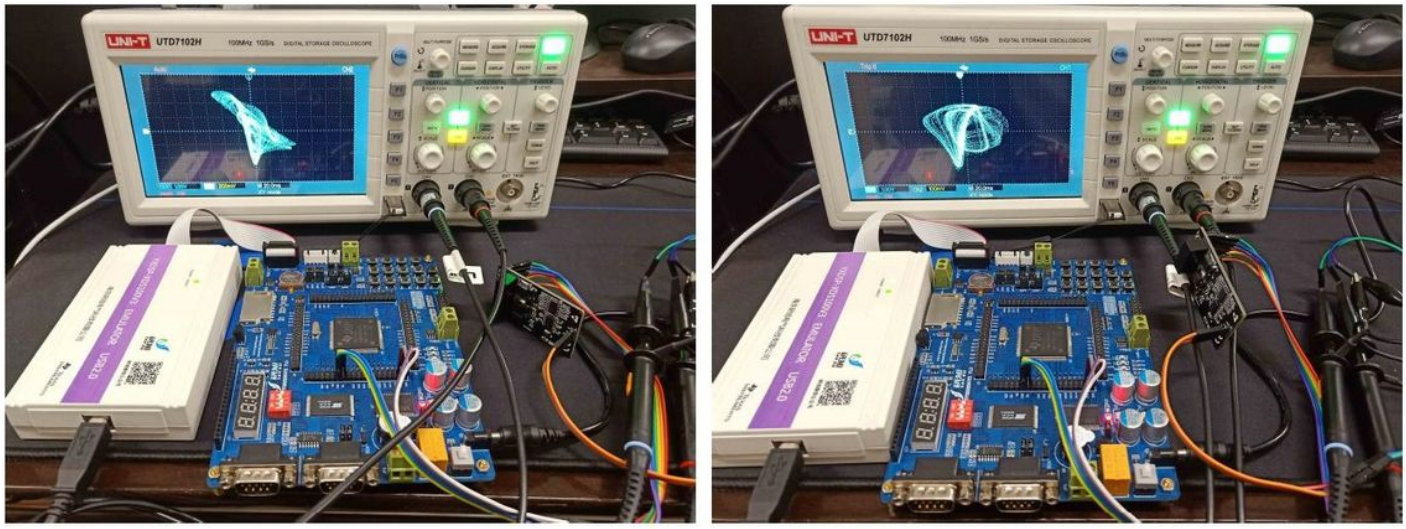


Figure 6

Please see the Manuscript PDF file for the complete figure caption

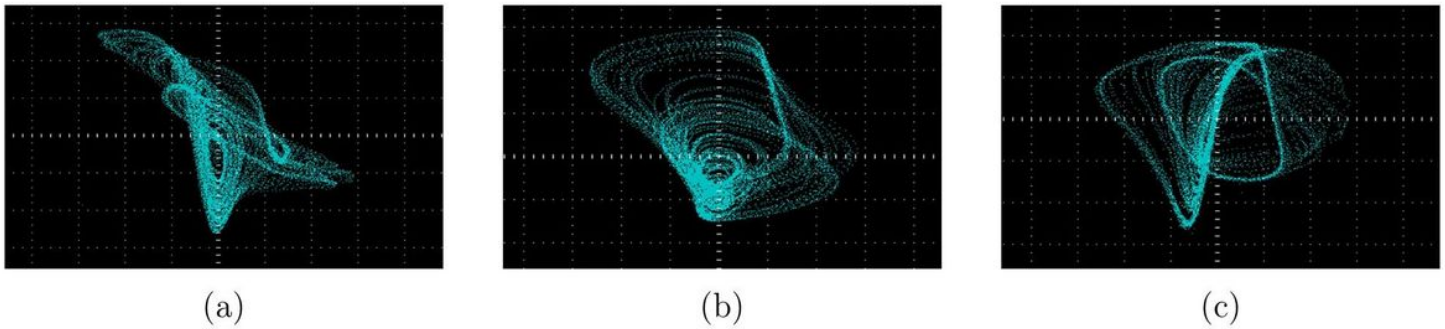


Figure 7

Please see the Manuscript PDF file for the complete figure caption

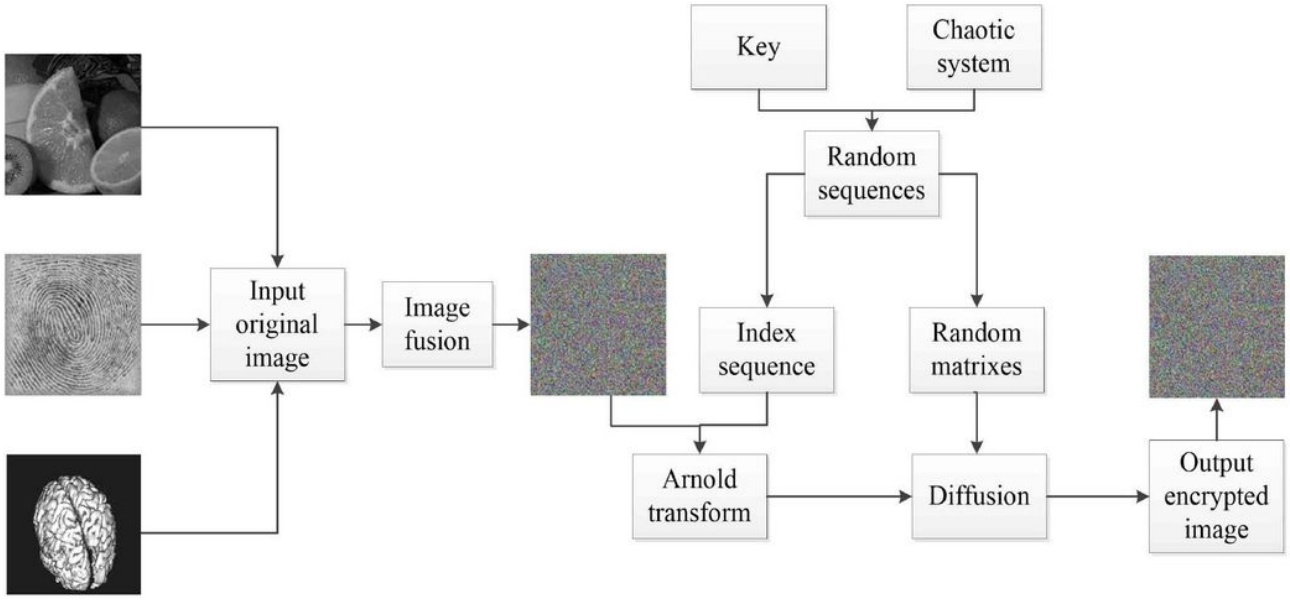


Figure 8

Please see the Manuscript PDF file for the complete figure caption

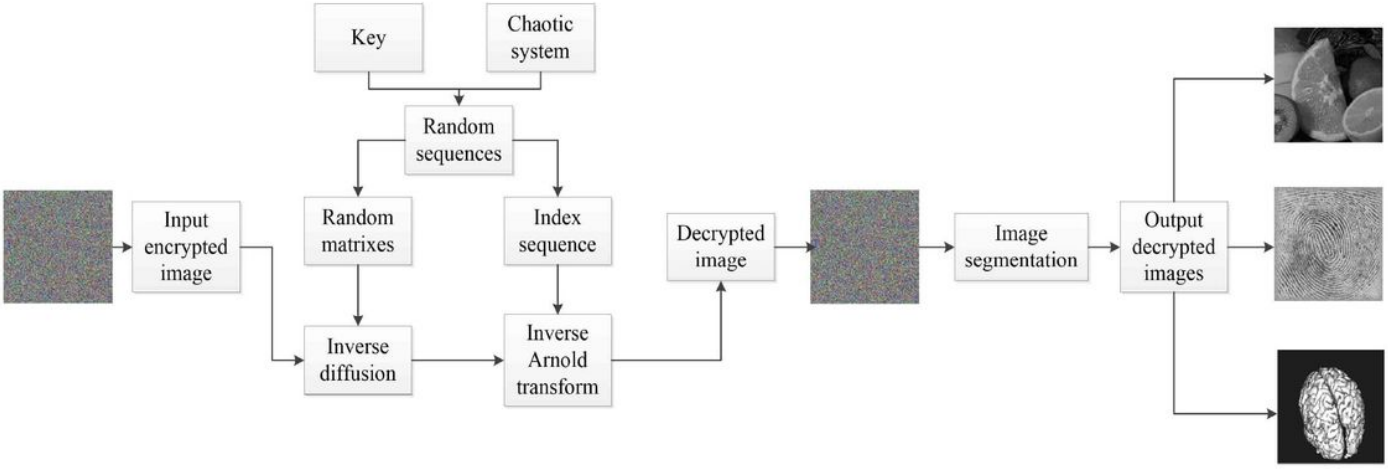


Figure 9

Please see the Manuscript PDF file for the complete figure caption

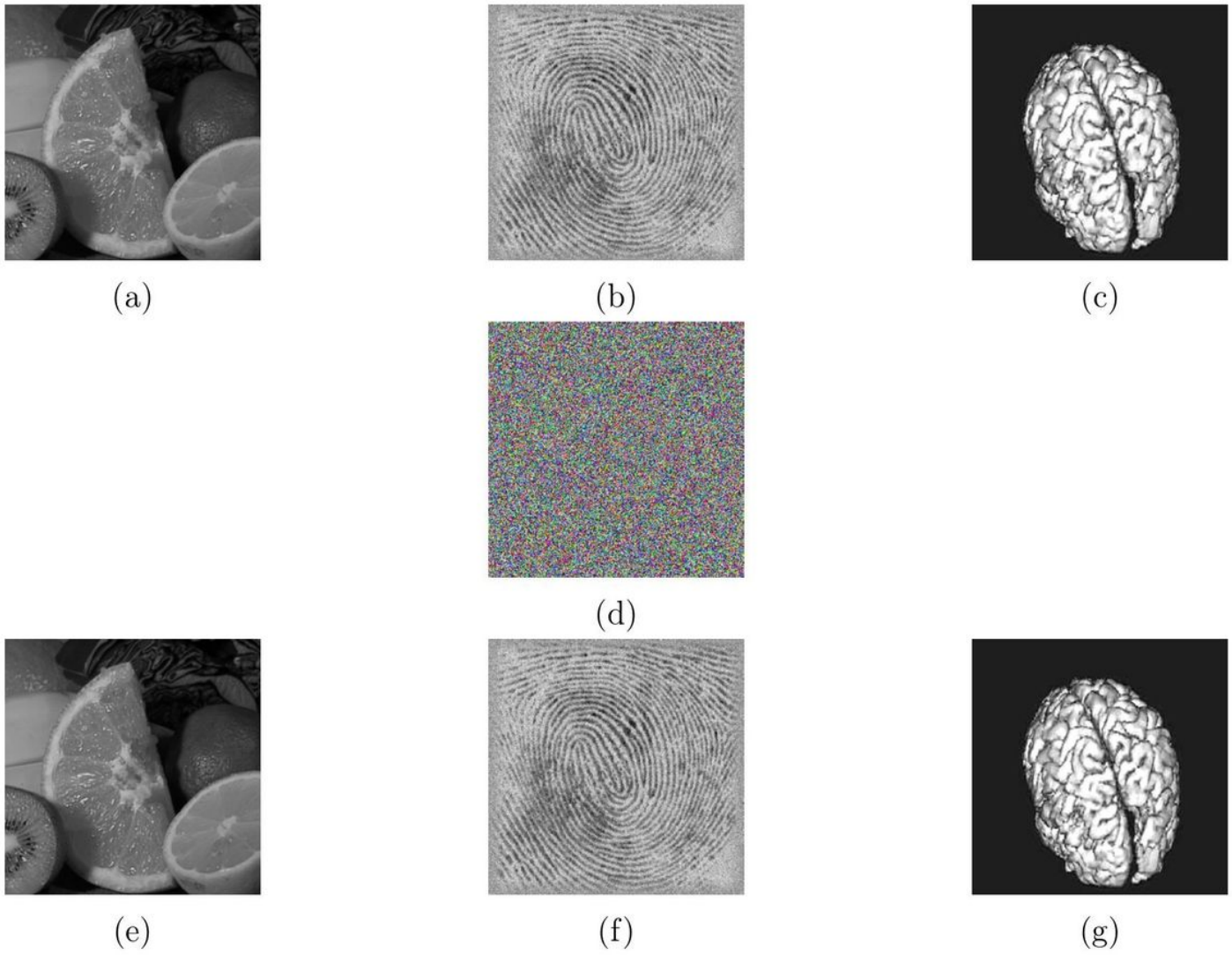


Figure 10

Please see the Manuscript PDF file for the complete figure caption

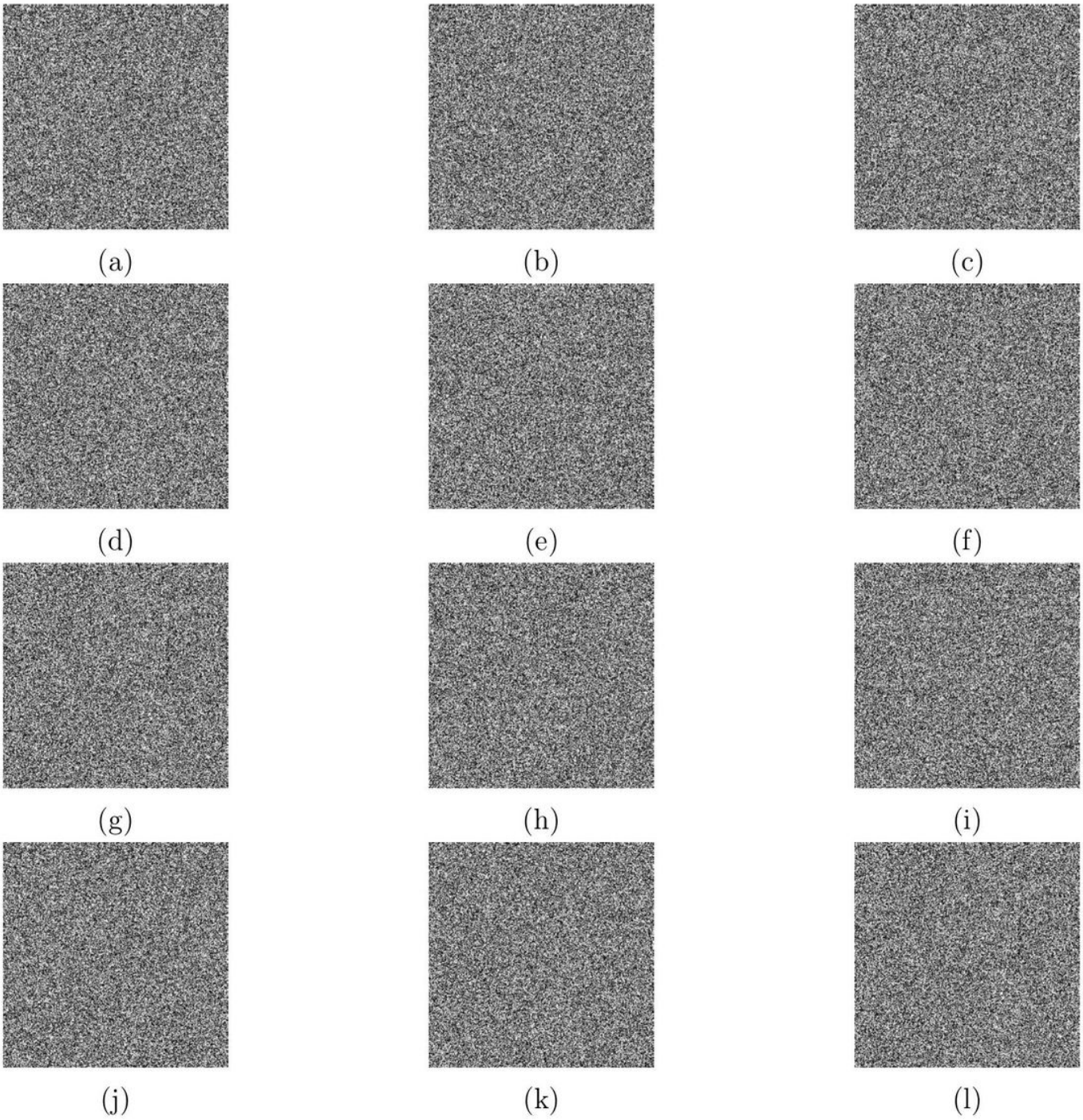


Figure 11

Please see the Manuscript PDF file for the complete figure caption

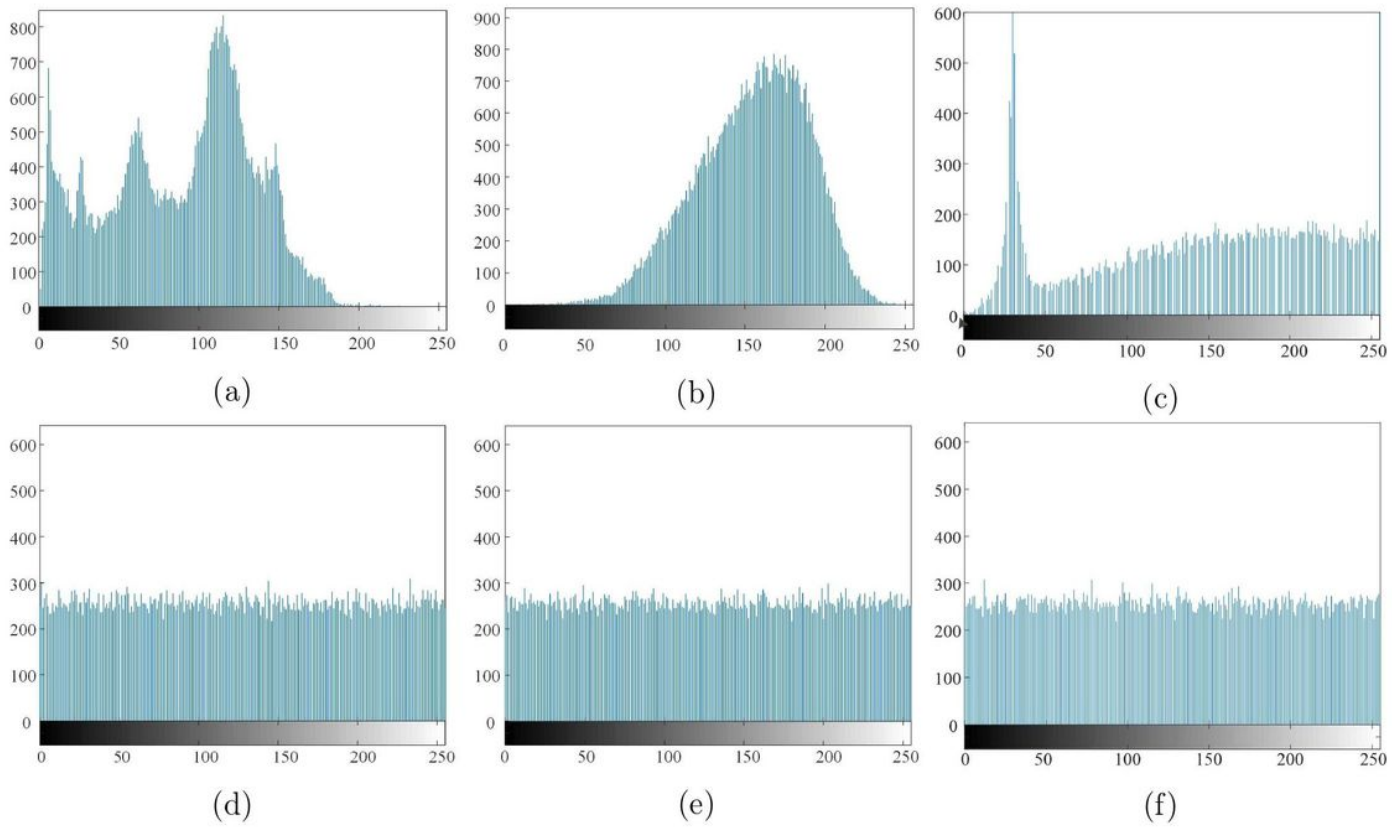


Figure 12

Please see the Manuscript PDF file for the complete figure caption

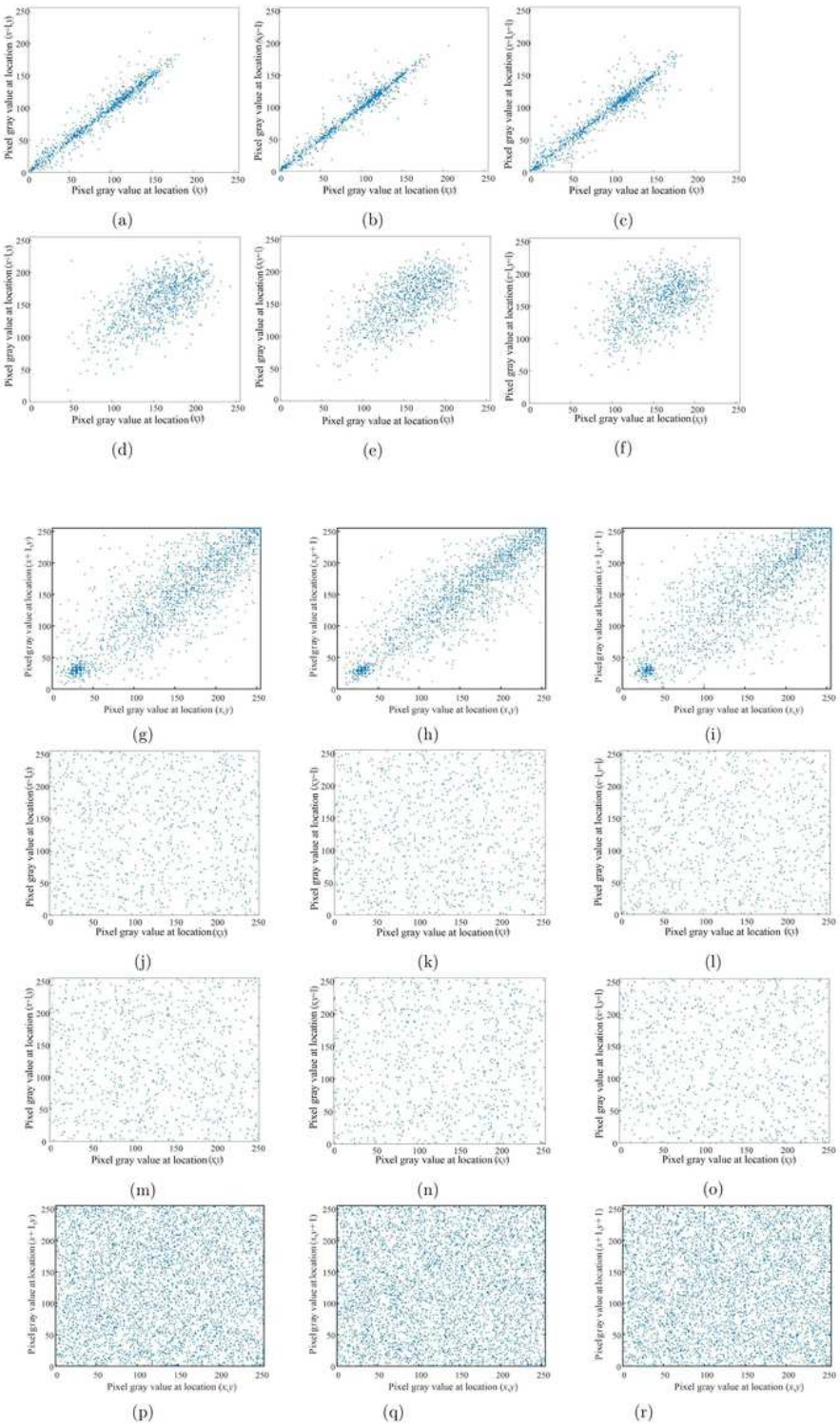


Figure 13

Please see the Manuscript PDF file for the complete figure caption

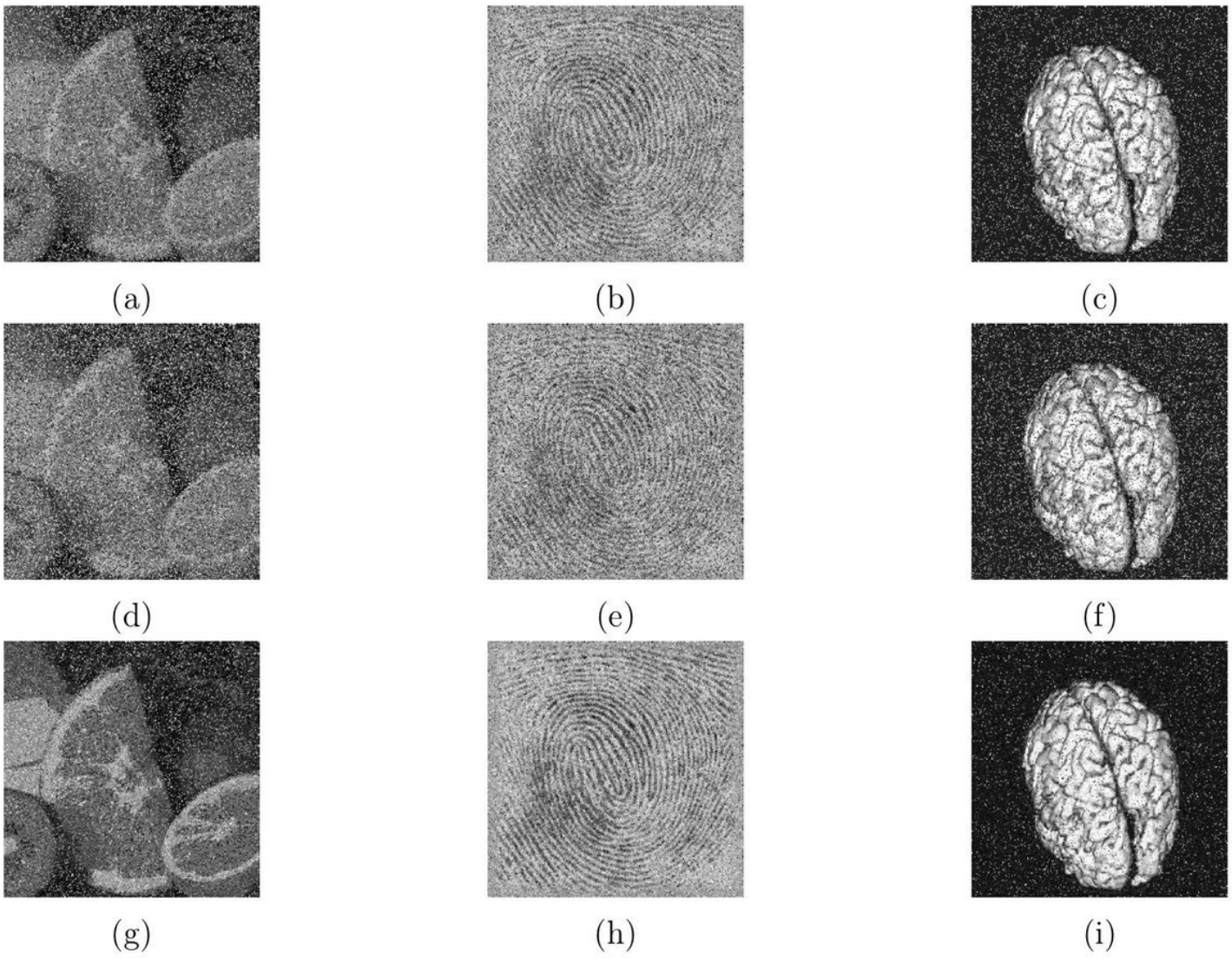


Figure 14

Please see the Manuscript PDF file for the complete figure caption

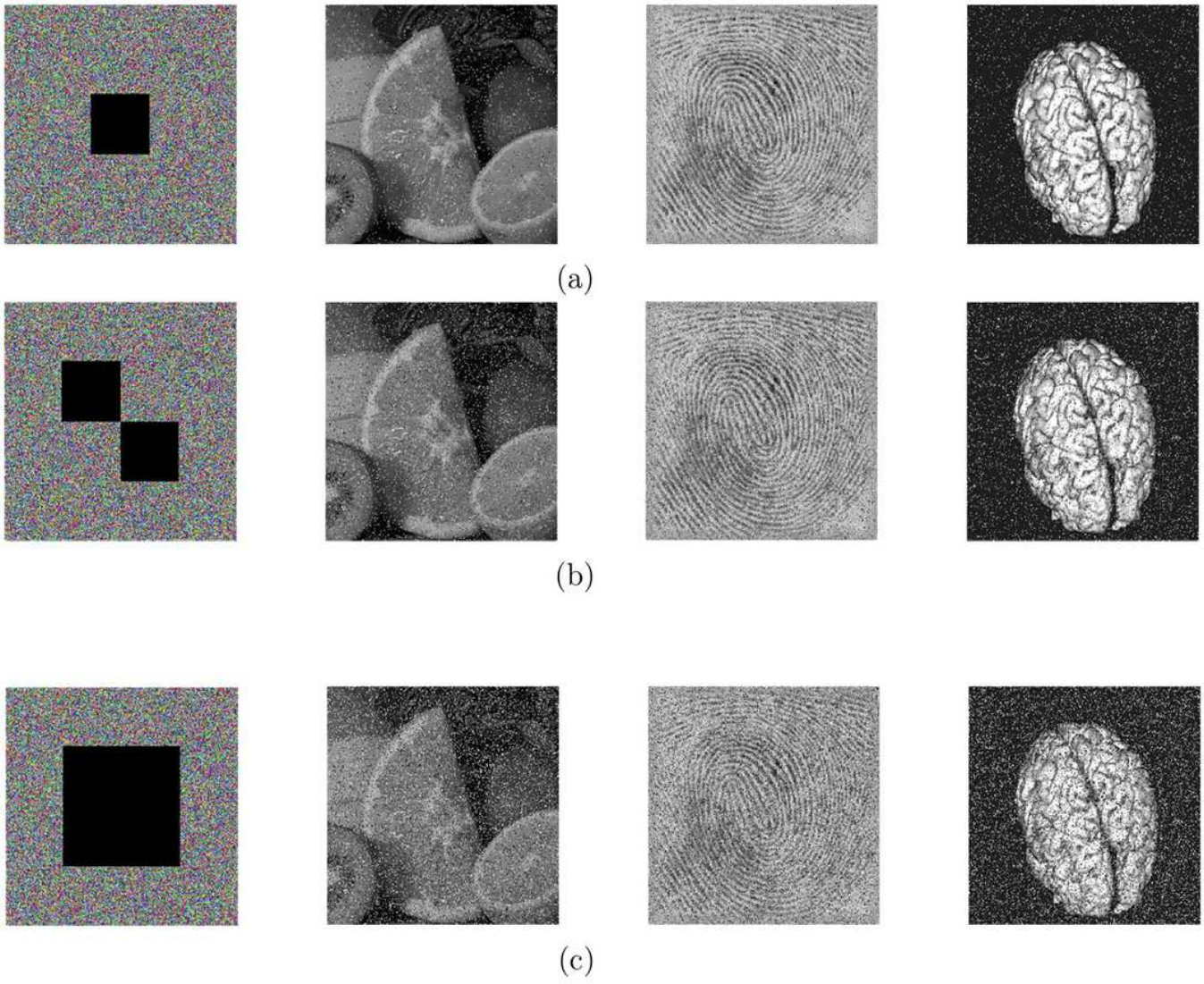


Figure 15

Please see the Manuscript PDF file for the complete figure caption