

Research Article

Chaos-Based Application of a Novel Multistable 5D Memristive Hyperchaotic System with Coexisting Multiple Attractors

Fei Yu ¹, Li Liu ¹, Shuai Qian,¹ Lixiang Li ¹, Yuanyuan Huang ¹, Changqiong Shi ¹, Shuo Cai ¹, Xianming Wu ², Sichun Du ³, and Qiuzhen Wan ⁴

¹School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China

²School of Mechanical and Electrical Engineering, Guizhou Normal University, Guiyang 550025, China

³College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

⁴College of Information Science and Engineering, Hunan Normal University, Changsha 410081, China

Correspondence should be addressed to Fei Yu; yufeyfyf@csust.edu.cn, Yuanyuan Huang; snailhyy@126.com, and Qiuzhen Wan; wanzhiuzhen@sina.com

Received 23 November 2019; Revised 8 February 2020; Accepted 17 February 2020; Published 29 March 2020

Guest Editor: Sundarapandian Vaidyanathan

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

Novel memristive hyperchaotic system designs and their engineering applications have received considerable critical attention. In this paper, a novel multistable 5D memristive hyperchaotic system and its application are introduced. The interesting aspect of this chaotic system is that it has different types of coexisting attractors, chaos, hyperchaos, periods, and limit cycles. First, a novel 5D memristive hyperchaotic system is proposed by introducing a flux-controlled memristor with quadratic nonlinearity into an existing 4D four-wing chaotic system as a feedback term. Then, the phase portraits, Lyapunov exponential spectrum, bifurcation diagram, and spectral entropy are used to analyze the basic dynamics of the 5D memristive hyperchaotic system. For a specific set of parameters, we find an unusual metastability, which shows the transition from chaotic to periodic (period-2 and period-3) dynamics. Moreover, its circuit implementation is also proposed. By using the chaoticity of the novel hyperchaotic system, we have developed a random number generator (RNG) for practical image encryption applications. Furthermore, security analyses are carried out with the RNG and image encryption designs.

1. Introduction

In recent years, chaos systems have become the subject of many studies in the fields of science and engineering. A large number of new chaotic systems have been proposed one after another, and their application scopes are more and more extensive [1–8]. With the progress of science and technology, chaos has been applied not only to communication [9–12], image processing [13–15], complex networks [16–21], synchronization [22–27], electronic circuits [28–30], and optimization [31–35] but also to encryption studies [36–41]. This is because chaotic signal has good pseudorandom, initial-value sensitive, and long-term unpredictable characteristics, which enhances the confusion and diffusion of encrypted data.

Due to the more complex structure and dynamic behavior of the hyperchaotic system, in order to better meet the needs

of secure communication and information hiding, people propose to construct hyperchaotic systems to improve the complexity of the systems. At present, hyperchaotic systems are usually constructed by loading feedback controller on 3D or 4D continuous chaotic systems [42–46]. The feedback controllers are divided into linear and nonlinear, among which the nonlinear-feedback term will further increase the complexity and unpredictability of the system, which is more suitable for the construction of hyperchaos [47–51].

Memristor is a kind of hardware implementation component of memory nonlinear electronic memristor chaotic circuit, which has research significance in chaotic secure communication, image encryption, neural networks, and other fields [52–56]. It describes the relationship between magnetic flux and charge. The concept of the memristor was proposed by Chua in 1971 [57], and it was not until 2008 that

HP laboratory realized the first real memristor [58]. Because of the nonlinear and memory characteristics of the memristor, as the feedback term of the hyperchaotic system, it can produce complex nonlinear dynamic phenomena, which provides a new development space for the design of the hyperchaotic system. At present, the main method is to use the memristor as the feedback term in typical chaotic systems to construct hyperchaotic systems. In [59], a novel 5D hyperchaotic four-wing memristive system (HFWMS) was proposed by introducing a flux-controlled memristor with quadratic nonlinearity into a 4D hyperchaotic system, the dynamic characteristics of the HFWMS were analyzed, and the FPGA realization of the 5D HFWMS was also reported. In [60], a new memristive system was presented by replacing the resistor in the circuit of modified Lü system with the flux-controlled memristor, respectively, which could exhibit a hyperchaotic multiwing attractor, and the values of two positive Lyapunov exponents were relatively large. The dynamical behaviors and the circuit implementation were also carried out.

Coexisting attractors depend on the symmetry of the systems and the initial condition of the systems [61]. Multistability refers to the phenomenon that the system shows different dynamic characteristics and different attractors coexist under same parameters [62]. In recent years, the study of multistability and coexistence attractors is a hot topic in nonlinear dynamics [63–70]. Lai et al. [63] showed the coexistence behavior of different attractors under different initial conditions and parameter values, such as four limit cycles, and two double-scroll attractors with a limit cycle. In [65], a new 4D fractional order chaotic system was proposed by adding a variable to the 3D chaotic system. This new system had no equilibrium point, but it could also show rich and complex hidden dynamics. Zhang et al. [66] introduced a state variable into a 3D chaotic system and then analyzed the dynamic characteristics of the new system under different initial conditions, proving that the new system has extreme multistability. In fact, various systems exhibiting multistability have been proposed. However, a review of literature revealed that this remarkable behavior is rare in 5D memristive hyperchaotic system with coexisting multiple attractors. Such systems cannot be ignored. Because of their complexity, the generated signals are usually used for secure communication and random number generation.

With the development of communication technology and the coming of information age, people are more and more aware of the important role of information security [71–76], and the research of various security protection has become the current research hotspot [77–82]. As an important part of information security transmission, random number generator (RNG) has been paid more and more attention. The unpredictable and unrepeatable random number sequence which can be produced by RNG plays an important role in information encryption. Based on Shannon information theory, in order to ensure the absolute security of communication, the RNG with high speed, unpredictability, and good randomness has great research value [83–89]. The chaotic system is a kind of complex nonlinear motion, which is highly sensitive to the initial

conditions, and its orbit is unpredictable for a long time. Therefore, the chaotic system shows very good cryptography characteristics.

In recent years, people are committed to the research and design of chaos-based RNGs [90–93]. Sometimes the key of generating random sequence by chaos is the choice of chaotic systems. However, most RNGs based on chaos have a typical disadvantage. That is to say, the limited precision of all processors may cause the chaotic system to degenerate into periodic function or fixed point [94]. In order to overcome this disadvantage, a generator based on hyperchaos was proposed in [94]. The self-shrinking generator was used to disturb the hyperchaotic sequence to reduce the period degradation and improve the sequence performance, which was superior to many other linear-feedback-shift register-based generators. Random numbers created in the chaotic systems are tested according to the randomness tests with the highest international standards such as AIS-31 and NIST 800 22 and then are ready to be used in encryption applications [95, 96]. In encrypted applications, it is not enough to encrypt data only. Encrypted data must also be equipped with the highest possible reliability. In order to prove the high level of reliability, some security analysis must be carried out according to the data type. Key space, sensitivity, floating frequency, histograms, correlation, and information entropy analysis are common security analysis in the literature [97–99].

Motivated by undiscovered features of systems with coexisting multiple attractors, we introduce a novel multistable 5D memristive hyperchaotic system with a line of equilibrium and its practical chaos-based application in the present work. The rest of this work is organized as follows. Section 2 describes the mathematical model of the novel multistable 5D memristive hyperchaotic system. Dynamical properties and circuit realization of the system are investigated in Sections 3 and 4, respectively. Section 5 presents a random number generation (RNG) using the chaoticity of the multistable 5D memristive hyperchaotic system, while security analyses are also carried out with the RNG designed. To validate the performance of the RNG, the application of image encryption is employed in Section 6, we also employ standard security analysis whose outcome is compared alongside available state-of-the-art methods. Finally, we conclude in Section 7.

2. A Novel Multistable 5D Memristive Hyperchaotic System

Recently, Yu and Wang [100] proposed a 4D four-wing chaotic system, and its mathematical model is

$$\begin{cases} \dot{x} = -ax + yz, \\ \dot{y} = by - xz, \\ \dot{z} = xy - cz + dw, \\ \dot{w} = xy - ew, \end{cases} \quad (1)$$

where x, y, z , and w are the state variables and a, b, c, d , and e are the system parameters. When $a = 10, b = 12, c = 60, d = 2,$

and $e = 3$, system (1) can display a fully four-wing chaotic attractor under the initial conditions $(2, 1, 1, 2)$.

Memristor is a passive two terminal device which describes the relationship between flux φ and charge q . In this paper, the memristor is controlled by flux, and the relationship between the current flowing through the two terminal device and the port voltage can be expressed as follows:

$$i = W(\varphi)u, \dot{\varphi} = u, \quad (2)$$

where $W(\varphi)$ is the memductance function of the flux-controlled memristor and defined as

$$W(\varphi) = f + 3g\varphi^2. \quad (3)$$

Based on system (1), by introducing the memristor model in (3) to the third equation of system (1), a novel 5D memristive hyperchaotic system is presented as follows:

$$\begin{cases} \dot{x} = -ax + yz, \\ \dot{y} = by - xz, \\ \dot{z} = xy - cz + dw(f + 3gu^2), \\ \dot{w} = xy - ew, \\ \dot{u} = -z, \end{cases} \quad (4)$$

where a, b, c, d, e, f , and g are the system parameters. When the typical parameters are fixed as $a = 10, b = 12, c = 30, d = 2, e = 4, m = 0.1$, and $n = 0.01$ and the initial conditions are chosen as $(2, 1, 1, 2, 2)$, the memristive system (4) exhibits a four-wing hyperchaotic attractor, as shown in Figure 1, from which it can be seen that the system has topologically more complex attractor structure than system (1) presented by [100]. The memristive chaotic system (4) has the same symmetry as the original 4D chaotic system (1) and remains unchanged under the coordinate transformation $(x, y, z, w, u) \rightarrow (\pm x, \mp y, -z, -w, -u)$.

Equilibrium points of system (4) are obtained by setting its right-hand side to zero, that is,

$$\begin{cases} -ax + yz = 0, \\ by - xz = 0, \\ xy - cz + dw(f + 3gu^2) = 0, \\ xy - ew = 0, \\ -z = 0. \end{cases} \quad (5)$$

According to equation (5), it is easy to see that system (4) has a line equilibrium point $O = \{(x, y, z, w, u) \mid x = y = z = w = 0, u = l\}$, where l is any real constant. The Jacobian matrix at the online equilibrium point O of system (4) is

$$J_o = \begin{bmatrix} -a & z & y & 0 & 0 \\ -z & b & -x & 0 & 0 \\ y & x & -c & d(f + 3gu^2) & 6dwgu \\ y & x & 0 & -e & 0 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix}. \quad (6)$$

According to (6), the characteristic equation can be obtained as

$$\lambda(\lambda + e)(\lambda + c)(\lambda + a)(\lambda - b) = 0. \quad (7)$$

It is easy to get $\lambda_1 = 0, \lambda_2 = -e, \lambda_3 = -a, \lambda_4 = -c$, and $\lambda_5 = b$ because the values of system parameters a, b, c , and e are greater than zero, so λ_2, λ_3 , and λ_4 are negative, λ_5 is positive, so system (4) has unstable saddle point. The dissipativity of memristive chaotic system (4) can be described as

$$\nabla V = \frac{dx}{dx} + \frac{dy}{dy} + \frac{dz}{dz} + \frac{dw}{dw} + \frac{du}{du} = -a + b - c - e. \quad (8)$$

Since $-a + b - c - e = -32$ satisfies $\nabla V < 0$, system (4) is dissipative.

3. Dynamic Analysis of the Novel 5D Memristive Chaotic System

In this section, we will use the tools of bifurcation diagram, Lyapunov exponent spectrum, time series, and phase diagram and use the fourth-order Runge–Kutta algorithm to study the complex dynamic behavior of system (4) through MATLAB. The proposed memristive chaotic system (4) has particularly complex dynamic characteristics, including coexistence attractors of the same type and different types, multistability, and transient transfer phenomena.

3.1. Lyapunov Exponent Spectrum and Bifurcation Diagram.

It is very interesting that there are different dynamic behaviors (such as periodic phenomena, quasi-periodic, chaotic attractors, and hyperchaotic attractors), according to different differential equations of parameter values. The system parameters are set as $b = 12, c = 30, d = 2, e = 4, m = 0.1$, and $n = 0.01$, the initial conditions are chosen as $x(0) = 2, y(0) = 1, z(0) = 1, w(0) = 2$, and $u(0) = 2$, and the parameter a is the bifurcation parameter of the system. Figure 2(a) is the corresponding Lyapunov exponent spectrum (in order to make the graph display clear, the fifth Lyapunov index is omitted here), and Figure 2(b) is the bifurcation diagram when the parameter a of the system changes from 0 to 20 with the state variable x . It can be seen from Figure 2(b) that as the parameter a gradually increases in the range, the system leads from periodic state to chaos and then to period, with some quasi-periodic windows and transient transfer phenomena in the middle. Table 1 lists the dynamic behavior of parameter a in different ranges and its Lyapunov exponent. Therefore, it can be shown that system (4) has a very rich and complex dynamic behavior:

- (i) When $0 \leq a \leq 1.6$, the maximum Lyapunov exponent of system (4) is zero ($\lambda_1 = 0, \lambda_{2,3,4,5} < 0$), so the system is in a multiperiod state.
- (ii) When $1.6 \leq a < 2.2, 5.8 < a < 11.5$, and $12.4 < a < 13.1$, the system has a positive Lyapunov exponent ($\lambda_1 > 0, \lambda_2 = 0, \lambda_{3,4,5} < 0$) and is in a chaotic state.

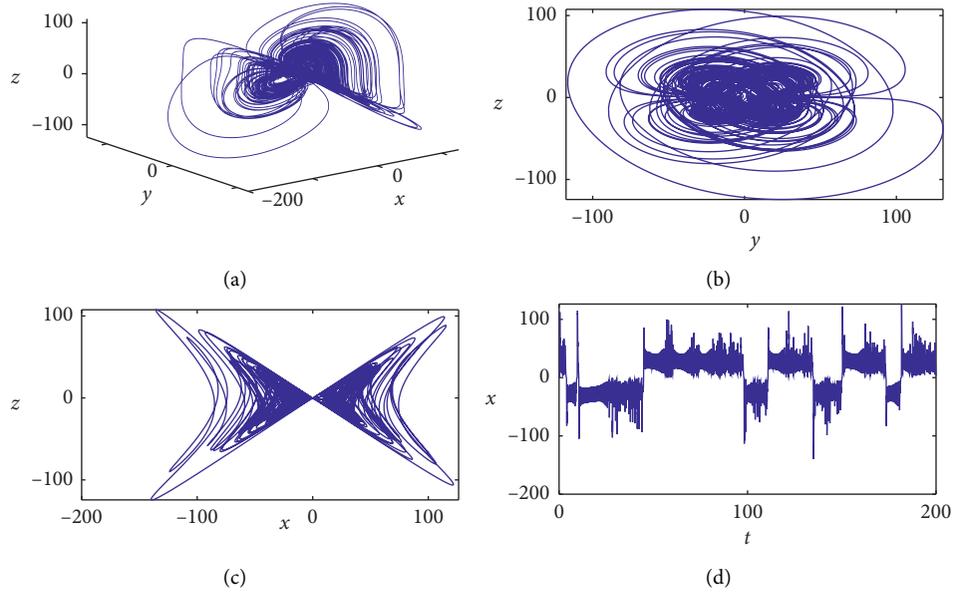


FIGURE 1: The four-wing chaotic attractor of system (4): (a) in the $x - y - z$ plane, (b) in the $y - z$ plane, (c) in the $x - z$ plane, and (d) time-domain waveform of x .

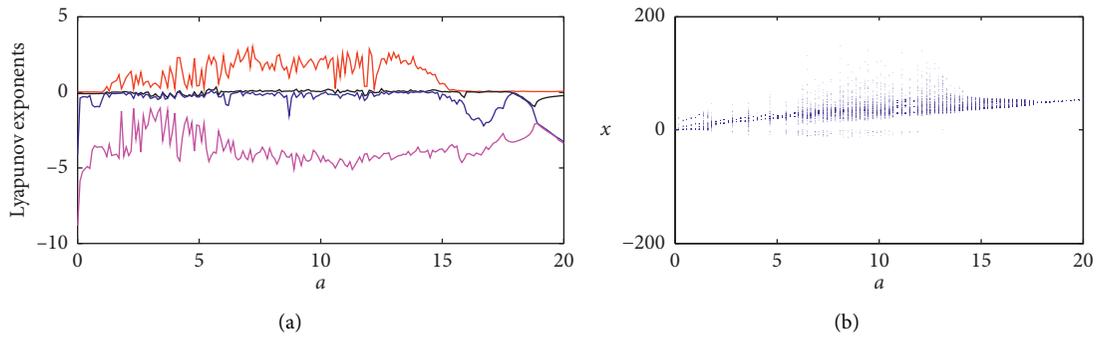


FIGURE 2: (a) Lyapunov exponent spectrum (the fifth LE is out of plot) and (b) bifurcation diagram for increasing parameter $a \in [0, 20]$.

TABLE 1: Dynamical behavior and Lyapunov exponents under different parameter ranges of a .

a	$(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5)$	Behavior of dynamics
$0 \leq a \leq 1.6$	$(0, -, -, -, -)$	Multiperiod
$1.6 \leq a < 2.2$	$(+, 0, -, -, -)$	Chaotic attractor
$2.2 \leq a \leq 5.8$	$(0, -, -, -, -)$	Transient chaos, stable state period-2
$5.8 < a < 11.5$	$(+, 0, -, -, -)$	Chaotic attractor
$11.5 \leq a \leq 12.4$	$(0, -, -, -, -)$	Transient chaos, stable state period-3
$12.4 < a < 13.1$	$(+, 0, -, -, -)$	Chaotic attractor
$13.1 \leq a \leq 14.8$	$(+, +, 0, -, -)$	Hyperchaotic attractor
$14.8 < a \leq 17.9$	$(0, 0, -, -, -)$	Quasi-periodic state
$17.9 < a \leq 20$	$(0, -, -, -, -)$	Limit cycle

(iii) When $3.1 \leq a \leq 14.8$, system (4) has two positive Lyapunov exponents ($\lambda_{1,2} > 0, \lambda_3 = 0, \lambda_{4,5} < 0$), so the system is hyperchaotic.

(iv) When $14.8 < a \leq 17.9$, the Lyapunov exponent of the system has two zeros ($\lambda_{1,2} = 0, \lambda_{3,4,5} < 0$), and the system is quasi-periodic.

(v) When $17.9 < a \leq 20$, the maximum Lyapunov exponent of system (4) is zero ($\lambda_1 = 0, \lambda_{2,3,4,5} < 0$), which is different from that of the system in the multiperiod state ($0 \leq a \leq 1.6$), but the parameter a is only in the limit cycle state in this range.

- (vi) When $2.2 \leq a \leq 5.8$ and $11.5 \leq a \leq 12.4$, the most interesting and also very important is the existence of transient chaos and steady-state periodic phenomena. Firstly, the system has a positive Lyapunov exponent, but when it reaches a certain time range, the maximum Lyapunov exponent becomes zero.

3.2. Multistability in the 5D Memristive Chaotic System.

In order to study the coexistence attractors and other characteristics of the system better, it is necessary to give some disturbance to the initial conditions under the condition of keeping the system parameters constant. Figure 3 shows the dynamic behavior with coexistence bifurcation, in which the initial conditions of blue trajectory and red trajectory are $(2, 1, 1, 2, 2)$ and $(-2, -1, 1, 2, 2)$, respectively. It can be seen from Figure 3 that, under these two initial conditions, the bifurcation mode of the system is almost the same, so the system has exactly the same coexistence attractor under these two conditions. Table 2 is a summary of the dynamic characteristics of different parameter values a . Figure 4 shows coexisting multiple attractors of system (4) for different parameter values a . Figure 4(a) shows that the system has the coexisting two-wing period-1 attractors for $a = 1$; Figure 4(b) shows that the system has two-wing chaotic attractors coexisting when $a = 2$; Figure 4(c) shows that the phenomenon is very rare, the system has transient chaos, and then transfers to stable state of period-2 for $a = 3.2$. When $a = 8$, Figure 4(d) is very similar to the two-wing chaotic attractors, as shown in Figure 4(b); The system has four-wing chaotic attractors coexisting for $a = 10.1$ (see Figure 4(e)). It is very similar to the phenomenon in Figure 4(c), but it is different that Figure 4(f) has the coexistence of stable state of period-3 for $a = 11.7$. It is different from the previous two kinds of two-wing chaotic attractors; when $a = 14.6$, the system has the coexisting two-wing hyperchaotic attractors, as shown in Figure 4(g). Figure 4(h) shows that when $a = 17$, the system has coexistence quasi-periodic phenomenon. Figure 4(i) shows that when $a = 18.2$, the system has coexistence limit cycle with period-1 under two different initial conditions.

If a chaotic system has different states of coexistence attractors under different initial conditions, the system has better randomness and is more suitable for random number generation, image encryption, secure communication, and other fields. As shown in Figure 5, system (4) has coexistence of various types of attractors under the initial conditions $(2, 1, 1, 2, 2)$ and $(-2, 1, 1, 2, 2)$, such as two-wing multiperiod and two-wing period-5 coexist (Figure 5(a)), different two-wing chaotic attractors coexist (Figure 5(b)), periodic-2 and two-wing chaotic attractors coexist (Figures 5(c) and 5(d)), two-wing chaotic attractors coexist with quasi-period (Figure 5(e)), and two-wing chaotic attractors coexist with four-wing chaotic attractors (Figure 5(f)).

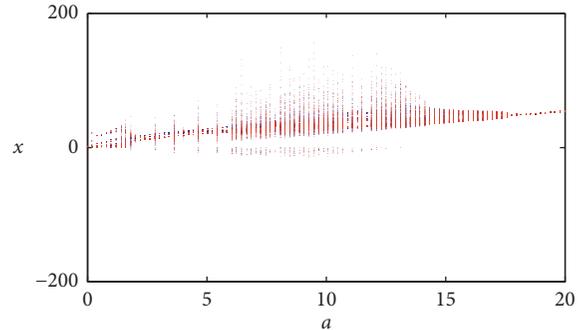


FIGURE 3: Bifurcation diagram with different initial values, the blue is $(2, 1, 1, 2, 2)$ and the red is $(-2, -1, 1, 2, 2)$.

TABLE 2: Dynamical behavior under different parameter of a when $b = 12$, $c = 30$, $d = 2$, $e = 4$, $m = 0.1$, and $n = 0.01$.

a	Dynamics	Figure
1.0	Limit cycle with period-1	Figure 4(a)
2.0	Two-wing chaotic attractor	Figure 4(b)
3.2	Stable state period-2	Figure 4(c)
8.0	Two-wing chaotic attractor	Figure 4(d)
10.1	Four-wing chaotic attractor	Figure 4(e)
11.7	Stable state period-3	Figure 4(f)
14.6	Hyperchaotic attractor	Figure 4(g)
17.0	Quasi-periodic	Figure 4(h)
18.2	Limit cycle with period-1	Figure 4(i)

3.3. Transient Chaos. Due to the appearance of nonattractive saddle point in phase space, chaos appears in the system in a limited period of time. After a period of time, the system finally becomes a nonchaotic state, which is called transient chaos. In practice, transient chaos is more common than permanent chaos. A close observation of Figure 2 shows that, in the interval ranges $[2.2, 5.8] \cup [11.5, 12.4]$ of system parameter a , a periodic window appears in Figure 2(b), but Figure 2(a) does indicate that the system is in a chaotic state in this range. This dynamic behavior with two different characteristics is called transient transfer behavior. With the evolution of time, system (4) changes from chaotic behavior to periodic behavior.

When $a = 3$, the time-domain waveform in the time interval $[0, 200]$ is shown in Figure 6(a), and Figures 6(b)–6(e) are the phase portraits of the system in x - z plane in different time intervals. It is clear from Figure 6(a) that the system is chaotic in $t \in [0, 40]$ and periodic in $t \in [40, 200]$. From Figures 6(b)–6(e), it is verified that the system evolves from chaos to period gradually with time. Figure 7 also proves that the system does have transient chaos. Different from Figure 6, with the evolution of time, Figure 6 finally becomes a stable state period-2, while Figure 7 tends to a stable state period-3. The above-mentioned two cases show that the nonlinear phenomenon from transient chaos to stable state period is not a sudden phenomenon, and it needs a process like chaos bifurcation. For example, when $t \in [0, 40]$ in Figure 6 is at a chaotic state but it is not just a stable state periodic

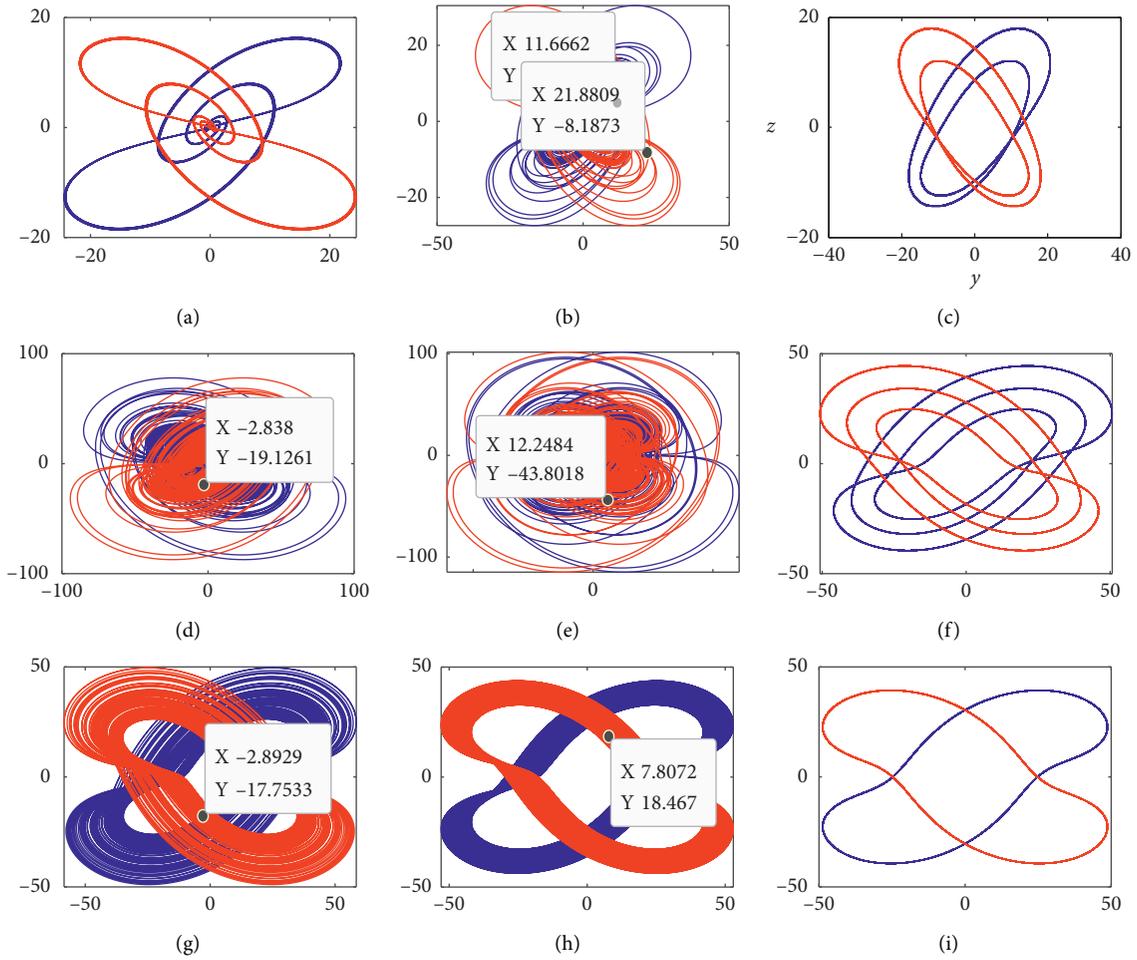


FIGURE 4: Various coexisting hidden attractors with different values of parameter a in the y - z plane: (a) $a = 1.0$, (b) $a = 2.0$, (c) $a = 3.2$, (d) $a = 8.0$, (e) $a = 10.1$, (f) $a = 11.7$, (g) $a = 14.6$, (h) $a = 17.0$, and (i) $a = 18.2$. The blue one from the initial values $(2, 1, 1, 2, 2)$ and the other from $(-2, -1, 1, 2, 2)$.

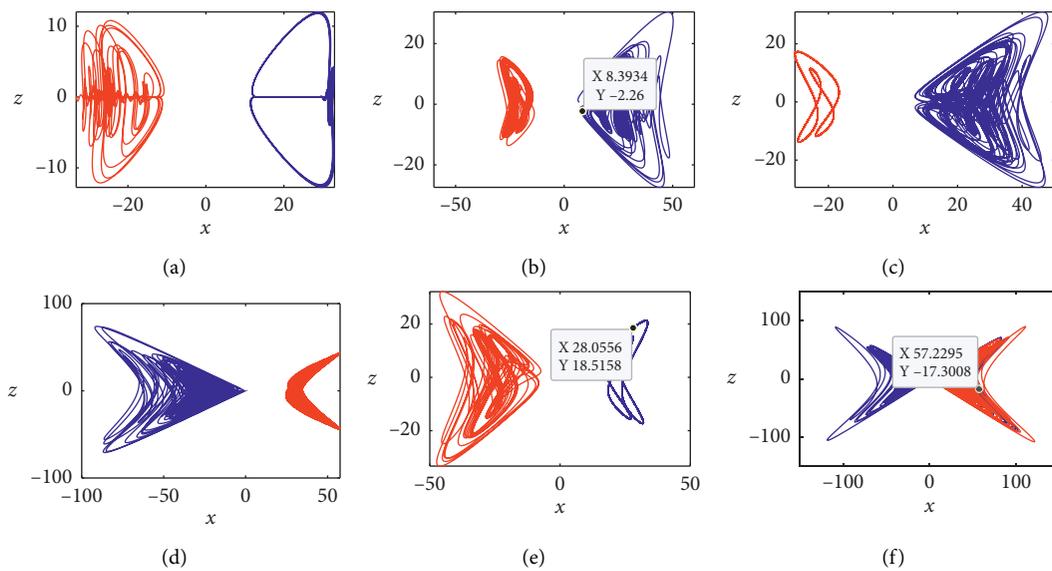


FIGURE 5: Various coexisting hidden attractors with different values of parameter a in the x - z plane: (a) $a = 0.2$, (b) $a = 2.0$, (c) $a = 3.0$, (d) $a = 4.2$, (e) $a = 6.75$, and (f) $a = 13.1$. The blue one from the initial values $(2, 1, 1, 2, 2)$ and the other from $(-2, 1, 1, 2, 2)$.

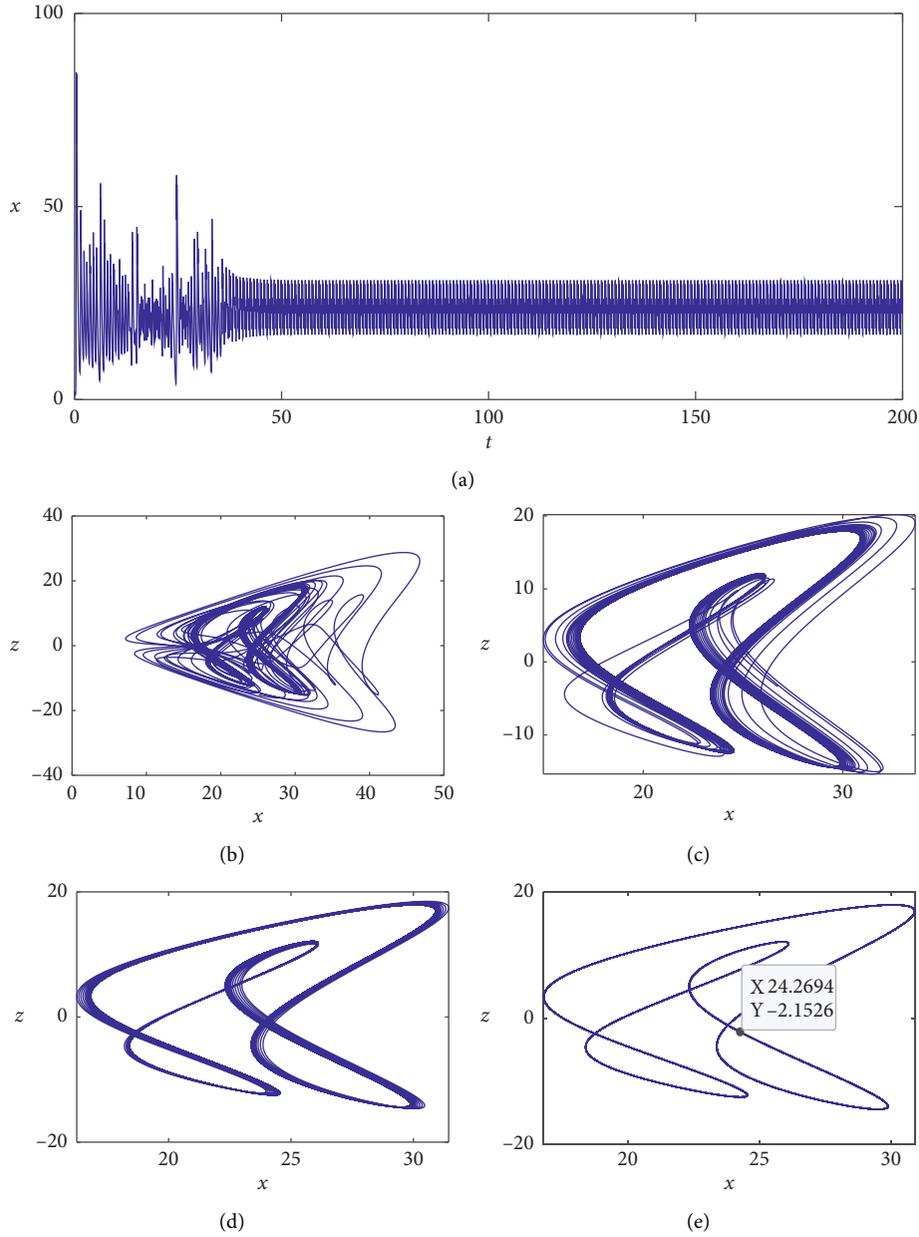


FIGURE 6: Transient chaos, steady-state period-2. (a) Time-domain waveform of x in the time interval $[0, 200]$, (b) phase portrait of the chaotic attractor in the x - z , (c) chaotic attractor, (d) phase portrait of multiperiod, and (e) steady-state period-2. Under the initial values $(2, 1, 1, 2, 2)$ and system parameter $a = 3.2$.

burning, the chaotic phase portraits will change from Figures 6(b)–6(e), which needs the same time interval (about $[0, 100]$) to completely change from chaos to period. Figures 6(b) and 6(c) are transient chaotic attractors, and Figures 6(d) and 6(e) are steady-state periodic states. Figure 6(a) is the time-domain waveform of state variable x , which is different from the time series generated by the general chaotic system. Before $t = 40$, the system is in chaotic state, and then it will slowly convert to periodic state.

4. Electronic Circuit Design

Using hardware circuit to realize the chaos mathematical model is a hot issue in practical application. The circuit design diagram of the 5D memristive hyperchaotic system (4) is shown in Figure 8. In the circuit design, LF347 is used as the operational amplifier, AD633JN is used as the multiplier chip, and the multiplication factor is $0.1/V$. The operating voltage of the operational amplifier is $\pm E = \pm 15$ V, and the actual saturation voltage

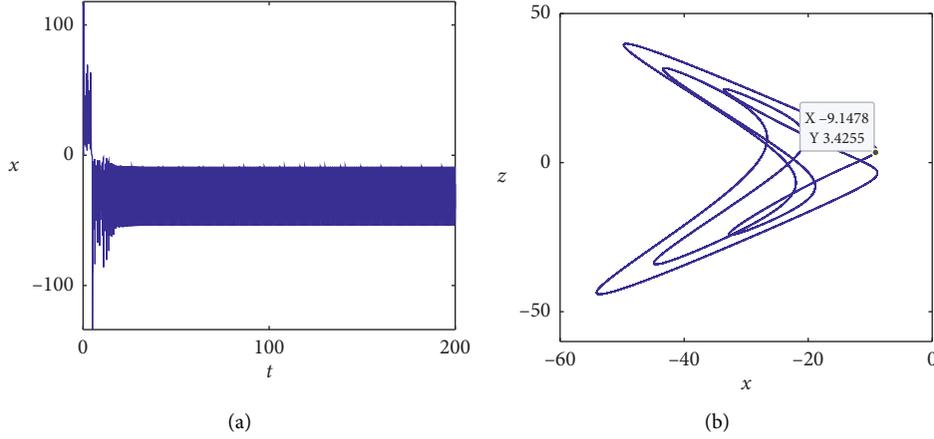


FIGURE 7: Transient chaos, stable state period-3. (a) Time-domain waveform of x in the time interval $[0, 200]$ and (b) stable state period-3, under the initial values $(2, 1, 1, 2, 2)$ and system parameter $a = 11.5$.

measured by the operational amplifier and multiplier is $\pm|V_{\text{sat}}| \approx \pm 13.5 \text{ V}$. Since the variables in the phase portraits shown in Figure 1 are beyond the linear dynamic range, we must scale the system, and the relevant circuit equations are as follows:

$$\begin{cases} \dot{v}_x = -\frac{1}{R_1 C_x} v_x + \frac{1}{10 \cdot R_2 C_x} v_y v_z, \\ \dot{v}_y = \frac{1}{R_3 C_y} v_y - \frac{1}{10 \cdot R_4 C_y} v_x v_z, \\ \dot{v}_z = \frac{1}{10 \cdot R_5 C_z} v_x v_y - \frac{1}{R_6 C_z} v_z - \frac{1}{C_z} \left(\frac{R v_w}{R_{11}} + \frac{R}{100 R_{12}} v_u^2 v_w \right), \\ \dot{v}_w = \frac{1}{10 \cdot R_8 C_w} v_x v_y - \frac{1}{R_9 C_w} v_w, \\ \dot{v}_u = \frac{1}{R_{10} C_u} v_z, \end{cases} \quad (9)$$

where $R_1 = R/a$, $R_3 = R/b$, $R_6 = R/c$, $R_9 = R/e$, $R_{11} = R/dm$, and $R_{12} = R/(100 \cdot 3dn)$. According to the parameters given in system (4), $b = 12$, $c = 30$, $d = 2$, $e = 4$, $m = 0.1$, and $n = 0.01$, we set $C_x = C_y = C_z = C_w = C_u = C = 10 \text{ nF}$, $R = 100 \text{ k}\Omega$, $R_2 = R_4 = R_5 = R_8 = 10 \text{ k}\Omega$, $R_3 = 8.25 \text{ k}\Omega$, $R_6 = 3.32 \text{ k}\Omega$, $R_9 = 25 \text{ k}\Omega$, $R_{11} = 500 \text{ k}\Omega$, and $R_{12} = 16.5 \text{ k}\Omega$. Figure 9 shows the phase portraits which are obtained by Multisim simulator. Compared with the MATLAB simulation Figure 4, it can be clearly seen that the phase portraits of Figure 9 and system (4) in initial condition $(2, 1, 1, 2, 2)$ are exactly the same, which confirm the correctness of the proposed 5D memristive hyperchaotic system (4).

5. RNG Design with the Novel Multistable 5D Memristive Hyperchaotic System

5.1. The Design of RNG. Random numbers are widely used in image encryption, information security, computer, and other fields, so the research on RNGs is particularly

important. Because the chaotic system has high sensitivity and strong complexity to parameters and initial conditions, random numbers generated by using the chaotic system as an entropy source of RNG have strong randomness. Algorithm 1 is a pseudocode for designing a RNG. As shown in Algorithm 1, (1) the initial conditions of the chaotic system, step value Δh , and sampling interval are given; (2) the fourth-order Runge–Kutta algorithm (RK4) is used to solve the differential equation of the chaotic system to obtain the 32 bit output of the chaotic system, in which 0–21 bit are used for the design of the RNG; (3) XOR the output 22 bit x , y , z , and w , respectively, to improve the randomness; (4) the abovementioned two steps to obtain the test bit stream are combined

In order to better evaluate the performance of generating random numbers of chaotic systems, NIST 800.22 with international high standard is used for random test. NIST 800.22 includes 15 test methods: frequency test, run test, overlapping templates test, linear complexity test, etc. The 22 bit sequence generated from the chaotic system must be large enough for RNG test. If the p value_T of NIST 800.22 is more than 0.0001, it shows that the p value_T is uniformly distributed and the sequence is random. NIST test is carried out with 130 sample sequences of 1M bit length generated by the chaotic random number generator. The test results are shown in Table 3. All p value_T are greater than the threshold value of 0.0001, so RNG passed the test. The lowest pass rate for each statistical test is about 0.975.

5.2. Security Analyses

5.2.1. Key Space Analysis. The main purpose of designing a random number sequence generator is encryption, and the size of key space determines the ability to withstand exhaustive attack. The larger the key space, the better the encryption effect. In order to ensure the security of encryption, the key space should be greater than 2^{128} . In this paper, the proposed multistable 5D memristive hyperchaotic system is used to construct a RNG, which can effectively increase the size of the key space. Five 16 bit keys are used to

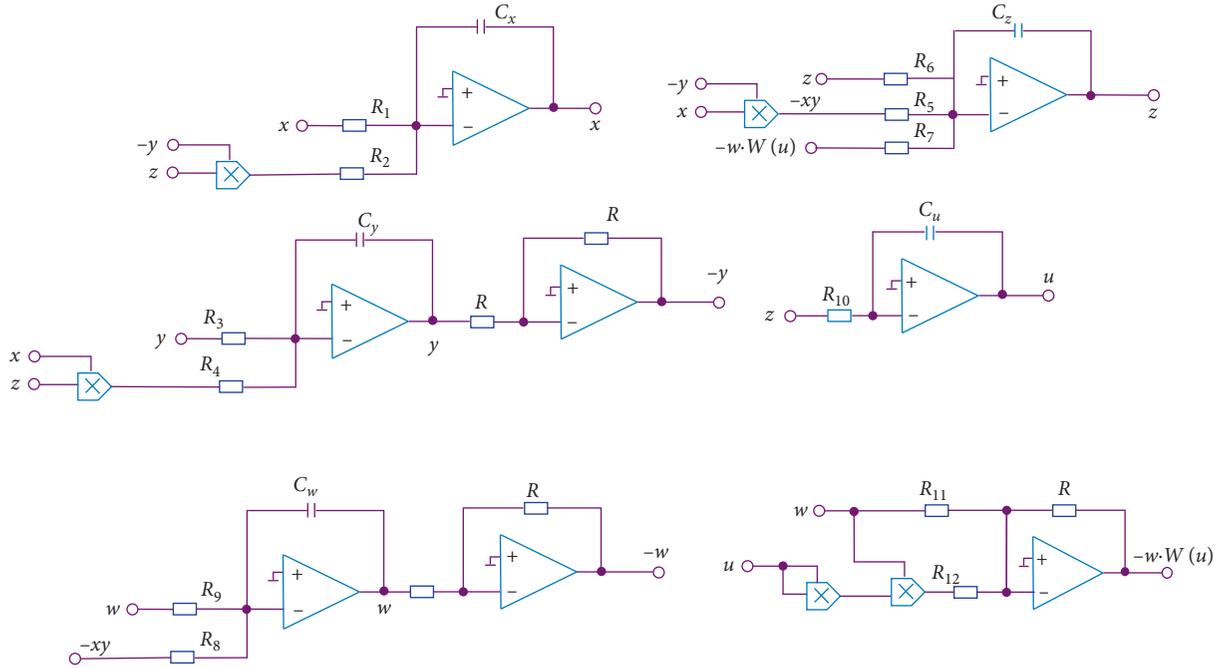


FIGURE 8: Circuit diagram of memristive chaotic system (4).

set the initial conditions $(x_0, y_0, z_0, w_0, u_0)$ of the hyperchaotic system, and seven 16 bit keys are used to set the parameters $a, b, c, d, e, f,$ and g of the hyperchaotic system. There are 192 bit keys in total, so the key space of this paper is $2^{192} > 2^{128}$, so the method used in this paper can effectively resist exhaustive attack.

5.2.2. Key Sensitivity Analysis. The chaos system is very sensitive to the initial value, so the random numbers generated by the chaotic system have good randomness. Generally, we make small changes to the initial value, and then judge the initial value sensitivity of the RNG by the bit change rate of two sequences. The closer the bit change rate is to 50%, the more sensitive it is to the initial value. Given $x(0) = 2$, $x(0)' = 2.00000001$, $a = 10$, and $a' = 10.00000001$ and the length of random number sequence is 10120000 bits, the change rate of bit with initial value is shown in Table 4. It can be seen that when the random sequence changes only 10^{-8} , the system's bit change rate is close to 50%, so the random sequence generator is very sensitive to the initial value of the 5D hyperchaotic system. Figure 10 is a time-domain waveform obtained by 50 iterations of the abovementioned two initial values. Figures 10(a) and 10(b) are time-domain oscillograms when the parameter value a and initial condition x change, respectively. The blue line represents the sequence generated when the system parameter value remains unchanged, and the red line represents the sequence generated by iteration when the initial value changes. As shown in Figure 10, when $t \in [0, 8]$, the sequence curves of two different initial values coincide completely. After $t = 8$, the sequence curves of different initial values begin to separate, and the difference is more obvious with the increase of time. All the above

show that the RNG is very sensitive to the initial value and small initial value changes will have a great impact on the sequence.

5.2.3. Correlation Analysis. Correlation is another important measure of randomness. For an ideal random number sequence, the autocorrelation function is δ . The cross-correlation function is 0. Figure 11 is the correlation graph of two random sequences generated by the RNG, given the initial conditions $x(0) = 2$ and $x(0)' = 2.00000001$. Figure 11(a) is the autocorrelation graph of the sequence, and Figure 11(b) is the crosscorrelation graph of the sequence. From these two figures, it can be seen that the random sequence generated by the RNG based on the 5D hyperchaotic system has strong randomness. In order to further verify the key sensitivity of the generated random number, two similar equal length sequences are generated by the RNG through small changes in the initial value of the system, and the correlation coefficient is used for testing. Correlation coefficient can measure the statistical relationship between sequences. If the correlation coefficient is zero, then there is no correlation between the two sequences. If it is ± 1 , then there is a strong correlation between the two sequences. In the experiment, one initial condition of the 5D chaotic system (4) changes 10^{-8} , all system parameters remain unchanged, and two groups of random sequences with a length of 4048000 bits are generated. The correlation value is calculated by MATLAB, and Table 5 is obtained. It can be noted that the correlation values obtained by changing the five initial conditions are very close to zero, so there is almost no correlation between the two sequences. This shows that the random number produced in this paper is very sensitive to the initial value.

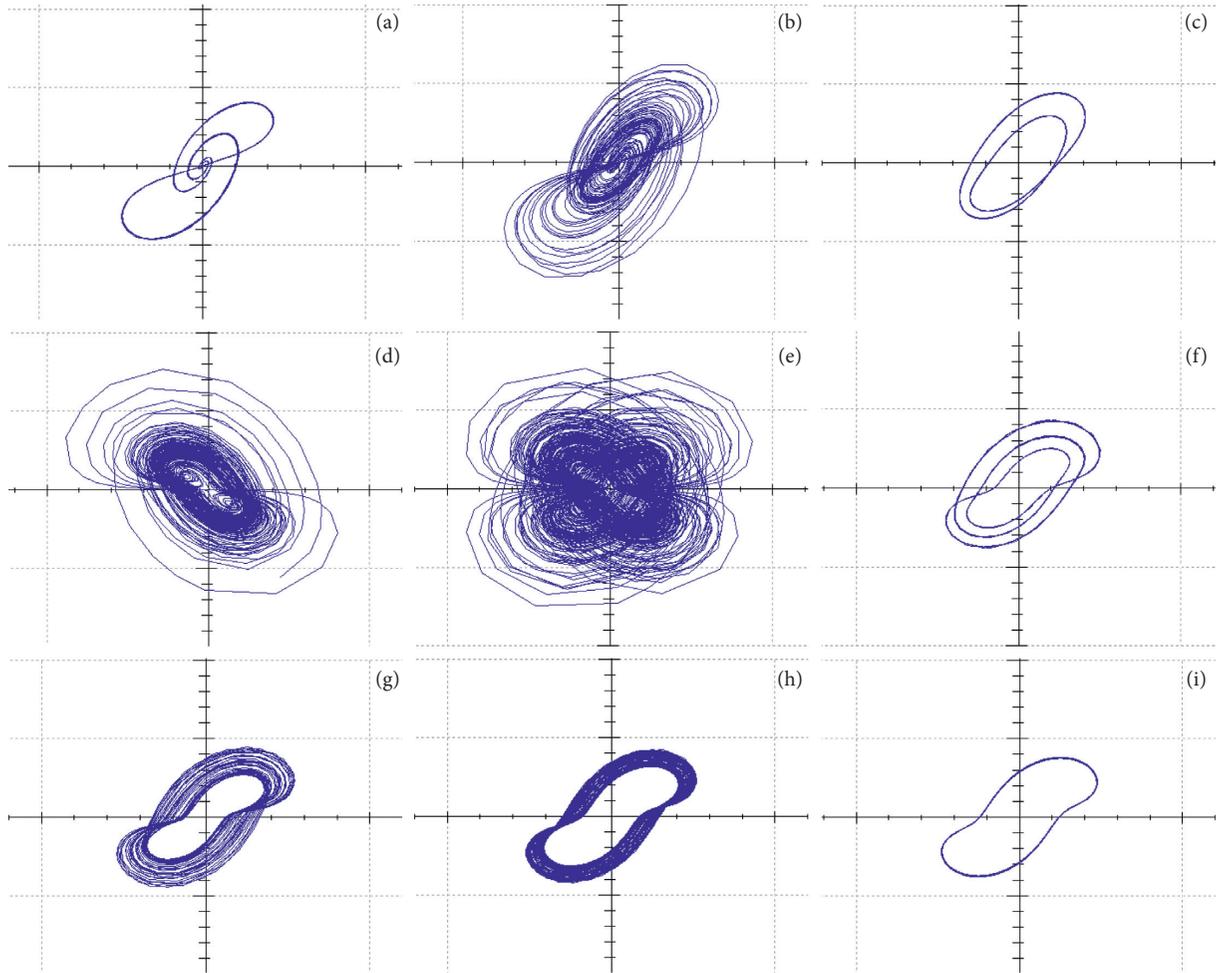


FIGURE 9: Various attractors with different values of resistance R_1 in the y - z plane observed from multisim simulation: (a) $R_1 = 100 \text{ k}\Omega$, (b) $R_1 = 50 \text{ k}\Omega$, (c) $R_1 = 31.6 \text{ k}\Omega$, (d) $R_1 = 12.5 \text{ k}\Omega$, (e) $R_1 = 10 \text{ k}\Omega$, (f) $R_1 = 8.5 \text{ k}\Omega$, (g) $R_1 = 6.81 \text{ k}\Omega$, (h) $R_1 = 6.0 \text{ k}\Omega$, and (i) $R_1 = 5.5 \text{ k}\Omega$.

```

(1) start
(2) Given the initial condition, parameter value, step value  $\Delta h$  and sampling interval of chaotic system (4);
(3) while (least 100 M. Bit data) do
(4) Using RK4 algorithm to solve chaotic system (4), 32 bit  $x, y, z, w, u$  has obtained;
(5) Select the last 22 bit number of 32 bit  $x, y, z,$  and  $w$ ;
(6) Obtain the bit stream of the chaotic system (4) by XOR  $x$  and  $y, z,$  and  $w$ ;
(7) Get test bit stream according to 5 and 6;
(8) end while
(9) End

```

ALGORITHM 1: RNG design algorithm pseudocode.

6. Image Encryption

With the rapid development of computer technology, image information acquisition, processing, transmission, and other related technologies have been rapidly developed and applied and have been widely studied by scholars [101–110]. Among them, image encryption plays an increasingly important role in the fields of information security, military, medicine, and meteorology and has become a hot issue of social concern. Chaotic systems show good randomness

because of their strong initial value and parameter sensitivity, and they are widely used in the field of image encryption [111–120]. In this section, as a typical application, we will use the random number generated by the proposed RNG for image encryption.

Suppose the size of the original image is $m \times n$, where m and n are the number of rows and columns of the image pixel matrix, respectively, and the pixel gray value is an integer between 0 and 255. The specific operation steps of encrypting image with random number are as follows:

TABLE 3: The results of RNG NIST 800.22 tests.

NIST statistical test	p value $_T$	Proportion	Result
Frequency (monobit) test	0.037157	0.975	Successful
Block frequency test	0.706149	0.983	Successful
Cumulative sums test	0.287306/0.204076	0.983/0.983	Successful
Runs test	0.602458	0.983	Successful
Longest-run test	0.074177	1	Successful
Binary matrix rank test	0.422034	0.983	Successful
Discrete fourier transform test	0.392456	1	Successful
Nonoverlapping templates test	0.605808	0.9875	Successful
Overlapping templates test	0.804337	1	Successful
Maurer's universal statistical test	0.602458	0.975	Successful
Approximate entropy test	0.195163	0.9917	Successful
Random excursions test	0.407530	0.9844	Successful
Random excursions variant	0.455004	0.9861	Successful
Serial test 1	0.551026	0.975	Successful
Serial test 2	0.637119	1	Successful
Linear complexity test	0.985035	1	Successful

TABLE 4: Initial value sensitivity analysis of random sequences.

Initial value	Amount of change	Changed number of bits	p (%)
$x(0)$	10^{-8}	5060283	50.0028
a	10^{-8}	5059553	49.9956

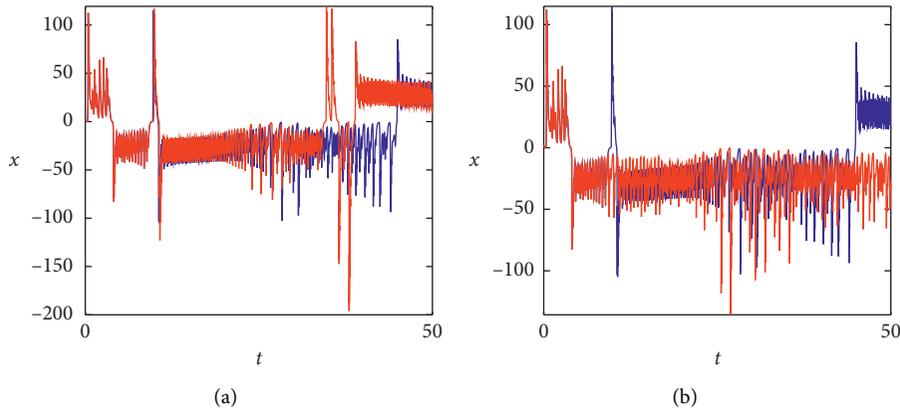


FIGURE 10: Time-domain waveform of x in the time interval $[0, 50]$. (a) parameters $a = 10$ and $a' = 10.00000001$ and (b) initial values $x(0) = 2$ and $x(0)' = 2.00000001$.

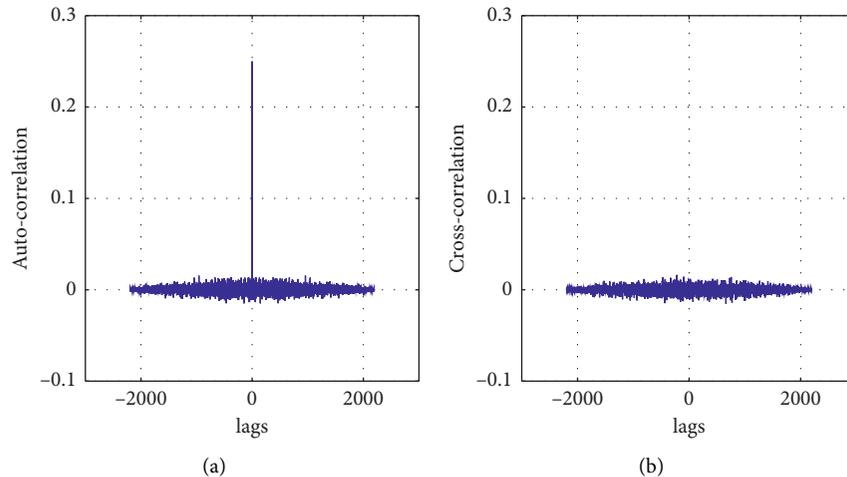


FIGURE 11: Correlation of random sequences: (a) autocorrelation and (b) crosscorrelation.

TABLE 5: Correlation value of random sequence.

Initial conditions	Amount of change	Changed value	Correlation value
$x(0) = 2$	10^{-8}	$x(0)' = 2.00000001$	0.00066917
$y(0) = 1$	10^{-8}	$x(0)' = 1.00000001$	-0.00047467
$z(0) = 1$	10^{-8}	$x(0)' = 1.00000001$	0.0017
$w(0) = 2$	10^{-8}	$x(0)' = 2.00000001$	0.00071957
$u(0) = 2$	10^{-8}	$x(0)' = 2.00000001$	-0.00069381

Step 1: using the proposed multistable 5D memristive hyperchaotic system, the random sequence is generated iteratively according to the given system parameters and initial conditions.

Step 2: transform the pixels in the image into a one-dimensional sequence I with a length of $m \times n$ in the order of traversal hierarchy.

Step 3: ensure the randomness of the sequence and discard the previous n iterations. Continue the iteration to generate the binary sequence of $m \times n \times 8$ bits. Then, we convert every 8 bits of binary sequence into an integer, ranging from 0 to 255. Finally, we get an integer sequence of length $m \times n$: $i = 1, 2, \dots, M \times N$.

Step 4: use the random sequence generated by the system to scramble all the pixel values in one-dimensional sequence I to get the scrambled sequence I' .

Step 5: store the generated image as the final encrypted image.

Decryption is the reverse of encryption.

6.1. Simulation Results. In this paper, the Lena image with the size of 256×256 is used as the encrypted plain image (note that the same photo is used in all subsequent safety analysis comparisons with other references), and the keys are $a = 10$, $b = 12$, $c = 30$, $d = 2$, $e = 4$, $m = 0.1$, and $n = 0.01$ and $(x_1(0), x_2(0), x_3(0), x_4(0), x_5(0)) = (2, 1, 1, 2, 2)$. The results of encryption and decryption of Lena images are shown in Figure 12, where Figure 12(a) is the original plain image, Figure 12(b) is the encrypted image, and Figure 12(c) is the decrypted image successfully decrypted using the key. It can be seen that the encrypted image does not have the characteristics of the original plain image, and the decrypted image is exactly the same as the original plain image.

6.2. Security Analyses

6.2.1. Histogram Analysis. Histogram is used to display the distribution characteristics of pixels. In the encryption algorithm, changing the distribution characteristics is very important. If the probability of all intensity pixels generated is equal in the histogram of the encrypted image, the encryption has a high degree of symmetry and good uniformity. Figures 13(a) and 13(b), respectively, represent the histogram of the plain image and the encrypted image. It can be seen that the original plain image has obvious statistical characteristics, while the probability of each gray value of the

encrypted image is almost equal. Therefore, encrypted images can effectively resist statistical analysis attacks.

6.2.2. Correlation Analysis. There is usually a strong correlation between adjacent pixels in an image, so a good encryption algorithm should be able to produce cipher images with low correlation, so as to hide image information and resist statistical attacks. The correlation of adjacent pixels is determined by the following formula:

$$r_{x,y} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}}, \quad (10)$$

where

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i, \quad (11)$$

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

where $E(x)$ and $D(x)$ represent the expectation and variance of the variable x , and $r_{x,y}$ is the correlation coefficient of adjacent pixels x and y . Figure 14 shows the phase diagrams of Lena plain text image and cipher text image with adjacent pixel points in all directions upward (where (a) and (b) are horizontal directions, (c) and (d) are vertical directions, and (e) and (f) are diagonal directions). It can be seen from these figures that the adjacent pixel values of the plain image are located near the line with slope 1, indicating that the two adjacent pixels are highly correlated. The pixel values of the cipher image are scattered throughout the region, indicating a low correlation between the adjacent pixels. Table 6 shows the test values of correlation in three directions: horizontal, vertical, and diagonal. It can be seen that the adjacent pixels of the plain image have high correlation ($r_{x,y} \rightarrow 1$), and the adjacent pixels of the cipher image have low correlation ($r_{x,y} \rightarrow 0$). At the same time, compared with the corresponding results of References [111–114], it shows that the proposed encryption algorithm has lower correlation between adjacent pixels and can more effectively resist statistical attacks.

6.2.3. Information Entropy. Information entropy is an important index to reflect the randomness of information. The more uniform the distribution of pixel gray value, the greater the information entropy, the greater the randomness, and the higher the security. The calculation formula is as follows:

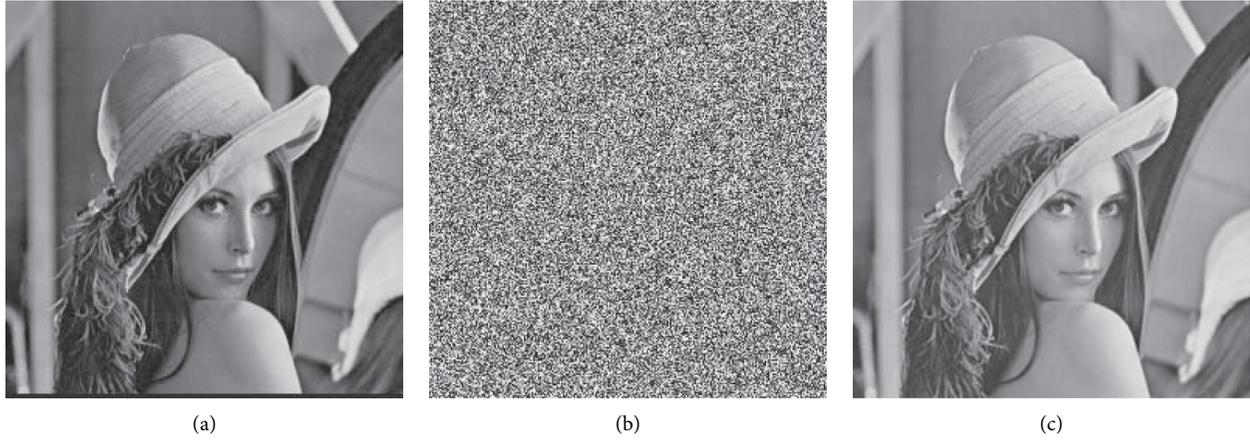


FIGURE 12: Image encryption and decryption. (a) Original plain image, (b) cipher image, and (c) decryption image.

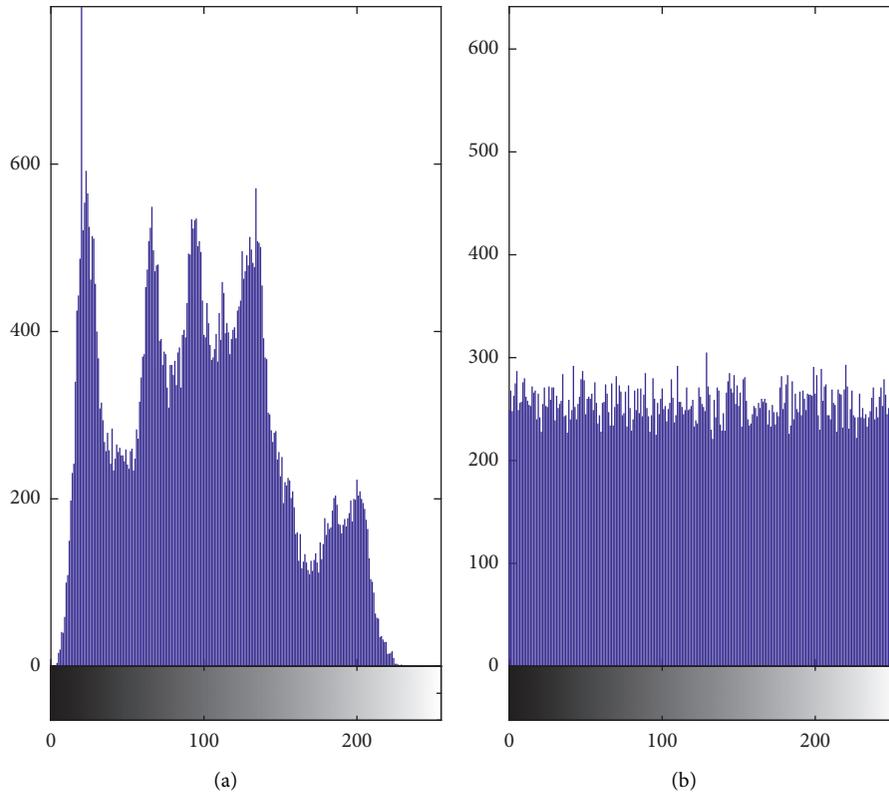


FIGURE 13: Histogram of (a) plain image and (b) cipher image.

$$H = \sum_{i=1}^{256} p_i \log_2 \frac{1}{p_i}, \quad (12)$$

where p_i is the probability of occurrence of pixel points with a pixel value of i . For grayscale images, the ideal value of information entropy is 8. As listed in Table 7, by comparing the information entropy of cipher and the cipher images in References [115–118], it can be concluded that the information entropy value of the encrypted images in the algorithm in this paper is closer to the ideal value 8, and the

encrypted images are closer to the random signal source, which can effectively resist the entropy attack.

6.2.4. Differential Attack. Pixels change rate (Number of Pixels Change Rate, NPCR) and normalized pixels flat change strong degree (Unified Average Changing Intensity, UACI) can be used to measure to express the sensitivity of the encryption algorithm, which is an important indicator of measuring algorithm ability to resist differential attack. NPCR and UACI, respectively, represent the proportion and

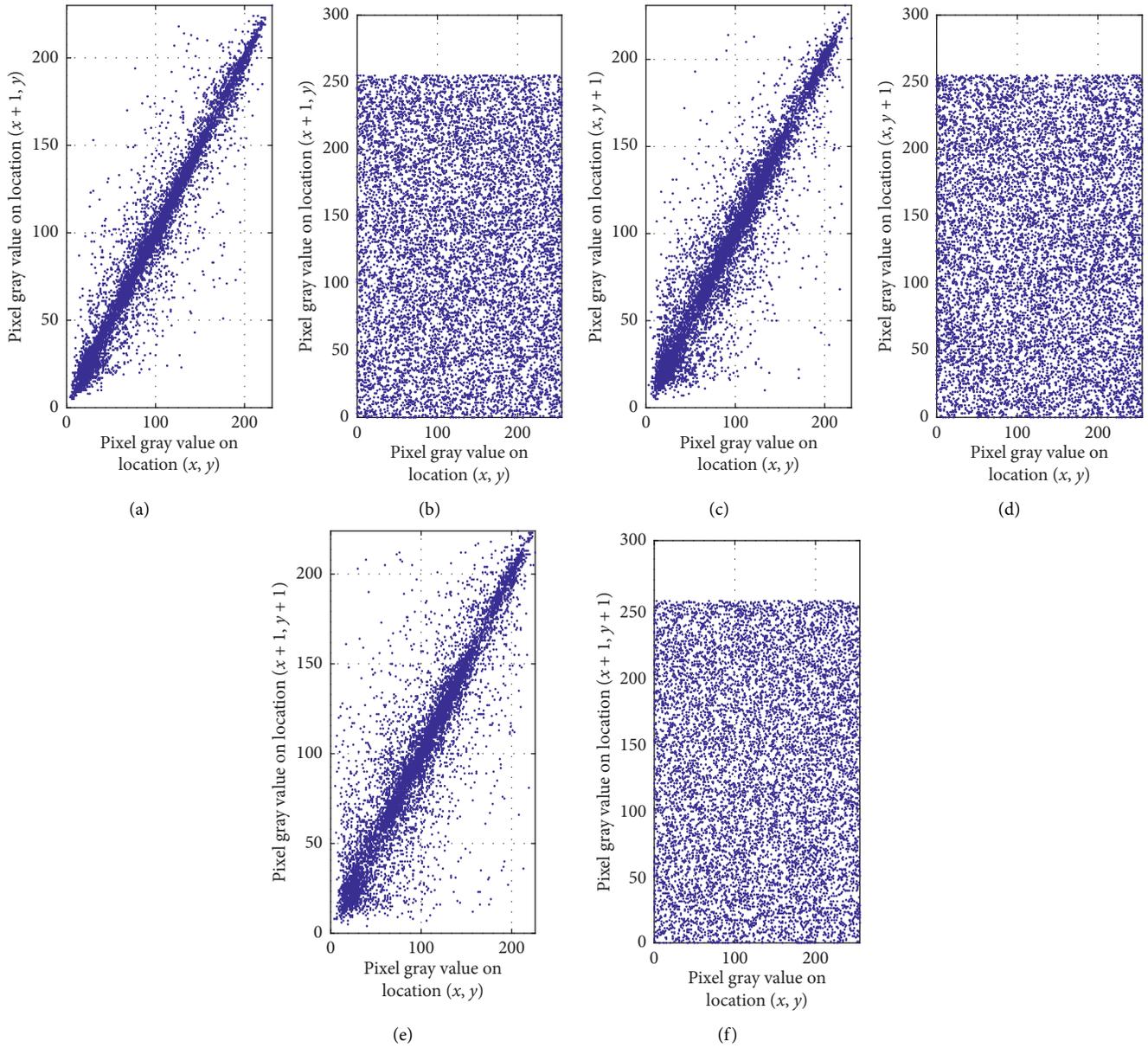


FIGURE 14: Correlation of two adjacent pixels of the plain image lena (256×256) and its cipher image. (a) Horizontal direction in plain image, (b) horizontal direction in cipher image, (c) vertical direction in plain image, (d) vertical direction in cipher image, (e) diagonal direction in plain image, and (f) diagonal direction in cipher image.

TABLE 6: Correlation coefficients of the plain and cipher images.

Image	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Ours	0.94505	0.96653	0.91917	0.00068299	-0.0007768	-0.0036362
Reference [111]	0.964227	0.982430	0.965609	-0.038118	-0.029142	0.002736
Reference [112]	0.812688	0.837959	0.782053	0.001251	-0.003543	0.001449
Reference [113]	0.91848	0.82921	0.80731	0.011899	0.018062	0.036784
Reference [114]	0.97165	0.98730	0.95440	0.00312	-0.00317	-0.00310

TABLE 7: The results of information entropy.

Image	Ours	Reference [115]	Reference [116]	Reference [117]	Reference [118]
Results	7.9974	7.9971	7.8232	7.9963	7.9951

TABLE 8: The results of NPCR and UACI compared to other state-of-the-art algorithms.

Image	Ours	Reference [111]	Reference [118]	Reference [119]	Reference [120]
NPCR	99.5956	99.6114	99.5511	99.57	99.58
UACI	33.4535	33.4523	33.3461	33.31	33.43

degree of change in the pixel value of the corresponding position. The larger the proportion and the higher the degree of change, the stronger the antiattack capability of the algorithm. The calculation formulas are as follows:

$$\left\{ \begin{array}{l} \text{NPCR} = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j)}{M \times N} \times 100\%, \\ D(i, j) = \begin{cases} c1, & P_1(i, j) \neq P_2(i, j), \\ 0, & \text{otherwise,} \end{cases} \\ \text{UACI} = \frac{1}{M \times N} \frac{\sum_{i=1}^M \sum_{j=1}^N (P_1(i, j) - P_2(i, j))}{255} \times 100\%, \end{array} \right. \quad (13)$$

where $M \times N$ is the size of the image, $P_1(i, j)$ and $P_2(i, j)$, respectively, represent the pixel values of the positions corresponding to the plain and cipher. When the NPCR and UACI of the image are close to the ideal values of 99.6094070% and 33.4635070%, the algorithm has good safety [112, 121]. As listed in Table 8, the algorithm in this paper is more sensitive to the plain than the NPCR and UACI values in References [111–120] can meet the security requirements and have a good ability to resist differential attacks.

7. Conclusion

In this study, a novel multistable 5D memristive hyperchaotic system with line equilibrium is first introduced. Dynamical analysis is performed in terms of phase portraits, Lyapunov exponential spectrum, bifurcation diagram, and spectral entropy. Several interesting properties such as multistability and transient chaos have been revealed by using classical nonlinear analysis tools. Then, an electronic circuit is designed, and its accuracy is verified by Multisim simulation. As the engineering application, a new chaos-based RNG is designed and internationally accepted NIST 800.22 random tests are run. Security analyses are carried out and they have proved that the design can be used in cryptography applications. Finally, a chaotic image encryption is proposed based on the random number sequences; security analyses show that the algorithm has good security and can resist common attacks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grants 61504013, 61702052, 61772087, 61741104, 61674054, and 61901169, Natural Science Foundation of Hunan Province under Grants 2019JJ50648, 2016jj2005, 2017JJ2049, and 2019JJ40190, Scientific Research Fund of Hunan Provincial Education Department under Grant 18A137, National Key Research and Development Project under Grant 2018YFE0111200, Guizhou Provincial Science and Technology Foundation under Grant [2018]1115, and Guizhou Province Science and Technology Plan Project under Grant [2018]5769.

References

- [1] F. Yu, C. H. Wang, J. W. Yin et al., "Novel four-dimensional autonomous chaotic system generating one-, two-, three- and four-wing attractors," *Chinese Physics B*, vol. 20, no. 11, Article ID 110505, 2011.
- [2] Q. Deng and C. Wang, "Multi-scroll hidden attractors with two stable equilibrium points," *Chaos*, vol. 29, no. 9, Article ID 093112, 2019.
- [3] X. Zhang, C. Wang, W. Yao, and H. Lin, "Chaotic system with bondorbital attractors," *Nonlinear Dynamics*, vol. 97, no. 4, pp. 2159–2174, 2019.
- [4] S. Çiçek, A. Ferikoğlu, and İ. Pehlivan, "A new 3D chaotic system: dynamical analysis, electronic circuit design, active control synchronization and chaotic masking communication application," *Optik*, vol. 127, no. 8, pp. 4024–4030, 2016.
- [5] F. Yu, L. Gao, K. Gu, B. Yin, Q. Wan, and Z. Zhou, "A fully qualified four-wing four-dimensional autonomous chaotic system and its synchronization," *Optik*, vol. 131, pp. 79–88, 2017.
- [6] M. Saleh, C. K. Volos, K. Sezgin et al., "A chaotic system with infinite number of equilibria located on an exponential curve and its chaos-based engineering application," *International Journal of Bifurcation and Chaos*, vol. 28, no. 9, Article ID 1850112, 2018.
- [7] F. Yu, P. Li, K. Gu, and B. Yin, "Research progress of multi-scroll chaotic oscillators based on current-mode devices," *Optik*, vol. 127, no. 13, pp. 5486–5490, 2016.

- [8] C. Wang, X. Liu, and H. Xia, "Multi-piecewise quadratic nonlinearity memristor and its $2N$ -scroll and $2N+1$ -scroll chaotic attractors system," *Chaos*, vol. 27, no. 3, Article ID 033114, 2017.
- [9] L. L. Zhou, F. Tan, and F. Yu, "A robust synchronization-based chaotic secure communication scheme with double-layered and multiple hybrid networks," *IEEE Systems Journal*, 2019.
- [10] L. Zhou and F. Tan, "A chaotic secure communication scheme based on synchronization of double-layered and multiple complex networks," *Nonlinear Dynamics*, vol. 96, no. 2, pp. 869–883, 2019.
- [11] F. Yu, Z. Zhang, L. Liu et al., "Secure communication scheme based on a new 5D multistable four-wing memristive hyperchaotic system with disturbance inputs," *Complexity*, vol. 2020, Article ID 5859273, 16 pages, 2020.
- [12] F. Yu, S. Qian, X. Chen et al., "A new 4D four-wing memristive hyperchaotic system: dynamical analysis, electronic circuit design, shape synchronization and secure communication," *International Journal of Bifurcation and Chaos*, 2020.
- [13] Q. Yin and C. H. Wang, "A new chaotic image encryption scheme using breadth-first search and dynamic diffusion," *International Journal of Bifurcation and Chaos*, vol. 28, no. 4, Article ID 1850047, 2018.
- [14] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm," *Optics and Lasers in Engineering*, vol. 128, Article ID 105995, 2020.
- [15] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *International Journal of Bifurcation and Chaos*, vol. 29, no. 9, Article ID 1950115, 2019.
- [16] F. Yu, L. Liu, L. Xiao, K. Li, and S. Cai, "A robust and fixed-time zeroing neural dynamics for computing time-variant nonlinear equation using a novel nonlinear activation function," *Neurocomputing*, vol. 350, pp. 108–116, 2019.
- [17] L. Zhou, F. Tan, F. Yu, and W. Liu, "Cluster synchronization of two-layer nonlinearly coupled multiplex networks with multi-links and time-delays," *Neurocomputing*, vol. 359, pp. 264–275, 2019.
- [18] W. Yao, C. Wang, J. Cao, Y. Sun, and C. Zhou, "Hybrid multisynchronization of coupled multistable memristive neural networks with time delays," *Neurocomputing*, vol. 363, pp. 281–294, 2019.
- [19] J. Jin, L. Zhao, M. Li, F. Yu, and Z. Xi, "Improved zeroing neural networks for finite time solving nonlinear equations," *Neural Computing and Applications*, 2019.
- [20] F. Tan, L. Zhou, F. Yu, and J. Lu, "Fixed-time continuous stochastic synchronisation of two-layer dynamical networks," *International Journal of Systems Science*, vol. 51, no. 2, pp. 242–257, 2020.
- [21] H. Lin and C. Wang, "Influences of electromagnetic radiation distribution on chaotic dynamics of a neural network," *Applied Mathematics and Computation*, vol. 369, Article ID 124840, 2020.
- [22] X. Yang, Q. Zhu, and C. Huang, "Lag stochastic synchronization of chaotic mixed time-delayed neural networks with uncertain parameters or perturbations," *Neurocomputing*, vol. 74, no. 10, pp. 1617–1625, 2017.
- [23] Y.-Y. Huang, Y.-H. Wang, and Y. Zhang, "Shape synchronization of drive-response for a class of two-dimensional chaotic systems via continuous controllers," *Nonlinear Dynamics*, vol. 78, no. 4, pp. 2331–2340, 2014.
- [24] F. Yu and Y. Song, "Complete switched generalized function projective synchronization of a class of hyperchaotic systems with unknown parameters and disturbance inputs," *Journal of Dynamic Systems, Measurement, and Control-Transactions of the ASME*, vol. 136, no. 1, Article ID 014505, 2014.
- [25] Y. Huang, Y. Wang, H. Chen, and S. Zhang, "Shape synchronization control for three-dimensional chaotic systems," *Chaos, Solitons & Fractals*, vol. 87, pp. 136–145, 2016.
- [26] F. Yu, C. Wang, Q. Wan, and Y. Hu, "Complete switched chaotic function projective synchronization of a five-term chaotic system with uncertain parameters and disturbances," *Pramana*, vol. 80, no. 2, pp. 223–235, 2013.
- [27] F. Yu, C. H. Wang, Y. Hu, and J. W. Yin, "Anti-synchronization of a novel hyperchaotic system with parameter mismatch and external disturbances," *Pramana*, vol. 79, no. 1, pp. 81–93, 2012.
- [28] X. Zhang and C. Wang, "A novel multi-attractor period multi-scroll chaotic integrated circuit based on CMOS wide adjustable CCCII," *IEEE Access*, vol. 7, no. 1, pp. 16336–16350, 2019.
- [29] J. Jie and L. V. Zhao, "Low voltage low power fully integrated chaos generator," *Journal of Circuits Systems & Computers*, vol. 27, no. 10, Article ID 1850155, 2018.
- [30] J. Jin, "Programmable multi-direction fully integrated chaotic oscillator," *Microelectronics Journal*, vol. 75, pp. 27–34, 2018.
- [31] M. Long, F. Peng, and Y. Zhu, "Identifying natural images and computer generated graphics based on binary similarity measures of PRNU," *Multimedia Tools and Applications*, vol. 78, no. 1, pp. 489–506, 2019.
- [32] Y.-S. Huang and Z.-Y. Wang, "Decentralized adaptive fuzzy control for a class of large-scale MIMO nonlinear systems with strong interconnection and its application to automated highway systems," *Information Sciences*, vol. 274, pp. 210–224, 2014.
- [33] Q. Xie, X. Wang, Z. Han, Y. Zuo, and M. Tang, "Immersion and invariance control of a class of nonlinear cascaded discrete systems," *Neurocomputing*, vol. 171, pp. 1661–1665, 2016.
- [34] Y.-S. Huang and M. Wu, "Robust decentralized direct adaptive output feedback fuzzy control for a class of large-scale nonaffine nonlinear systems," *Information Sciences*, vol. 181, no. 11, pp. 2392–2404, 2011.
- [35] F. Wang, L. Zhang, S. Zhou, and Y. Huang, "Neural network-based finite-time control of quantized stochastic nonlinear systems," *Neurocomputing*, vol. 362, pp. 195–202, 2019.
- [36] V. T. Pham, S. Vaidyanathan, E. Tlelo-Cuautle et al., "Memory circuit elements: complexity, complex systems, and applications," *Complexity*, vol. 2019, Article ID 4936123, 4 pages, 2019.
- [37] W. S. Sayed, A. G. Radwan, A. A. Rezk, and H. A. H. Fahmy, "Finite precision logistic map between computational efficiency and accuracy with encryption applications," *Complexity*, vol. 2017, Article ID 8692046, 21 pages, 2017.
- [38] Z. Xiong, S. Qu, and J. Luo, "Adaptive multi-switching synchronization of high-order memristor-based hyperchaotic system with unknown parameters and its application in secure communication," *Complexity*, vol. 2019, Article ID 3827201, 18 pages, 2019.
- [39] N. Nesa, T. Ghosh, and I. Banerjee, "Design of a chaos-based encryption scheme for sensor data using a novel logarithmic

- chaotic map,” *Journal of Information Security and Applications*, vol. 47, pp. 320–328, 2019.
- [40] R. Montero-Canela, E. Zambrano-Serrano, E. I. Tamariz-Flores, J. M. Muñoz-Pacheco, and R. Torrealba-Melendez, “Fractional chaos based-cryptosystem for generating encryption keys in Ad Hoc networks,” *Ad Hoc Networks*, vol. 97, Article ID 102005, 2020.
- [41] W. Wang, M. Si, Y. Pang et al., “An encryption algorithm based on combined chaos in body area networks,” *Computers & Electrical Engineering*, vol. 65, pp. 282–291, 2018.
- [42] C. Volos, J.-O. Maaita, S. Vaidyanathan, V.-T. Pham, I. Stouboulos, and I. Kyprianidis, “A novel four-dimensional hyperchaotic four-wing system with a saddle-focus equilibrium,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 64, no. 3, pp. 339–343, 2017.
- [43] X. Zhang and C. H. Wang, “Multiscroll hyperchaotic system with hidden attractors and its circuit implementation,” *International Journal of Bifurcation and Chaos*, vol. 29, no. 9, Article ID 1950117, 2019.
- [44] V.-T. Pham, S. Vaidyanathan, C. Volos, S. Jafari, and S. T. Kingni, “A no-equilibrium hyperchaotic system with a cubic nonlinear term,” *Optik*, vol. 127, no. 6, pp. 3259–3265, 2016.
- [45] P. Daltzis, S. Vaidyanathan, V. T. Pham, C. Volos, E. Nistazakis, and G. Tombras, “Hyperchaotic attractor in a novel hyperjerk system with two nonlinearities,” *Circuits, Systems, and Signal Processing*, vol. 37, no. 2, pp. 613–635, 2018.
- [46] V. T. Pham, F. Rahma, M. Frasca et al., “Dynamics and synchronization of a novel hyperchaotic system without equilibrium,” *International Journal of Bifurcation and Chaos*, vol. 24, no. 6, Article ID 1450087, 2014.
- [47] Z. Wan, C. Wang, X. Luo, Y. Lin, and T. Huang, “Generating variable number of wings from a novel four-dimensional hyperchaotic system with one equilibrium,” *Optik*, vol. 125, no. 3, pp. 1371–1376, 2014.
- [48] L. Zhou, C. Wang, and L. Zhou, “A novel no-equilibrium hyperchaotic multi-wing system via introducing memristor,” *International Journal of Circuit Theory and Applications*, vol. 46, no. 1, pp. 84–98, 2018.
- [49] J. Jin and L. Cui, “Fully integrated memristor and its application on the scroll-controllable hyperchaotic system,” *Complexity*, vol. 2019, Article ID 4106398, 8 pages, 2019.
- [50] L. Xiong, Z. Liu, and X. Zhang, “Dynamical analysis, synchronization, circuit design, and secure communication of a novel hyperchaotic system,” *Complexity*, vol. 2017, Article ID 4962739, 23 pages, 2017.
- [51] A. Lassoued and O. Boubaker, “Dynamic analysis and circuit design of a novel hyperchaotic system with fractional-order terms,” *Complexity*, vol. 2017, Article ID 3273408, 10 pages, 2017.
- [52] Q. Zhao, C. H. Wang, and X. Zhang, “A universal emulator for memristor, memcapacitor, and meminductor and its chaotic circuit,” *Chaos*, vol. 29, no. 1, Article ID 013141, 2019.
- [53] M. E. Sahin, Z. G. Cam Taskiran, H. Guler, and S. E. Hamamci, “Simulation and implementation of memristive chaotic system and its application for communication systems,” *Sensors and Actuators A: Physical*, vol. 290, pp. 107–118, 2019.
- [54] G. Peng, F. Min, and E. Wang, “Circuit implementation, synchronization of multistability, and image encryption of a four-wing memristive chaotic system,” *Journal of Electrical and Computer Engineering*, vol. 2018, Article ID 8649294, 13 pages, 2018.
- [55] C. Wang, L. Xiong, J. Sun, and W. Yao, “Memristor-based neural networks with weight simultaneous perturbation training,” *Nonlinear Dynamics*, vol. 95, no. 4, pp. 2893–2906, 2018.
- [56] A. G. Radwan, A. T. Azar, S. Vaidyanathan, J. M. Muñoz-Pacheco, and A. Ouannas, “Fractional-order and memristive nonlinear systems: advances and applications,” *Complexity*, vol. 2017, Article ID 3760121, 2 pages, 2017.
- [57] L. Chua, “Memristor—the missing circuit element,” *IEEE Transactions on Circuit Theory*, vol. 18, no. 5, pp. 507–519, 1971.
- [58] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, “The missing memristor found,” *Nature*, vol. 453, no. 7191, pp. 80–83, 2008.
- [59] F. Yu, L. Liu, B. He et al., “Analysis and FPGA realization of a novel 5D hyperchaotic four-wing memristive system, active control synchronization and secure communication application,” *Complexity*, vol. 2019, Article ID 4047957, 18 pages, 2019.
- [60] L. Zhou, C. Wang, and L. Zhou, “Generating hyperchaotic multi-wing attractor in a 4D memristive circuit,” *Nonlinear Dynamics*, vol. 85, no. 4, pp. 2653–2663, 2016.
- [61] C. Li and J. C. Sprott, “Multistability in the Lorenz system: a broken butterfly,” *International Journal of Bifurcation and Chaos*, vol. 24, no. 10, Article ID 1450131, 2014.
- [62] C. Li and J. C. Sprott, “Finding coexisting attractors using amplitude control,” *Nonlinear Dynamics*, vol. 78, no. 3, pp. 2059–2064, 2014.
- [63] Q. Lai, A. Akgul, X. W. Zhao et al., “Various types of coexisting attractors in a new 4D autonomous chaotic system,” *International Journal of Bifurcation and Chaos*, vol. 27, no. 9, Article ID 1750142, 2017.
- [64] B. Bao, T. Jiang, Q. Xu, M. Chen, H. Wu, and Y. Hu, “Coexisting infinitely many attractors in active band-pass filter-based memristive circuit,” *Nonlinear Dynamics*, vol. 86, no. 3, pp. 1711–1723, 2016.
- [65] X. Zhang and Z. Li, “Hidden extreme multistability in a novel 4D fractional-order chaotic system,” *International Journal of Non-linear Mechanics*, vol. 111, pp. 14–27, 2019.
- [66] S. Zhang, Y. Zeng, Z. Li et al., “Generating one to four-wing hidden attractors in a novel 4D no-equilibrium chaotic system with extreme multistability,” *Chaos*, vol. 28, no. 1, Article ID 013113, 2018.
- [67] 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*, vol. 89, no. 2, pp. 1157–1171, 2017.
- [68] B. A. Mezatio, M. T. Motchongom, B. R. Wafo Tekam, R. Kengne, R. Tchitnga, and A. Fomethé, “A novel memristive 6D hyperchaotic autonomous system with hidden extreme multistability,” *Chaos, Solitons & Fractals*, vol. 120, pp. 100–115, 2019.
- [69] V.-T. Pham, C. Volos, S. Jafari, and T. Kapitaniak, “Coexistence of hidden chaotic attractors in a novel no-equilibrium system,” *Nonlinear Dynamics*, vol. 87, no. 3, pp. 2001–2010, 2017.
- [70] F. Yu, H. Shen, L. Liu et al., “CCII and FPGA realization: a multistable modified fourth-order autonomous Chua’s chaotic system with coexisting multiple attractors,” *Complexity*, vol. 2020, Article ID 5212601, 17 pages, 2020.
- [71] L. Xiang, Y. Li, W. Hao, P. Yang, and X. Shen, “Reversible natural language watermarking using synonym substitution and arithmetic coding,” *CMC: Computers, Materials & Continua*, vol. 55, no. 3, pp. 541–559, 2018.

- [72] K. Gu, N. Wu, B. Yin et al., "Secure data sequence query framework based on multiple fogs," *IEEE Transactions on Emerging Topics in Computing*, 2019.
- [73] L. Xiang, X. Shen, J. Qin, and W. Hao, "Discrete multi-graph hashing for large-scale visual search," *Neural Processing Letters*, vol. 49, no. 3, pp. 1055–1069, 2019.
- [74] K. Gu, X. Dong, and L. Wang, "Efficient traceable ring signature scheme without pairings," *Advances in Mathematics of Communications*, 2019.
- [75] M. Long, F. Peng, and H.-Y. Li, "Separable reversible data hiding and encryption for HEVC video," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 171–182, 2018.
- [76] K. Gu, K. Wang, and L. Yang, "Traceable attribute-based signature," *Journal of Information Security and Applications*, vol. 49, pp. 102400–102416, 2019.
- [77] S. He, W. Zeng, K. Xie et al., "PPNC: privacy preserving scheme for random linear network coding in smart grid," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 3, pp. 1510–1533, 2017.
- [78] L. Xiang, G. Guo, J. Yu et al., "A convolutional neural network-based linguistic steganalysis for synonym substitution steganography," *Mathematical Biosciences and Engineering*, vol. 17, no. 2, pp. 1041–1058, 2020.
- [79] Z. Xia, Z. Fang, F. Zou et al., "Research on defensive strategy of real-time price attack based on multiperson zero-determinant," *Security and Communication Networks*, vol. 2019, Article ID 6956072, 13 pages, 2019.
- [80] K. Gu, N. Wu, B. Yin, and W. J. Jia, "Secure data query framework for cloud and fog computing," *IEEE Transactions on Network and Service Management*, 2019.
- [81] Z. Liu, Z. Lai, W. Ou et al., "Structured optimal graph based sparse feature extraction for semi-supervised learning," *Signal Processing*, vol. 170, Article ID 107456, 2020.
- [82] K. Gu, W. Zhang, S.-J. Lim, P. K. Sharma, Z. Al-Makhadmeh, and A. Tolba, "Reusable mesh signature scheme for protecting identity privacy of IoT devices," *Sensors*, vol. 20, no. 3, p. 758, 2020.
- [83] J. J. He and B. Xu, "Quick pseudo-random topology optimization design based on triangle element," *Journal of Vibroengineering*, vol. 19, no. 4, pp. 2822–2843, 2017.
- [84] A. R. Ahmed, H. M. Ahmed, G. R. Ahmed et al., "Reconfigurable chaotic pseudo random number generator based on FPGA," *AEU-international Journal of Electronics and Communications*, vol. 98, pp. 174–180, 2019.
- [85] M. Narek, S. Konstantin, and S. George, "Spectral test of the MIXMAX random number generators," *Chaos, Solitons & Fractals*, vol. 118, pp. 242–248, 2019.
- [86] H. Xu, N. Massari, L. Gasparini, A. Meneghetti, and A. Tomasi, "A SPAD-based random number generator pixel based on the arrival time of photons," *Integration*, vol. 64, pp. 22–28, 2019.
- [87] R. S. Hasan, S. K. Tawfeeq, N. Q. Mohammed, and A. I. Khaleel, "A true random number generator based on the photon arrival time registered in a coincidence window between two single-photon counting modules," *Chinese Journal of Physics*, vol. 56, no. 1, pp. 385–391, 2018.
- [88] M. M. Abutaleb, "A novel true random number generator based on QCA nanocomputing," *Nano Communication Networks*, vol. 17, pp. 14–20, 2018.
- [89] C. Wannaboon, M. Tachibana, and W. San-Um, "A 0.18- μm CMOS high-data-rate true random bit generator through $\Delta\Sigma$ modulation of chaotic jerk circuit signals," *Chaos*, vol. 28, no. 6, Article ID 063126, 2018.
- [90] F. Yu, Q. Wan, J. Jin et al., "Design and FPGA implementation of a pseudorandom number generator based on a four-wing memristive hyperchaotic system and Bernoulli map," *IEEE Access*, vol. 7, pp. 181884–181898, 2019.
- [91] F. Yu, L. Li, Q. Tang, S. Cai, Y. Song, and Q. Xu, "A survey on true random number generators based on chaos," *Discrete Dynamics in Nature and Society*, vol. 2019, Article ID 2545123, 10 pages, 2019.
- [92] R. A. Elmanfaloty and E. Abou-Bakr, "Random property enhancement of a 1D chaotic PRNG with finite precision implementation," *Chaos, Solitons & Fractals*, vol. 118, pp. 134–144, 2019.
- [93] O. Katz, D. A. Ramon, and I. A. Wagner, "A robust random number generator based on a differential current-mode chaos," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 16, no. 12, pp. 1677–1686, 2008.
- [94] Y. Liu and X. Tong, "Hyperchaotic system-based pseudo-random number generator," *IET Information Security*, vol. 10, no. 6, pp. 433–441, 2016.
- [95] A. Akgul, H. Calgan, I. Koyuncu, I. Pehlivan, and A. Istanbulu, "Chaos-based engineering applications with a 3D chaotic system without equilibrium points," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 481–495, 2016.
- [96] Z. Wang, A. Akgul, V. T. Pham et al., "Chaos-based application of a novel no-equilibrium chaotic system with coexisting attractors," *Nonlinear Dynamics*, vol. 89, no. 46, pp. 1877–1887, 2017.
- [97] M. O. Meranza-Castillón, M. A. Murillo-Escobar, R. M. López-Gutiérrez, and C. Cruz-Hernández, "Pseudo-random number generator based on enhanced Hénon map and its implementation," *AEU—International Journal of Electronics and Communications*, vol. 107, pp. 239–251, 2019.
- [98] L. G. D. L. Fraga, E. Torres-Perez, and E. Tlelo-Cuautle, "Hardware implementation of pseudo-random number generators based on chaotic maps," *Nonlinear Dynamics*, vol. 90, no. 2, pp. 1661–1670, 2017.
- [99] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 101–111, 2014.
- [100] F. Yu and C. Wang, "Secure communication based on a four-wing chaotic system subject to disturbance inputs," *Optik*, vol. 125, no. 20, pp. 5920–5925, 2014.
- [101] Y. Chen, R. Xia, Z. Wang, J. Zhang, K. Yang, and Z. Cao, "The visual saliency detection algorithm research based on hierarchical principle component analysis method," *Multimedia Tools and Applications*, 2019.
- [102] W. Wang, Y. Li, T. Zou et al., "A novel image classification approach via dense-MobileNet models," *Mobile Information Systems*, vol. 2020, Article ID 7602384, 8 pages, 2020.
- [103] Y. Chen, J. Wang, S. Liu et al., "Multiscale fast correlation filtering tracking algorithm based on a feature fusion model," *Concurrency and Computation: Practice and Experience*, 2019.
- [104] D. Zhang, Z. Liang, G. Yang, Q. Li, L. Li, and X. Sun, "A robust forgery detection algorithm for object removal by exemplar-based image inpainting," *Multimedia Tools and Applications*, vol. 77, no. 10, pp. 11823–11842, 2018.
- [105] Y. Chen, J. Wang, R. Xia, Q. Zhang, Z. Cao, and K. Yang, "The visual object tracking algorithm research based on adaptive combination kernel," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 12, pp. 4855–4867, 2019.

- [106] J. Zhang and C. Liu, "A study of a clothing image segmentation method in complex conditions using a features fusion model," *Automatika*, vol. 61, no. 1, pp. 150–157, 2020.
- [107] Y. Chen, J. Xiong, W. Xu, and J. Zuo, "A novel online incremental and decremental learning algorithm based on variable support vector machine," *Cluster Computing*, vol. 22, no. 3, pp. 7435–7445, 2019.
- [108] W. Wei, T. Can, W. Xin, L. Yanhong, H. Yongle, and L. Ji, "Image object recognition via deep feature-based adaptive joint sparse representation," *Computational Intelligence and Neuroscience*, vol. 2019, Article ID 8258275, 9 pages, 2019.
- [109] Y. Chen, J. Wang, X. Chen et al., "Single-image super-resolution algorithm based on structural self-similarity and deformation block features," *IEEE Access*, vol. 7, pp. 58791–58801, 2019.
- [110] Y. Chen, J. Wang, X. Chen, A. K. Sangaiah, K. Yang, and Z. Cao, "Image super-resolution algorithm based on dual-channel convolutional neural networks," *Applied Sciences*, vol. 9, no. 11, p. 2316, 2019.
- [111] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, Article ID 107484, 2020.
- [112] H. Liu, Y. Zhang, A. Kadir, and Y. Xu, "Image encryption using complex hyper chaotic system by injecting impulse into parameters," *Applied Mathematics and Computation*, vol. 360, pp. 83–93, 2019.
- [113] Y. Xu, H. Wang, Y. Li, and B. Pei, "Image encryption based on synchronization of fractional chaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 10, pp. 3735–3744, 2014.
- [114] S. E. Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing Image Communication*, vol. 41, pp. 144–157, 2016.
- [115] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Processing: Image Communication*, vol. 52, no. 6, pp. 6–19, 2017.
- [116] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017.
- [117] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.
- [118] 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*, vol. 66, pp. 10–18, 2015.
- [119] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A colour image encryption scheme using permutation-substitution based on chaos," *Entropy*, vol. 17, no. 6, pp. 3877–3897, 2015.
- [120] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.
- [121] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," *Optics & Laser Technology*, vol. 121, Article ID 105777, 2020.