Hindawi
Complexity
Volume 2020, Article ID 8274685, 17 pages
https://doi.org/10.1155/2020/8274685

Research Article

Pseudorandom Number Generator Based on Three Kinds of Four-Wing Memristive Hyperchaotic System and Its Application in Image Encryption

Xi Chen,[1] Shuai Qian,[1] Fei Yu ,[1,2] Zinan Zhang,[1] Hui Shen,[1] Yuanyuan Huang,[1] Shuo Cai,[1] Zelin Deng,[1] Yi Li,[3] and Sichun Du[4]

[1]*School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China*
[2]*Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China*
[3]*Hunan Post & Telecommunication Planning and Designing Institute, No. 236 Yuanda Road, Changsha 410126, China*
[4]*College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China*

Correspondence should be addressed to Fei Yu; yufeiyfyf@csust.edu.cn

Received 23 July 2020; Revised 21 October 2020; Accepted 28 October 2020; Published 24 December 2020

Academic Editor: Jesus M. Muñoz-Pacheco

In this paper, we propose a method to design the pseudorandom number generator (PRNG) using three kinds of four-wing memristive hyperchaotic systems (FWMHSs) with different dimensions as multientropy sources. The principle of this method is to obtain pseudorandom numbers with good randomness by coupling XOR operation on the three kinds of FWMHSs with different dimensions. In order to prove its potential application in secure communication, the security of PRNG based on this scheme is analyzed from the perspective of cryptography. In addition, PRNG has passed the NIST 800.22 and ENT test, which shows that PRNG has good statistical characteristics. Finally, an image encryption algorithm based on PRNG is adopted. In the encryption algorithm, the optimized Arnold matrix scrambling method and the diffusion processing based on XOR are used to obtain the final encrypted image. Through the evaluation of encryption performance, it is concluded that there is no direct relationship between the pristine image and encrypted image. The results show that the proposed image encryption scheme has good statistical output characteristics and security performance in line with cryptography.

1. Introduction

With the continuous development of information technology, from the security of state secrets to the security of personal privacy, the issue of information security is increasingly concerned by the society and researchers [1–9]. Random numbers (RNs) are closely related to cryptography, which has attracted much attention due to its extreme sensitivity to keys, mixed data, pseudorandom behavior, and determinism. Therefore, the research of random number generator (RNG) with cryptographic security has become a hot spot [10–12]. These generators, which can produce true random numbers (TRNs) or pseudorandom numbers (PRNs), are called true random number generators (TRNGs) [11] and pseudorandom number generators (PRNGs) [10, 12], respectively. The TRNG based on physical phenomena (e.g., thermal noise and oscillator) has the disadvantage of the slow generation of TRN. In order to meet the needs of practical calculation, PRNG has been widely used due to its advantages of fast generation, repeatability, and less memory.

The existing PRNGs include linear congruence generators, carry-add-borrow subtractive generators, inverse congruence generators, and PRNGs based on chaotic systems. Due to some advantages of chaotic systems, such as sensitivity to initial conditions, ergodicity, pseudorandom behavior, and high complexity, chaotic systems are widely used in electronic circuits [13–17], synchronization [18–21],

secure communication [22–24], complex networks [25–29], and PRNGs [10–12, 30–32]. In [10], in order to make the possible key of the encryption scheme more difficult to crack, the author proposes a multiparameter mapping to determine the region of chaotic behavior and introduces additional disturbance into the chaotic map. Compared with traditional mapping, the randomness and superiority of the proposed scheme are proved. In [12], a PRNG based on piecewise logistic mapping (PLM) is proposed, and PLM is an enhanced version of logistic mapping. However, the PRNG based on this system needs 18 arithmetic operations to obtain 8-bit numbers, which is complex in calculation and inefficient in speed. Because the behavior characteristics of hyperchaotic systems are more complex than those of chaotic systems, which leads to better chaotic characteristics, higher sensitivity to initial conditions and control parameters, larger key space, stronger antidecoding ability of algorithms, and more complex dynamic characteristics [33–36]. This indicates that their dynamic sequences are more divergent than chaotic systems, and all these advantages are very useful for generating pseudo-random sequences with better statistical properties. Therefore, the PRNGs construction method based on the hyperchaotic system has attracted more and more scholars' attention and research. In [37], a self-perturbed PRNG based on the hyperchaotic system is proposed. A novel hyperchaotic system is constructed, in which the linear feedback controller is used as a disturbance factor to make the controllers interact with each other, thus achieving more complex dynamic behavior and avoiding the appearance of a short period sequence.

Memristor is a physically realized dynamic nonvolatile nanoscale device. As a controllable nonlinear device, it makes the generation of chaotic signals easier. Due to the addition of a memristor, the interaction between each variable in the memristive chaotic system or hyperchaotic system is intensified, resulting in the chaos, or hyperchaotic range is enlarged, and the dynamic characteristics become more complex [38–45]. On this basis, some RNGs based on memristive chaotic system or hyperchaotic system have been proposed successively [42, 46, 47]. Yu et al. [42] proposed a multistable 5D memristive hyperchaotic system. The multistable system is reflected in its different types of coexistence attractors, chaos, hyperchaos, period, and limit cycle. The authors designed an RNG suitable for actual image encryption application based on the complex characteristics of the multistable memristive hyperchaotic system. The resulting sequence passed the National Institute of Standards and Technology (NIST) test package and security analysis. Hashim et al. [46, 47] proposed a five-stage random number generator based on memristor. Each stage includes a memristor and an NMOS transistor. Their results show that the random number generator based on memristor is more random than the inverter-based random number generator because the memristor can produce highly random output in the circuit design.

Due to the good autocorrelation characteristics and larger key space, the design of RNG using multiple chaotic systems as entropy sources has attracted extensive attention of scholars recently [48–53]. In [48], a PRNG using a 4D memristor memristive hyperchaotic and Bernoulli map as double entropy source is proposed and implemented by FPGA. The pseudorandom sequence generated based on the double entropy source system has a good effect, which has passed the tests of statistical test suites such as NIST 800.22, ENT, and AIS.31. The key space, key sensitivity, and information entropy are analyzed to meet the security requirements of cryptography. In [49], a new PRNG is proposed based on two Tinkerbell maps. Despite the success of the statistical tests, the Tinkerbell mapping is a 2D system, and if the PRNG algorithm uses two mappings, there will be 26 arithmetic operations in each iteration, which will be slower to implement in hardware digital systems. In [50], a PRNG is designed by mixing three chaotic maps generated by an input initial vector together as an entropy source. In [51], a random bitstream is generated by comparing piecewise linear chaotic maps consisting of cross-coupled two Tent maps. In [51, 52], a PRNG based on two chaotic logistic maps and two standard chaotic maps is proposed, respectively. The abovementioned PRNGs based on multi-entropy source chaotic system meet the requirements of cryptographic communication through NIST 800.22 test package, statistical analysis, and relevant security analysis.

Images are processed differently from text because of their larger data capacity and the serious correlation between adjacent pixels. Image encryption algorithm involves a variety of alternative or transposition methods to convert ordinary images into encrypted images. For image, video, and other multimedia data with a large amount of data and strong correlation between adjacent data, the chaotic key has a stronger advantage in real-time encryption, so the research of the chaotic image encryption method is attracting more and more attention [54–60]. PRNG can generate sufficiently long pseudo-random digital key streams that are critical to the encryption of image pixels. For example, Ismail et al. [61] proposed a lossless image encryption algorithm based on edge detection and generalized chaotic mapping. A variety of pseudo-random number key generators based on generalized chaotic maps, including fractional order, delay, and bimodal logistic maps, are designed. Tsafack et al. [62] implemented an image encryption protocol based on chaos using the S-box structure and PRNG generation mechanism. In order to verify the performance of the protocols, the standard security analysis methods are adopted in [61, 62] and compared with other methods. The results show that the chaotic pseudorandom sequence has a broad application prospect in image encryption.

This paper presents a method to generate PRNGs using three kinds of four-wing memristive hyperchaotic systems (FWMHSs) with different dimensions. We conducted a comprehensive security analysis from the perspective of cryptography to verify the effectiveness of the proposed PRNG algorithm in cryptography applications, and the PRNG passed the NIST 800.22 test suite and ENT test. On this basis, a PRNG image encryption algorithm based on the multientropy source FWMHSs is proposed, and related security analysis is carried out. The rest of the paper is organized as follows. Section 2 enumerates the mathematical

models of three kinds of FWMHSs and briefly introduces their dynamic characteristics. In Section 3, these three kinds of FWMHSs are used to obtain the real number sequence by XOR operation, and then the binary quantization process is designed. Finally, the quantized binary sequence successfully passed the statistical test of NIST 800.22 and ENT test. Section 4 analyzes the proposed PRNG algorithm and its performance. In Section 5, PRNG is used to study the image encryption algorithm, and some security analysis is carried out on the image encryption. Finally, the conclusion is drawn in Section 6.

2. Three Kinds of FWMHSs

In recent years, many researchers have suggested using the complex chaotic system as an entropy source to design RNG, which can be used to improve the complexity and security level of the system because the complex chaotic system may have good randomness and complex chaos characteristics, so that the cipher system can obtain higher security [48–53]. In this paper, three kinds of FWMHSs with different dimensions are used as composite systems to construct the PRNG. The following three kinds of FWMHSs are, respectively, introduced.

2.1. 4D FWMHS. Recently, a 4D FWMHS is proposed in [38]. In this system, the periodic piecewise function is used to replace the control parameters of the Chen system, and a flux-controlled memristor with linear memductance is introduced. The nonlinear equation of the system is given by the following equation:

$$\begin{cases} \dot{x}_1 = a_1(x_2 - x_1), \\ \dot{x}_2 = (c_1 - a_1)x_1 - (k_1 + \operatorname{sign}(\sin(\omega t)))x_1x_3 + c_1x_2 + W(x_4)x_1, \\ \dot{x}_3 = x_1x_2 - b_1x_3, \\ \dot{x}_4 = x_1, \end{cases} \tag{1}$$

where x_1, x_2, x_3, x_4 are state variables and a_1, b_1, c_1, k_1 are system parameters. $W(x_1)$ is the flux-controlled memristor with linear memductance and $W(x_4) = -\beta_1 x_4$. When $a_1 = 35, b_1 = 3, c_1 = 28, k_1 = 2, \beta_1 = 0.24$ and the initial conditions are $[0.1, 0.1, 0.1, 0.1]$, the Lyapunov exponents are calculated as LE1 = 1.976, LE2 = 0.l, LE3 = 0 and LE4 = –11.950, respectively. System (1) contains two positive Lyapunov exponents, and the bifurcation diagram of the corresponding parameter range is shown in Figures 1(c) and 1(d), indicating that it is a hyperchaotic system, and its four-wing phase portrait is shown in Figures 1(a) and 1(b).

2.2. 5D FWMHS. A 5D FWMHS is proposed in [24] which has rich dynamic characteristics, and there exists a new critical point, called the permanent point. The coexistence of symmetric and multiwing attractors under different initial values of system parameters is discussed. Therefore, under certain initial conditions, chaotic or hyperchaotic attractors, periodic attractors, and quasiperiodic attractors also exist; for more dynamic characteristics, please refer to [24]. The mathematical model of the 5D memristor hyperchaotic system is

$$\begin{cases} \dot{y}_1 = -a_2y_1 + y_2y_3, \\ \dot{y}_2 = -b_2y_2 + y_1y_3, \\ \dot{y}_3 = y_1y_2 - c_2y_3 + d_2y_4W(y_5), \\ \dot{y}_4 = y_1y_2 - e_2y_4, \\ \dot{y}_5 = -y_3, \end{cases} \tag{2}$$

where y_1, y_2, y_3, y_4, y_5 are state variables and a_2, b_2, c_2, d_2, e_2 are system parameters. $W(y_5)$ is the flux-controlled memristor and $W(y_5) = 1 - \beta_2|y_5|$. When the system parameters are $a_2 = 10, b_2 = 12, c_2 = 30, d_2 = 2, e_2 = 3$, and $\beta_2 = 0.2$, and the initial values of system (2) are given as $[0.1, 0.1, 0.1, 0.1, 0.1]$, the Lyapunov exponents of system (2) are calculated as follows: LE1 = 3.5610, LE2 = 0.3092, LE3 = 0, LE4 = –2.0660, and LE5 = –23.4708. It can be seen that system (2) has two positive Lyapunov exponents, which means that the 5D FWMHS (2) can exhibit hyperchaotic dynamics. The bifurcation diagram of the four-wing hyperchaotic attractor, the Lyapunov exponent spectrum, and the bifurcation diagram of the corresponding parameters of system (2) are shown in Figure 2.

2.3. 6D FWMHS. More and more attention has been paid to high dimensional systems. The generated signals are usually used for secure communication and random number generation due to their complexity. High dimensional systems originated from neuroscience, laser, and other real-world systems with many interaction characteristics [63]. In [40], a 6D FWMHS with line equilibria based on a flux-controlled memristor model is proposed. Under different system parameters and initial values, the system exhibits rich dynamic behaviors, including quasiperiodic bifurcation and one-wing, two-wing, and four-wing chaotic attractors. The dynamics of the 6D FWMHS is described by the following set of equations:

$$\begin{cases} \dot{z}_1 = -a_3z_1 + z_1z_2, \\ \dot{z}_2 = -b_3z_2 + f_3W(z_6)z_5, \\ \dot{z}_3 = -c_3z_3 + z_1z_2 + g_3z_5, \\ \dot{z}_4 = d_3z_4 - h_3z_3, \\ \dot{z}_5 = e_3z_5 - z_1^2z_2, \\ \dot{z}_6 = z_5, \end{cases} \tag{3}$$

where $z_1, z_2, z_3, z_4, z_5, z_6$ are state variables and $a_3, b_3, c_3, d_2, e_3, f_3, g_2, h_3$ are system parameters. $W(z_6)$ is the flux-controlled memristor and $W(z_6) = m + 3nz_6^2$. When system parameters are select as $a_3 = 10, b_3 = 60, c_3 = 20, d_3 = 15, e_3 = 40, f_3 = 1, g_3 = 50, h_3 = 10, m = 13$, and $n = 0.02$, the initial conditions are $[1, 1, 1, 1, 1, 1]$,

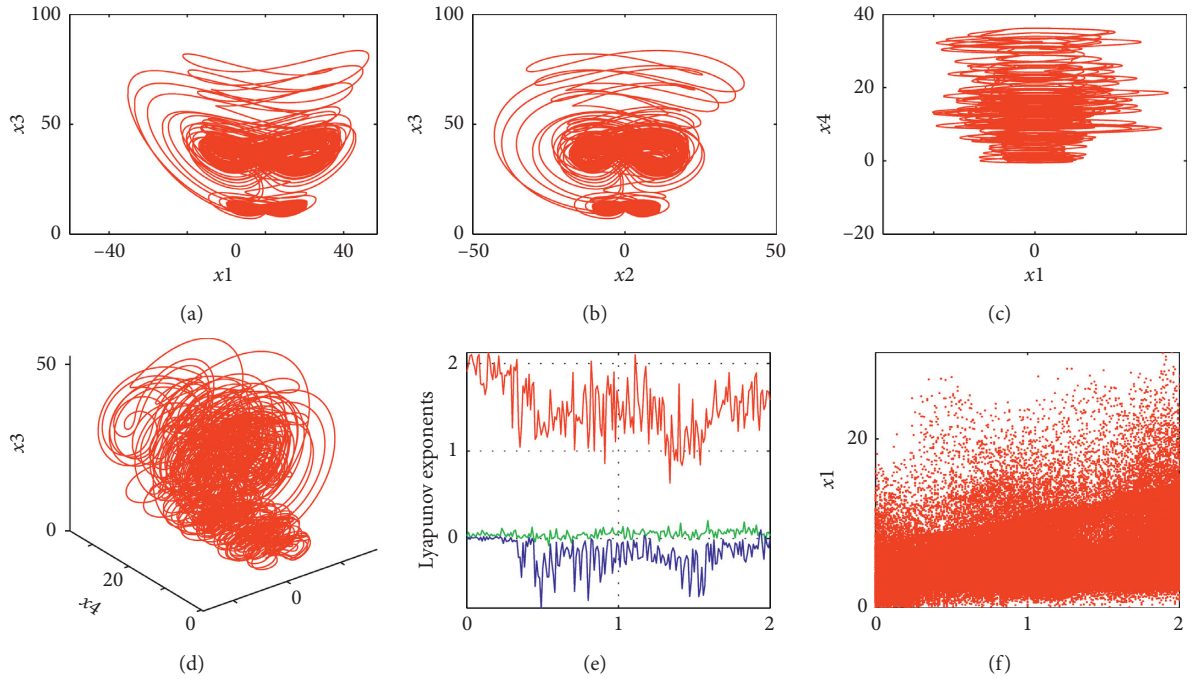


Figure 1: (a) $x_1 - x_3$ plane of 4D FWMHS attractors; (b) $x_2 - x_3$ plane of 4D FWMHS attractors; (c) $x_1 - x_4$ plane of 4D FWMHS attractors; (d) $x_2 - x_3 - x_4$ plane of 4D FWMHS attractors; (e) the Lyapunov exponent spectrum for control parameter β_1; (f) bifurcation diagram for control parameter β_1.

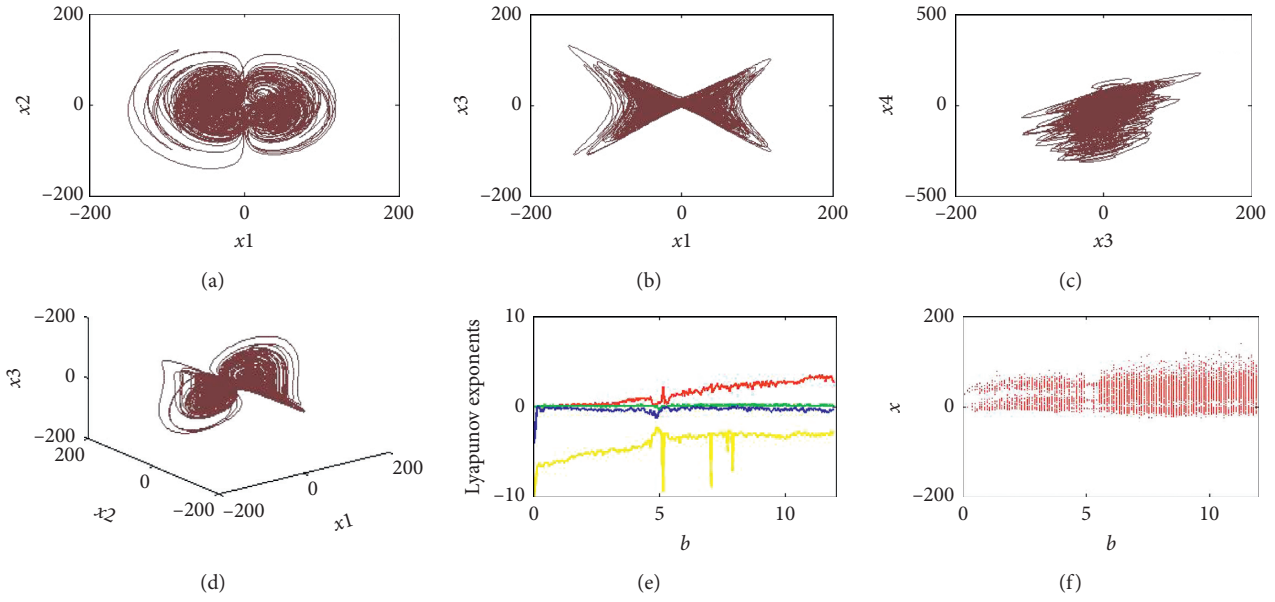


Figure 2: (a) $y_1 - y_2$ plane of 5D FWMHS attractors; (b) $y_1 - y_3$ plane of 5D FWMHS attractors; (c) $y_2 - y_3$ plane of 5D FWMHS attractors; (d) $y_3 - y_4$ plane of 5D FWMHS attractors; (e) the Lyapunov exponent spectrum for control parameter b_2; (f) bifurcation diagram for control parameter b_2.

$LE_s = [10.16, 2.187, 0.0136, -0.5759, -16.08, -18.86]$, which indicates system (3) has two positive Lyapunov exponents and the 6D FWMHS is in hyperchaos. Figure 3 shows the phase portrait of the four-wing hyperchaotic attractor, Lyapunov exponent spectrum, and the bifurcation diagram of corresponding parameters of system (3).

3. PRNG Based on Three Kinds of FWMHSs

3.1. The Structure of PRNG Algorithm. The PRNG design method of the chaotic system with a single entropy source is too simple, easy to be intercepted reversely, and the complexity is low. The chaotic characteristics of multientropy

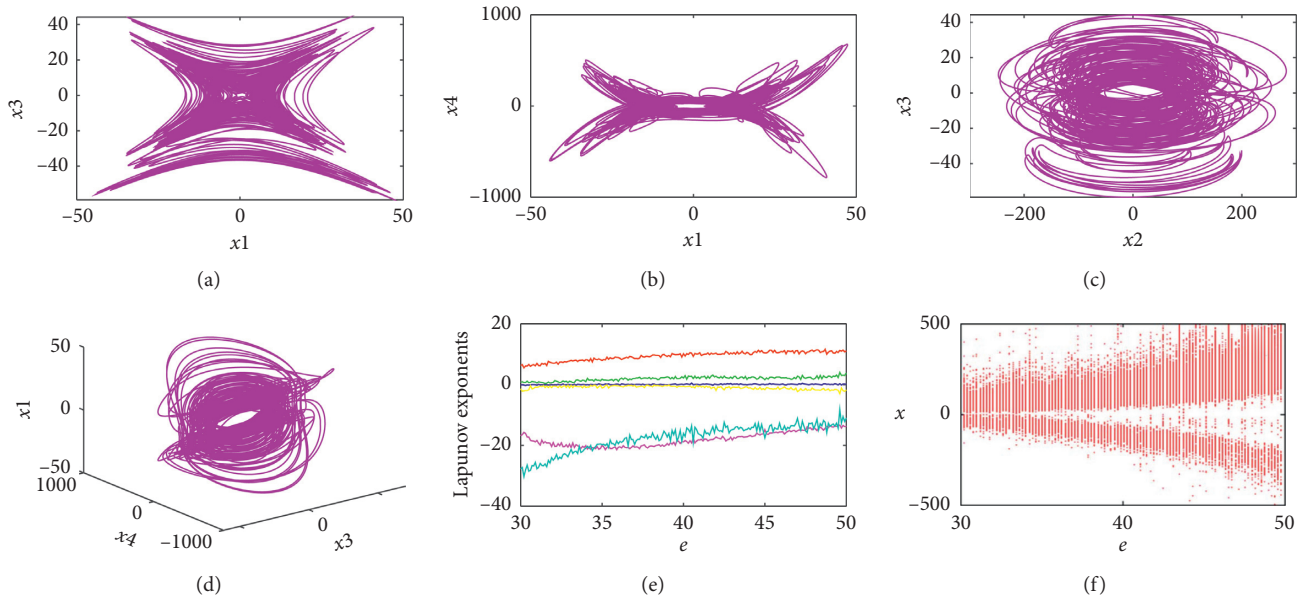


FIGURE 3: (a) $z_1 - z_3$ plane of 6D FWMHS attractors; (b) $z_1 - z_5$ plane of 6D FWMHS attractors; (c) $z_2 - z_3$ plane of 6D FWMHS attractors; (d) $z_1 - z_3 - z_4$ plane of 6D FWMHS attractors; (e) bifurcation diagram for control parameter e_3; and (f) bifurcation diagram for control parameter e_3.

source memristive hyperchaotic systems are dependent on the hyperchaotic systems (1)–(3) described above. Therefore, it is more complex than every single hyperchaotic system. The RNs generated by PRNG is designed with these three kinds of FWMHSs as multientropy source to achieve a better random effect and meet security requirements.

The binary quantization process of the chaotic real number sequence is an important step in the design of generating the pseudo-random sequence. It will directly affect the randomness and complexity of the sequence and ultimately affect the security of its application system. In order to make the pseudo-random generator have a good output rate and good robustness, the binary quantization of three kinds of fwmhs is carried out, and the real number sequence is output. For three kinds of continuous memristive hyperchaotic systems, the RK-4 algorithm is used to discretize the system, and a 32-bit floating-point number is generated for every iteration. Then, the output sequence of chaos in each dimension is calculated by exclusive or operation, and the hetero scheme is as follows: $x_1y_1, x_1z_1, x_2y_2, x_2z_2, x_3y_3, x_3z_3, x_4y_4, x_4z_4, y_5z_5$.

Then, the XOR operation is performed to enhance the randomness, and the output sample is taken as the final bit sequence. The specific flow chart is shown in Figure 4, where X_i_OUT, Y_i_OUT, Z_i_OUT are the output sequences of 4D, 5D, and 6D continuous memristive hyperchaotic systems.

3.2. Randomness Tests. A large number of randomness testing algorithms and related standards have been published to evaluate the generated pseudo-random sequences, which can provide a lot of reference data for theoretical analysis. ENT (pseudo-random number sequence test program) test program can easily give four statistics to measure randomness, Shannon entropy of each byte in a pseudo-random sequence, π value calculated by the Monte Carlo method, arithmetic mean root of sequence, and first-order self-correlation number of sequence. The 800.22 test grouping provided by NIST suggests 16 statistical test methods for randomness testing arbitrary long binary sequences. Some of these 16 test items contain multiple subtest items, and the results of each test item have two indicators, namely, $p$value and pass rate. For p value, when p value ≥ 0.01 0.01, we consider the sequence to be random. The usual value is $[0.001, 0.01]$, where we deem the set significance level $\alpha = 0.01$. For the value of the pass rate, if the value is within the confidence interval, it means that the sequence passes the test and is set as the group number of the sequencing column; then, the confidence interval is

$$\left[1 - \alpha - 3\sqrt{\frac{\alpha(1-\alpha)}{\beta}}\beta, 1 - \alpha + 3\sqrt{\frac{\alpha(1-\alpha)}{\beta}}\right]. \quad (4)$$

In this experiment, the pseudorandom sequences generated by our proposed method generate 130 different binary sequences of 1M bits length. That is, $\beta = 130$, and the calculated confidence interval is $[0.96384, 1]$. As can be seen from Table 2, the $P-$value of each item is greater than the significance level, and the pass rate proportion value is within the confidence interval, so the generated sequence can completely pass the NIST test, and Table 3 shows that the test results of ENT reach the ideal value. That is, the sequence is random.

4. Security Analysis

4.1. Complexity Analysis. The complexity of multientropy source memristor hyperchaotic system is mainly reflected by approximate entropy (ApEn). ApEn is a kind of used to quantify the time sequence regularity of volatility and

Table 1: Flow chart of the specific process of the PRNG design.

Initialization:	$\{X\} = \{x_1, x_2, x_3, x_4\}$ $\{Y\} = \{y_1, y_2, y_3, y_4, y_5\}$ $\{Z\} = \{z_1, z_2, z_3, z_4, z_5, z_6\}$ X_i–OUT = (32 : 0) Y_i–OUT = (32 : 0) Z_i–OUT = (32 : 0)
While (key condition) do choose the last 22 binary decimal values from the sequences of 4D, 5D, and 6D continuous memristive hyperchaotic that called Xi_OUT, Yi_OUT, and Zi_OUT,	
Obtain bit stream based on XOR of $x_1y_1, x_1z_1, x_2y_2, x_2z_2, x_3y_3, x_3z_3, x_4y_4, x_4z_4, y_5z_5$ $t = t + 1$ until $n = N$ end while	

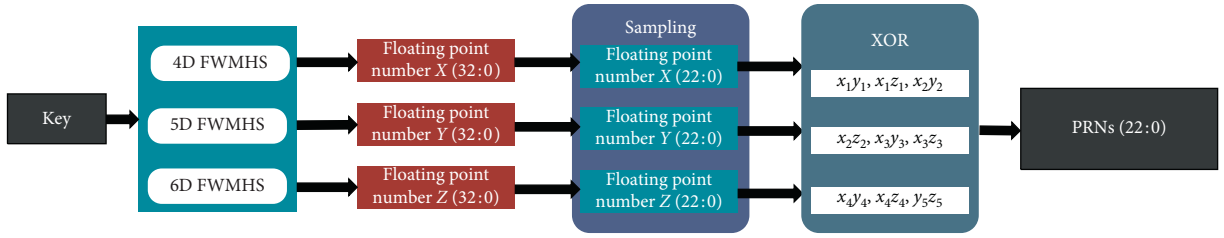


Figure 4: Flow diagram of PRNG design.

Table 2: The results of NIST test suite.

Statistical test	Proportion	P–value	Results
Frequency	0.9667	0.074177	Success
Block Frequency	0.9917	0.585209	Success
Cumulative Sums	0.9750	0.051391	Success
Runs	0.9917	0.980883	Success
Longest Run	0.9667	0.378138	Success
Rank	0.9917	0.213309	Success
Fft	0.9750	0.931952	Success
Nonoverlapping Template	1	0.772760	Success
Overlapping Template	0.9833	0.970538	Success
Universal	0.9833	0.337162	Success
Approximate Entropy	0.9917	0.222869	Success
Random Excursions	1	0.437274	Success
Random Excursions Variant	1	0.706149	Success
Serial	0.9917	0.324180	Success
Linear Complexity	0.9917	0.048716	Success

Table 3: The results of ENT test suite.

Test name	Test output	Ideal value	Results
Entropy	7.99999	8	Success
Arithmetic Mean	0.5000	0.5	Success
Monte Carlo Value for Pi	3.142444	3.141592	Success
Serial Correlation Coefficient	−0.000033	0	Success

unpredictability of nonlinear dynamics parameters, it, with a negative number to represent the complexity of a time series, reflects the time series of the possibility of new information, its physical meaning is when the dimension change, the size of the time series of the new model of probability, produce the greater the probability of new pattern, the more complex time series, the greater the corresponding approximate entropy [64]. Later, the approximate entropy is extended to measure the randomness of binary sequences [65]. In this chapter, we discuss the effect of the length of the pseudo-random sequence on the approximate entropy value. The more uniform the general probability distribution is, the more complex the sequence will be, and the greater the approximate entropy will be. The process of ApEn definition is as follows:

Definition. 1

(1) When there is an n-dimensional time series $\kappa(1), \kappa(2), \ldots, \kappa(N)$ obtained by sampling at equal time intervals.

(2) Reconstruct m-dimension vector $X(1), X(2), \ldots, X(N-m+1)$, where $X(i) = [\kappa(i), \kappa(i+1), \ldots, \kappa(i+m-1)]$.

(3) For $1 \le i \le N-m+1$, count the number of vectors that meet the following conditions:

$$C_i^m(r) = \frac{(\text{number of } X(j) \text{such that } d[X(i), X(j)] \le r)}{(N-m+1)}, \tag{5}$$

where $d[X, X^*]$ is defined as $d[X, X^*] = \max|\kappa(a) - \kappa^*(a)|$, $\kappa(a)$ is the element of vector X, d is the distance between vectors $X(i)$ and $X(j)$, which is determined by the maximum difference value of the corresponding element, and the value range of j is $[1, N-m+1]$, including $j = i$.

(4) ApEn is defined as

$$\text{ApEn} = \theta^m(r) - \theta^{m+1}(r), \tag{6}$$

where m is an integer representing the length of the comparison vector; r is a real number, representing the measure of "similarity," usually $r = 0.2 \times \text{std}$, where std represents the standard deviation of the original time series.

Table 4 lists the ApEn values corresponding to different sequence lengths. It can be seen that with the increase of chaotic sequence length, the complexity of chaotic sequence increases, and the ApEn value of chaotic sequence also has risen, showing the superiority of random sequence.

4.2. Key Space and Running Speed Analysis. Generally speaking, it is not secure when the key space is less than 2^{128}. With the respect to an ideal cryptosystem, it should be lagre enough to make brute force attack infeasible. In a multi-entropy source based on FWMHSs, when we fix another parameter or initial value and change a parameter or initial value, the changed parameter or initial value is called a secret key. The key is sensitive to any differences equal to or larger than 10^{-12}. Therefore, the key space is larger than 10^{12}. So that roughly the key space of the multientropy source based on FWMHSs can be calculated as follows: $\underbrace{(10^{13} \times 10^{13} \times \cdots \times 10^{13})}_{\text{4 keys for 4 DFWMHS}} \times \underbrace{(10^{13} \times 10^{13} \times \cdots \times 10^{13})}_{\text{6 keys for 5 DFWMHS}} \times \underbrace{(10^{13} \times 10^{13} \times \cdots \times 10^{13})}_{\text{9 keys for 6 DFWMHS}} = 10^{228} \approx 2^{760}$, which is enough to resist all kinds of violent attacks. One of the advantages of chaotic cryptography is higher running speed. In addition, when it comes to the proposed PRNGs meeting today's safety standards, the proposed method has a fairly satisfactory running speed. The experimental hardware environment is 1.8 GHz Intel Celeron CPU and 8 GB memory computer; the software environment is windows 7 and MATLAB 2014 compiler, and the proposed PRNG can achieve a running speed of 0.3256 Mbits/s.

Table 4: ApEn values corresponding to different sequence lengths.

Sequence length (bits)	ApEn
1320	0.6930
6600	0.6931
22000	0.7707

4.3. Key Sensitivity Analysis. In the key sensitivity analysis, we use the bit change rate to measure its sensitivity to the key, that is, to observe the degree of the number of bits in the sequence generated by the PRNG when the key is slightly changed. By counting the change of the value of "0" and "1" in the corresponding position of the binary sequence, the corresponding bit change rate is calculated:

$$T = \frac{n'}{n}, \tag{7}$$

where n and n' are binary sequences generated before and after minor changes in the initial key of the system. Take the key of 4D FWMHS as an example, when a_1 to $a_1 + 10^{-12}$ (K_{a_1}) and x_0 to $x_0 + 10^{-12}$ (K_{x_0}) change, respectively, the key sensitivity analysis of PRNG proposed in this paper is shown in Table 5. The ideal bit change rate is 50%. The closer the bit change rate obtained through simulation is to 50%, the more sensitive the PRNG is to the initial value.

4.4. Correlation Analysis. Correlation analysis refers to the analysis of two or more elements with correlation variables to measure the degree of correlation between two sequences. Autocorrelation function refers to the correlation between a sequence $\{\eta_i\}$ and its corresponding shifted sequence $\{\eta_i + t\}$. The autocorrelation function of a pseudorandom sequence with good performance is similar to that of a function δ. When used to measure the correlation of two given sequences at different times, the autocorrelation function of a pseudo-random sequence with good performance tends to 0. The correlation coefficient between sequence $X_i\,(i = 0, 1, \ldots, n)$ generated by the original key and sequence $Y_i\,(i = 0, 1, \ldots, n)$ generated after the key is slightly changed can be expressed as

$$C_o = \frac{\sum_{i=0}^{N}[(X_i - \mu X) \cdot (Y_i - \mu Y)]}{\sigma X \cdot \sigma Y}, \tag{8}$$

where μ and σ represent mean and standard deviation, respectively. If $C_o = 0$, the difference between the two sequences is obvious and there is almost no correlation. Take the key of 4D FWMHS as an example, the trajectories of each sequence and the corresponding sequence generated after the minor change of the key are shown in Figure 5. The red trajectory represents the sequence generated after the minor change of the original key, and the blue trajectory represents the sequence after the minor change of the original key. The system trajectory produced a separation after about five iterations, indicating that it was very sensitive to small changes in the key. Moreover, from the uniform results of autocorrelation and cross-correlation in Figure 6 and the

Table 5: Sensitivity analysis of initial value.

Initial key	K_{a_1}	K_{x_0}
T/%	49.911	49.796

correlation coefficient in Table 6 approaching 0, it is verified that there is almost no correlation between the pseudorandom sequences generated by this method, and it can be seen that the PRNG proposed by our method is ideal and conforms to security. The academic degree of the proposed PRNG has a high sensitivity to the key.

4.5. Spectral Entropy Complexity Analysis. Based on the Fourier transform, the SampEn algorithm is used to calculate the relative power spectrum and spectral entropy complexity of the sequence in combination with the Shannon entropy [66–68]. Its function is to analyze the complexity and security of the chaotic system. The more complex the spectrum of a general sequence, the greater the spectral entropy [69–71]. Figure 7 shows the spectral entropy complexity of the three kinds of FWMHSs when some parameters change with each other. It can be seen from these figures that spectral entropy is in these high-complexity regions when $a_1 \in (10, 10.5)$ and $d_2 \in (4, 6)$ (as shown in Figure 7(a)), $a_1 \in (6, 10)$ and $\beta_3 \in (4, 6)$ (as shown in Figure 7(b)), and $d_2 \in (0, 8)$ and $\beta_3 \in (6.2, 6.8)$ (as shown in Figure 7(c)). It shows that these three systems have high complexity in a large range; that is, chaos or hyperchaos exist in these ranges.

As people are more and more interested in the study of chaotic systems, some PRNGs based on chaos have been implemented. Since the PRNG is the main core of cryptography encryption algorithm, in order to evaluate the advantages of the proposed scheme, we focus on the security and give the comparison results with other latest schemes in Table 7, including the number of types of entropy sources, randomness test packages, and security analysis.

5. Image Encryption Application

Digital image has been regarded as the main carrier of information communication because of its intuitive and vivid features. Digital image files mainly store the color and grayscale information of the image, but the image information in the process of image transmission may involve a large number of private information, so ensuring the security of the image in the process of transmission and storage has become the focus of attention and research [72–77]. At present, the combination of the chaotic system and image encryption becomes a hot topic in cryptography. In this section, based on the pseudorandom sequence generated by the three kinds of FWMHSs, the position or pixel value of image pixels is scrambled and replaced. Finally, the validity analysis of encrypted images, key space, histogram analysis, key sensitivity, antidifferential aggression, and correlation between adjacent pixel points are carried out.

5.1. Bit Plane Layering. In an image, a pixel is a number of bits. The grayscale of each pixel is made up of eight bits (bytes). Then, an 8-bit image can be considered to be composed of 8 1-bit planes [78], as shown in Figure 8. Figures 9(b)–9(i) refer to the eight 1-bit planes of the 8-bit image, from top to bottom, from the highest order bit to the lowest order bit. The acquisition of each bit layer is the binary image obtained under the processing of the threshold gray transformation function (denoted as ε). Generally speaking, all grayscale mappings greater than ε are 1, and all grayscale mappings less than ε are 0. However, for the convenience of image encryption, we set all grayscale mappings less than ε to 0.5.

The decomposition of an image into a bit plane can help us determine the adequacy of the number of bits used to quantify the image. Reconstruction is made by multiplying the pixels of the n-th plane by the constant 2^{n-1}. The plane used to reconstruct an image can be less than all the bitplanes decomposed. As can be seen from Figure 9, the higher the bit image, the more information the original image contains. The three-bit layers constitute the image in Figure 10(c), which generally restores the original image. Although the main features of the original image have been restored, they are somewhat flat and lack details, especially in the background area. Adding bitplane 5 to reconstruction effectively improves this situation, as shown in Figure 10(b). After many trials, adding more planes will not contribute much to the appearance of the image. Similarly, compared with the time consumed by the proposed encryption scheme, it takes 0.1568 s to encrypt an 8-bit Lena image and 0.1576 s to encrypt a 4-bit Lena image. The time consumed by encrypting two different bit planes can be regarded as equal. Thus, storing four higher-order bitplanes can restore the details in the accepted range to reconstruct the original image, and using four bit planes to reconstruct the original image can reduce the storage by 50%.

5.2. Proposed Image Encryption Algorithm. In this section, we will encrypt the image based on the proposed pseudorandom number sequence, and the image scrambling and diffusion can be realized in the spectrum domain. The process of the proposed image encryption algorithm is as follows:

Step 1: The 4-bit plane obtained by bit layered decomposition and reconstruction is used as the original 2D plaintext image P, as shown in Figures 11(a) and 11(d).

Step 2: Random scrambling. PRNG based on multientropy source FWMHSs is used to generate pseudorandom number vector X with length $2(M \times N)$, each random number $X_i \in \{1, 2, \ldots, 10MN\}$, and then random one-dimensional vector a and b with size $M \times N$ are generated from X. The image matrix P is then transformed into a one-dimensional vector A with the size of $M \times N$. Arnold transformation is performed on any coordinate position of vector A to obtain the coordinate (m, n) of the row, namely,

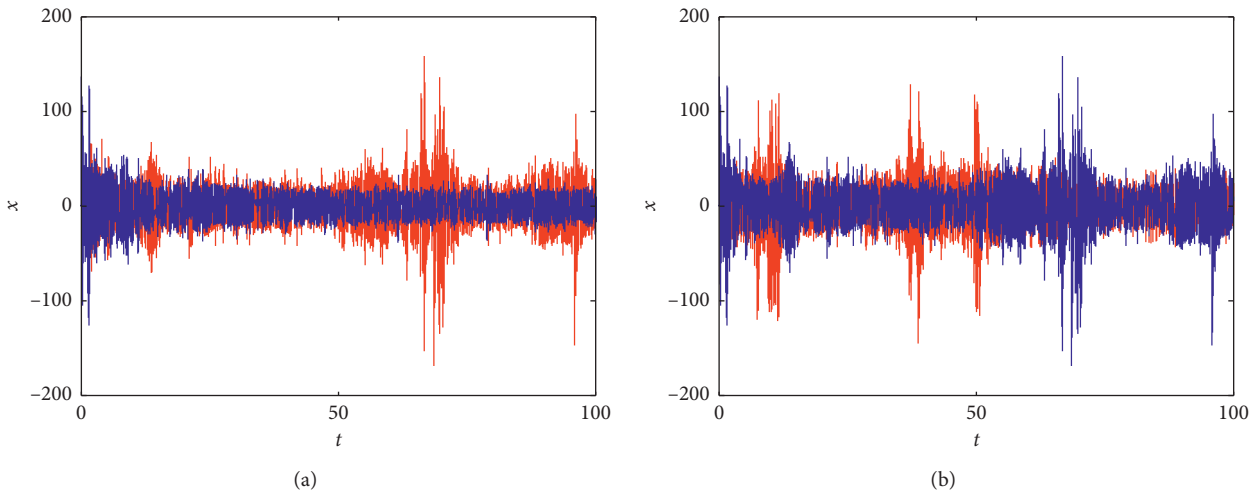


Figure 5: Time domain waveform. (a) The parameters a_1 (red) and $a_1 + 10^{-12}$ (blue). (b) The initial conditions x_0 (red) and $x_0 + 10^{-12}$ (blue).

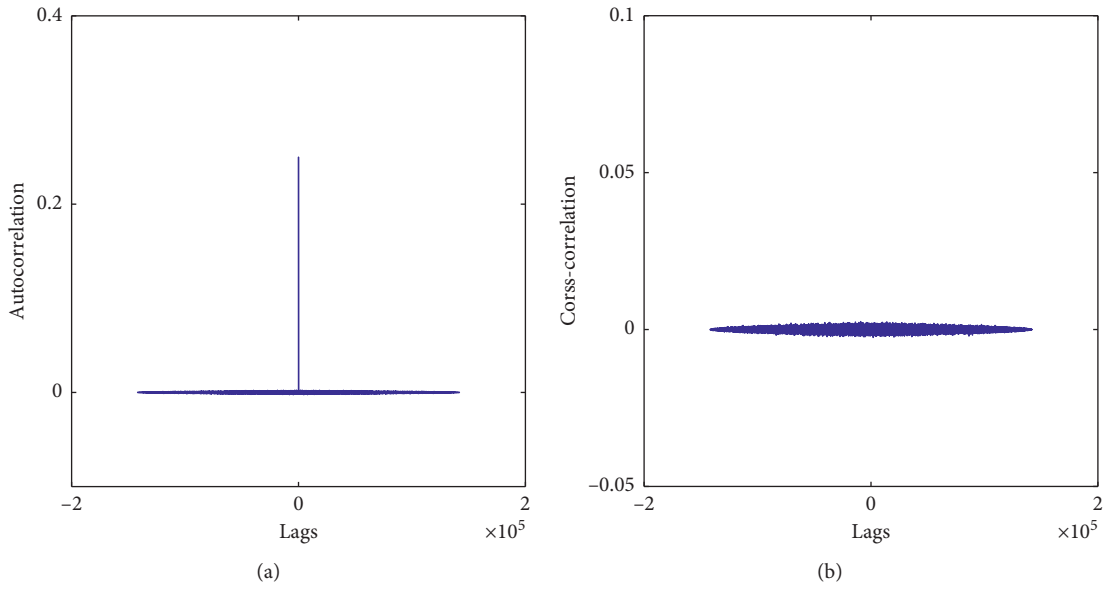


Figure 6: The correlation properties analysis. (a) Autocorrelation. (b) Cross-correlation.

Table 6: Correlation coefficient of different initial keys.

Initial key	Correlation coefficient		
	K_{x_0}	K_{a_1}	K_{b_1}
—	0.0041	0.0018	−0.0022

$$\begin{bmatrix} m \\ n \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} 1 \\ j \end{bmatrix}. \tag{9}$$

So $m = 1 + aj$ and $n = b + (ab + 1)j$. Here, take $ab + 1$ as a new random number through optimization, which is still recorded as a; then $n = b + aj$. Finally, the scrambled image D is obtained, as shown in Figures 11(b) and 11(e).

Step 3: The image D and the pseudorandom sequence $C_d \in \{d = 1, 2, \ldots, M \times N\}$ generated by PRNG of length $M \times N$ are diffused for XOR; that is, the final encrypted image is $T = D \oplus C$, as shown in Figures 11(c) and 11(f). The decryption algorithm is the inverse process of the encryption algorithm. The specific encryption and decryption flow chart is shown in Figure 12.

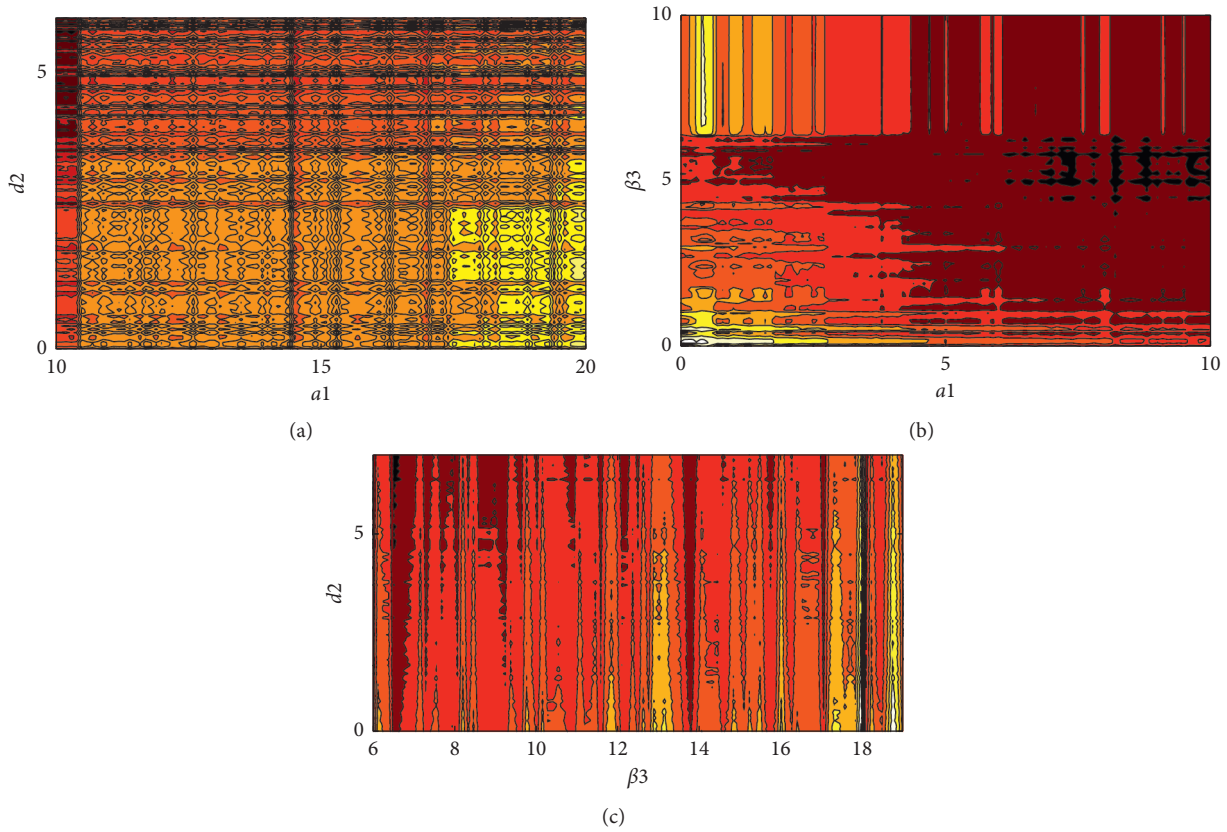


Figure 7: Spectral entropy complexity: (a) in $a_1 - d_2$ plane; (b) in $a_1 - \beta_3$ plane; and (c) in $d_2 - \beta_3$ plane.

Table 7: Comparison of the three kinds of FWMHSs with recent literature.

Refs.	[10]	[12]	[37]	[40]	[49]	[50]	Proposed
Type	PRNG	PRNG	PRNG	PRNG	PRNG	PRNG	PRNG
Entropy source	Adaptive chaotic maps	Multimodal map	4D hyperchaotic system	5D memristive hyperchaotic system	Two Tinkerbel maps	Three chaotic maps	Three kinds of FWMHSs
Past processing	✓	XOR	✓	XOR	✓	XOR	XOR
Test suit	NIST	NIST	NIST	NIST	NIST, ENT DIEHARD	NIST	NIST, ENT
Key space	2^{424}	2^{159}	2^{70}	2^{192}	2^{183}	—	2^{760}
Key sensitivity	—	?	49.74% (bit change rate)	50.0028% (bit change rate)	?	✓	49.911% (bit change rate)
Correlation	<0.02	<0.05	−0.00047	0.000198	−0.000330	—	0.0018
Entropy	—	—	7.9896	—	—	—	—
Speed (Mbit/s)	0.3	—	0.5017	—	0.4901	—	0.3256
Comparison analysis	✓	—	—	✓	—	—	✓
Entropy complexity	—	—	—	—	—	—	✓

5.3. Security Analysis

5.3.1. Key Space and Execution Efficiency. The encryption scheme proposed in this paper uses the initial value of state variables of multientropy source memristor hyperchaotic system as the original key, and the key space can reach 2^{760}, which is equivalent to 760-bit key length. If the system parameters are also used as the original key, the key space is larger. Therefore, this algorithm has the ability to resist the exhaustive attack. The main way to improve efficiency is to use integer operation and implement the subgraph parallel encryption strategy.

5.3.2. Histogram and Correlation Analysis. Due to the spectrum characteristics of the digital image, the algorithm must have similar security and performance for any image

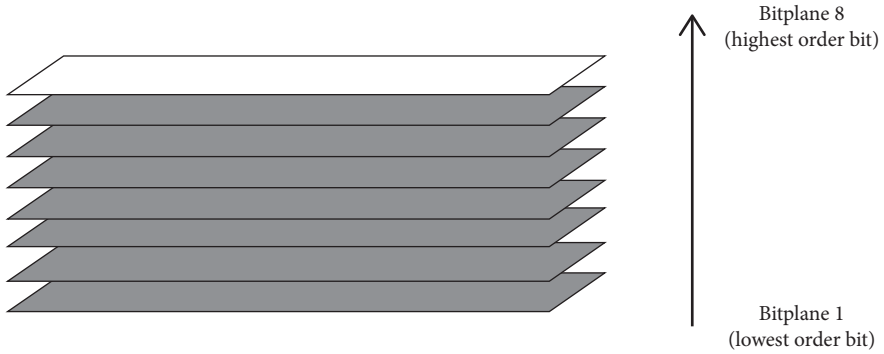


Figure 8: Bit plane representation of an 8-bit image.

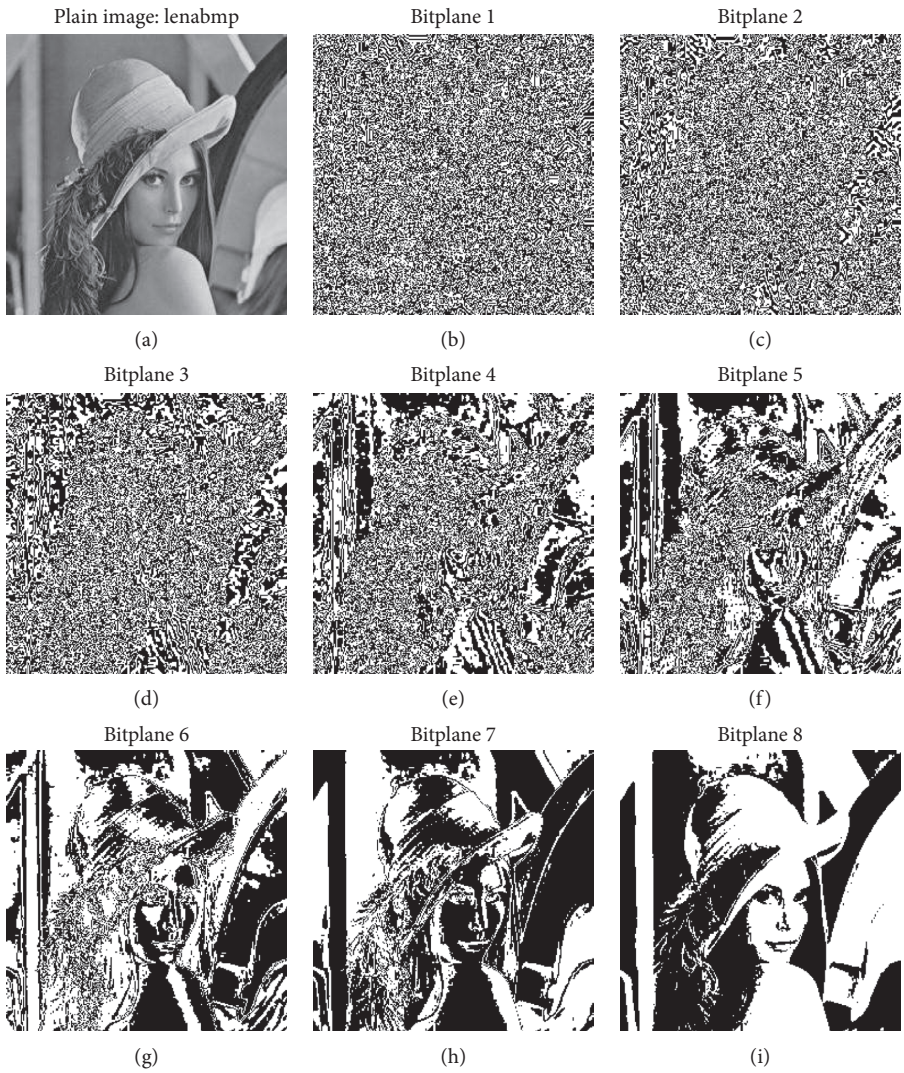
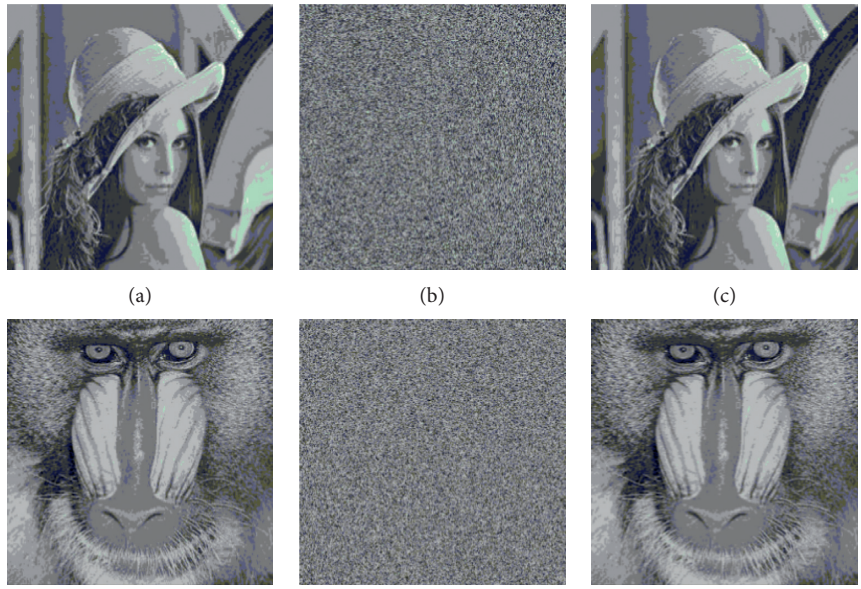


Figure 9: An 8-bit grayscale image with a size of 256×256 pixels.

encryption. The ideal histogram distribution of the ciphertext image should be uniform to prevent attackers from obtaining some information from the fluctuating histogram. We use the proposed algorithm to encrypt the original two-dimensional plaintext image P to obtain an encrypted image similar to noise, as shown in Figure 11(c). When we use four-bit layer image analysis and image encryption, some pixels in each pixel $p_i \in [0, 255]$ of the original plain-text reconstructed image P are missing, and the histogram display is shown in Figures 13(a) and 13(c)). However, we will

(a) (b) (c)

Figure 10: (a) Eight-bit grayscale original image of 256 × 256 pixels in size; (b) images reconstructed using bitplanes 5, 6, 7, and 8; and (c) image reconstructed using bitplanes 6, 7, and 8.



(a) (b) (c)

(d) (e) (f)

Figure 11: (a) Original image Lena. (b) Encrypted image Lena. (c) Decrypted image Lena. (d) Original image Baboon. (e) Encrypted image Baboon. (f) Decrypted image Baboon.

inevitably lose some unimportant values (mainly the image micro detail data, which does not affect the image vision). Through the histogram of ciphertext in Figures 13(b) and 13(d), we can see that the value of ciphertext pixel is very small, which is due to the loss of some micro detail data pixel value; in this case, the histogram cannot reflect the uniformity. We will verify the uniformity of the encrypted image by the following security analysis.

The correlation between adjacent pixels indicates the quality of image encryption. Of course, the correlation between adjacent pixels of the plaintext image will be very high. Through a good encryption algorithm, the correlation between these pixels can be eliminated, which avoids the attacker from the perspective of correlation to obtain image information. We randomly select 1000 pairs of pixel values on the horizontal, vertical, and diagonal adjacent pixels of plaintext image p and encrypted image t. Then, we calculate the correlation coefficient in Table 8 through the correlation coefficient equation (8). Among the correlation coefficients of the two images, the two correlation coefficients of the encrypted image generated by the proposed algorithm are the smallest among all the comparable algorithms, and [79, 80] have a minimum correlation coefficient, respectively. In addition, the correlation coefficients of the encrypted image in three directions are close to 0, which means that the correlation between adjacent pixels in the plane image is effectively eliminated, and the image obtained is completely unrecognizable. In this paper, histogram and correlation tests are used to prove the resistance to statistical attacks.

5.3.3. Differential Key Attack Analysis. Differential cryptanalysis is one of the most effective methods to attack iterative block cipher. It is to recover some key bits by analyzing the influence of plaintext pair difference on ciphertext pair difference. The number of pixels change rate (NPCR) and the unified average changing intensity (UACI)

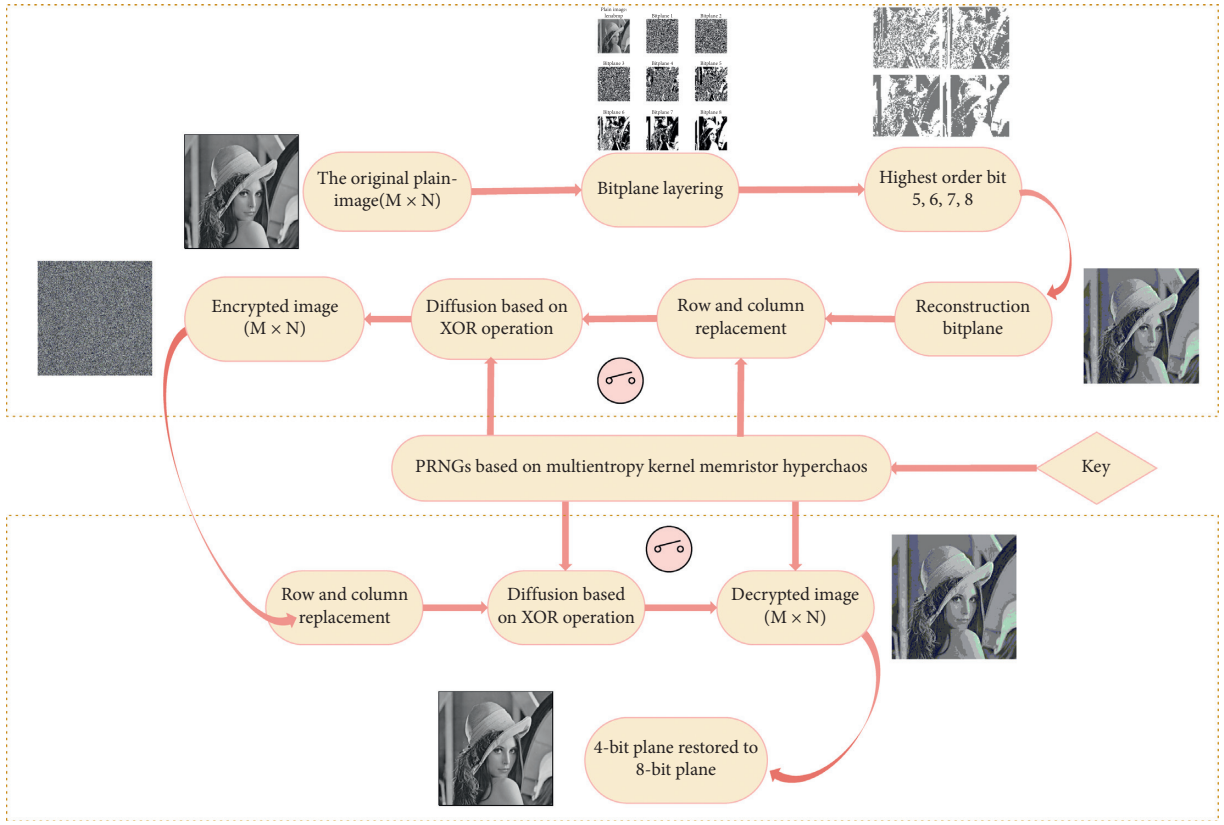


Figure 12: Proposed chaotic digital image cryptography system.

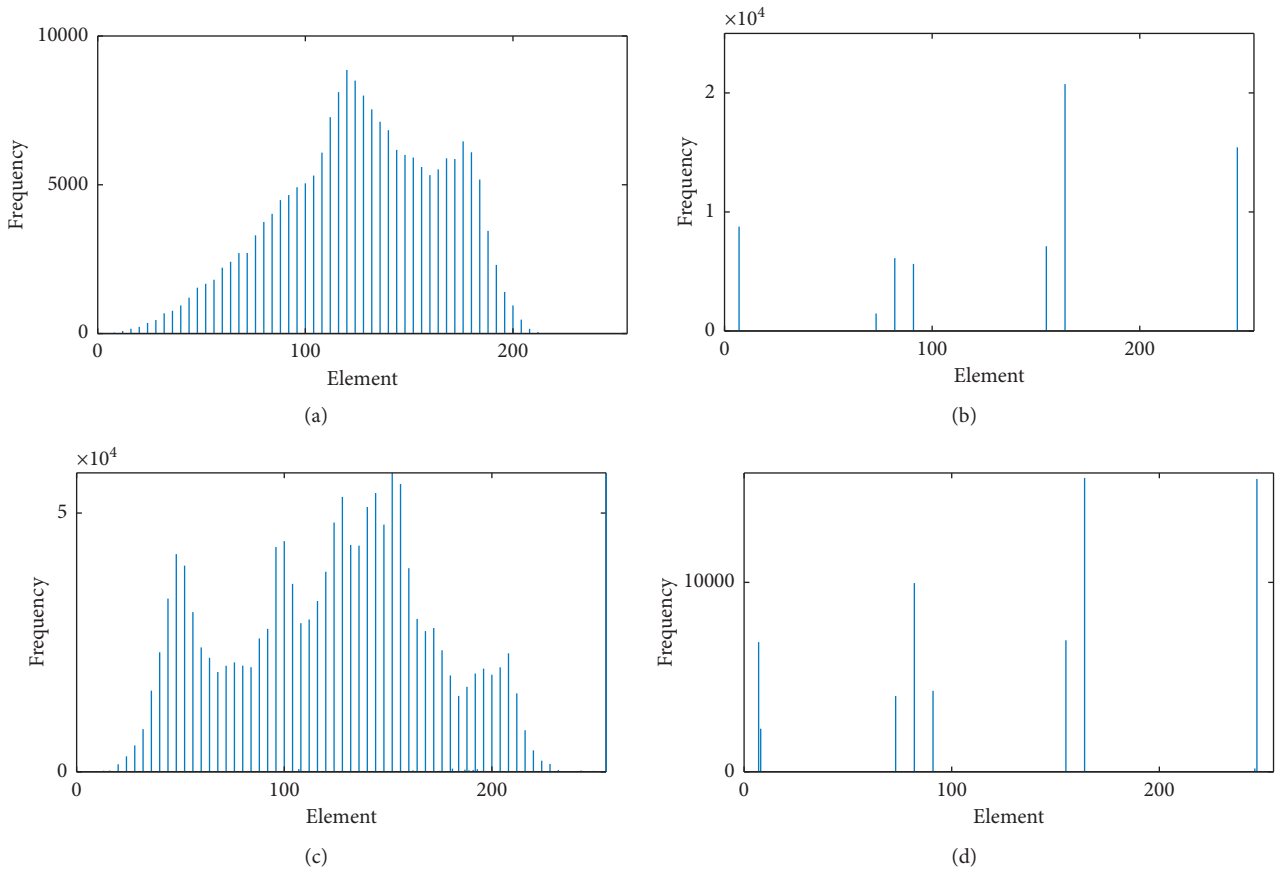


Figure 13: (a) Histogram of the original image Lena. (b) Histogram of the encrypted image Lena. (c) Histogram of the original image Baboon. (d) Histogram of the encrypted image Baboon.

Table 8: Correlation coefficients analysis.

Image	Direction	Plain image	Encrypted image	Ref. [57]	Ref. [79]	Ref. [80]	Ref. [81]
Lena	Horizontal	0.77724	−0.0045	−0.0031	−0.0084	−0.0124	0.0519
	Vertical	0.84858	0.0004	−0.0293	−0.0017	−0.0038	−0.0385
	Diagonal	0.7369	−0.0194	−0.0077	−0.0194	−0.0090	0.0046
Baboon	Horizontal	0.52256	−0.148	0.0224	—	—	—
	Vertical	0.51042	0.0060	0.0115	—	—	—
	Diagonal	0.41989	0.0069	−0.0025	—	—	—

are two widely used metrics to evaluate the strength of the image encryption algorithm (or cipher) under differential attack. Assuming that the encrypted image after the pixel change of the original plaintext image is P and T, respectively; then, the pixel values at (i, j) in P and T are expressed as $P(i, j)$ and $T(i, j)$, and their bipolar array is expressed as equation (10). Then, NPCR and UACI can be defined by equations (11) and (12). For the reconstruction of the four-bit layer image, the results of NPCR and UACI are ideal and the results are shown in Table 9:

$$\Delta(i, j) = \begin{cases} 0, & \text{if } P(i, j) = T(i, j), \\ 1, & \text{if } P(i, j) \neq T(i, j), \end{cases} \tag{10}$$

$$\text{NPCR: } N(P, T) = \sum_{i,j} \frac{\Delta(i, j)}{T} \times 100\%, \tag{11}$$

$$\text{UACI: } U(P, T) = \sum_{i,j} \frac{|P(i, j) - T(i, j)|}{255 \times \text{MN}} \times 100\%. \tag{12}$$

5.3.4. Entropy Analysis. Information entropy is a measure of system complexity and reflects the randomness of system information. If the system information is more complex and there are more types of different situations, then its information entropy is relatively large [82], and its value can be calculated by equation (13). For an 8-bit gray level image, the closer it is to 8 bits, the less likely the algorithm is to leak information:

$$H_m = \sum_{i=0}^{n} p(m_i) \log \frac{1}{p(m_i)}. \tag{13}$$

In Table 10, we can see that the entropy of the plaintext image is relatively low, and the entropy of the encrypted image is close to 8. In the information entropy of the two images, compared with [57, 83–85], the entropy of the encrypted image generated by our proposed algorithm is close to 8 bits.

6. Conclusion

In this paper, a new PRNG method is proposed by coupling three kinds of FWMHSs with different dimensions. The security of the generated chaotic pseudo-random sequence is analyzed. The results show that the random number generated by the proposed method has good statistical characteristics, including large enough key space and excellent key sensitivity, and the generated random number sequence can pass NIST and ENT randomness detection. As a typical application of PRNG, an image encryption algorithm based on PRNG using three kinds of FWMHSs different dimensions as a multientropy source is proposed. The results of encryption and decryption, security analysis, and anti-differential attack ensure the effectiveness of the algorithm, and the pixel correlation of encrypted image tends to zero. Finally, the performance comparison with the existing encryption algorithms shows that the proposed image encryption algorithm based on the proposed PRNG can be effectively applied in cryptography.

Table 9: NPCR and UACI test results for the two images reported in the experiments.

Image	Lena	Baboon
NPCR (%)	83.4564	83.2596
UACI (%)	34.6828	34.7289

Table 10: Information entropy.

Image	Lena	Baboon
Proposed	7.9972	7.9971
Ref. [57]	7.9993	7.9993
Ref. [83]	7.9972	7.9025
Ref. [84]	7.8683	—
Ref. [85]	7.9030	7.9026

Data Availability

All 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, 61901169, and 61674054; the Natural Science Foundation of Hunan Province under Grants 2019JJ50648, 2020JJ4622, 2019JJ40190, and 2020JJ4221; the Guangxi Key Laboratory of Cryptography and Information Security under Grant GCIS201919; the Postgraduate Training Innovation Base Construction Project of Hunan Province under Grant 2020-172-48; the Postgraduate Scientic Research Innovation Project of Hunan Province under Grant CX20200884; the

Scientific Research Fund of Hunan Provincial Education Department under Grant 18A137; and the Young Teacher Development Program Project of Changsha University of Science and Technology under Grant 2019QJCZ013.

References

[1] W. Z. Wang, X. Q. Wang, J. Wang, N. N. Xiong, S. Cai, and P. Liu, "Ensuring cryptography chips security by preventing scan-based side-channel attacks with improved DFT architecture," *IEEE Transactions on Systems, Man and Cybernetics: Systems*, 2020.

[2] Z. Xia, Z. Fang, F. Zou, J. Wang, and A. K. Sangaiah, "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.

[3] K. Gu, X. Dong, and W. Jia, "Malicious node detection scheme based on correlation of data and network topology in fog computing-based VANETs," *IEEE Transactions on Cloud Computing*, p. 1, 2020.

[4] J.-L. Zhang, W.-Z. Wang, X.-W. Wang, and Z.-H. Xia, "Enhancing security of FPGA-based embedded systems with combinational logic binding," *Journal of Computer Science and Technology*, vol. 32, no. 2, pp. 329–339, 2017.

[5] C. Yin, X. Ju, Z. Yin et al., "Location recommendation privacy protection method based on location sensitivity division," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 266, 2019.

[6] Z. Min, G. Yang, J. Wang et al., "A privacy-preserving BGN-type parallel homomorphic encryption algorithm based on LWE," *Journal of Internet Technology*, vol. 20, no. 7, pp. 2189–2200, 2017.

[7] N. Liao, Y. Song, S. Su, X. Huang, and H. Ma, "Detection of probe flow anomalies using information entropy and random forest method," *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 1, pp. 433–447, 2020.

[8] K. Gu, N. Wu, B. Yin, and W. Jia, "Secure data query framework for cloud and fog computing," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 332–345, 2020.

[9] D. Cao, Y. Jiang, J. Wang et al., "ARNS: adaptive relay-node selection method for message broadcasting in the internet of vehicles," *Sensors*, vol. 20, no. 5, p. 1338, 2020.

[10] A. V. Tutueva, E. G. Nepomuceno, A. I. Karimov, V. S. Andreev, and D. N. Butusov, "Adaptive chaotic maps and their application to pseudo-random numbers generation," *Chaos, Solitons & Fractals*, vol. 133, Article ID 109615, 2020.

[11] F. Yu, L. Li, Q. Tang et al., "A survey on true random number generators based on chaos," *Discrete Dynamics in Nature and Society*, vol. 2019, Article ID 2545123, 10 pages, 2019.

[12] Y. Wang, Z. Liu, J. Ma, and H. He, "A pseudorandom number generator based on piecewise logistic map," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2373–2391, 2016.

[13] Q. L. Deng, C. H. Wang, and L. M. Yang, "Four-wing hidden attractors with one stable equilibrium point," *International Journal of Bifurcation and Chaos*, vol. 30, no. 6, Article ID 2050086, 2020.

[14] R. Wu and C. Wang, "A new simple chaotic circuit based on memristor," *International Journal of Bifurcation and Chaos*, vol. 26, no. 9, Article ID 1650145, 2016.

[15] F. Yu, H. Shen, L. Liu et al., "CII 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.

[16] F. Yu, L. Liu, H. Shen et al., "Multistability analysis, coexisting multiple attractors and FPGA implementation of Yu-Wang four-wing chaotic system," *Mathematical Problems in Engineering*, vol. 2020, Article ID 7530976, 16 pages, 2020.

[17] Q. L. Deng and C. H. Wang, "Multi-scroll hidden attractors with two stable equilibrium points," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, no. 9, Article ID 093112, 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] 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, no. 24, pp. 264–275, 2019.

[20] W. Yao, C. Wang, Y. Sun, C. Zhou, and H. Lin, "Synchronization of inertial memristive neural networks with time-varying delays via static or dynamic event-triggered control," *Neurocomputing*, vol. 404, pp. 367–380, 2020.

[21] C. Zhou, C. H. Wang, Y. C. Sun, and W. Yao, "Weighted sum synchronization of memristive coupled neural networks," *Neurocomputing*, vol. 403, pp. 225–232, 2020.

[22] Y. Li, Z. Li, M. Ma et al., "Generation of grid multi-wing chaotic attractors and its application in video secure communication system," *Multimedia Tools and Applications*, vol. 79, pp. 29161–29177, 2020.

[23] 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*, vol. 14, no. 2, pp. 2508–2519, 2020.

[24] 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.

[25] 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*, vol. 32, no. 9, pp. 4151–4160, 2020.

[26] 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.

[27] 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.

[28] Y. M. Tan and C. H. Wang, "A simple locally active memristor and its application in HR neurons," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 30, no. 5, Article ID 053118, 2020.

[29] H. Lin, C. Wang, W. Yao, and Y. Tan, "Chaotic dynamics in a neural network with different types of external stimuli," *Communications in Nonlinear Science and Numerical Simulation*, vol. 90, Article ID 105390, 2020.

[30] M. J. Barani, P. Ayubi, M. Y. Valandar et al., "A new Pseudo random number generator based on generalized Newton complex map with dynamic key," *Journal of Information Security and Applications*, vol. 53, Article ID 102509, 2020.

[31] D. Lambic and M. Nikolic, "Pseudo-random number generator based on discrete-space chaotic map," *Nonlinear Dynamics*, vol. 90, no. 1, pp. 223–232, 2017.

[32] H. S. Alhadawi, M. F. Zolkipli, D. Lambic et al., "Designing a pseudo-random bit generator based on LFSR and discrete chaotic map," *Cryptologia*, vol. 42, no. 6, pp. 1–22, 2019.

[33] X. Ye, J. Mou, C. Luo, and Z. Wang, "Dynamics analysis of Wien-bridge hyperchaotic memristive circuit system," *Nonlinear Dynamics*, vol. 92, no. 3, pp. 923–933, 2018.

[34] H. Lin, C. Wang, and Y. Tan, "Hidden extreme multistability with hyperchaos and transient chaos in a Hopfield neural network affected by electromagnetic radiation," *Nonlinear Dynamics*, vol. 99, no. 3, pp. 2369–2386, 2020.

[35] C. Wang, H. Xia, and L. Zhou, "Implementation of a new memristor-based multiscroll hyperchaotic system," *Pramana*, vol. 88, no. 2, p. 34, 2017.

[36] Q. Wan, Z. Zhou, W. Ji, C. Wang, and F. Yu, "Dynamic analysis and circuit realization of a novel no-equilibrium 5D memristive hyperchaotic system with hidden extreme multistability," *Complexity*, vol. 2020, Article ID 7106861, , 2020.

[37] Y. Zhao, C. Gao, J. Liu et al., "A self-perturbed pseudo-random sequence generator based on hyperchaos," *Chaos, Solitons & Fractals: X*, vol. 4, Article ID 100023, 2019.

[38] 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*, vol. 30, no. 10, Article ID 2050147, 2020.

[39] H. Lin, C. Wang, Y. Sun, and W. Yao, "Firing multistability in a locally active memristive neuron model," *Nonlinear Dynamics*, vol. 100, no. 4, pp. 3667–3683, 2020.

[40] F. Yu, L. Liu, H. Shen et al., "Dynamic analysis, Circuit design and Synchronization of a novel 6D memristive four-wing hyperchaotic system with multiple coexisting attractors," *Complexity*, vol. 2020, Article ID 5904607, 17 pages, 2020.

[41] X. Ma, J. Mou, J. Liu, C. Ma, F. Yang, and X. Zhao, "A novel simple chaotic circuit based on memristor-memcapacitor," *Nonlinear Dynamics*, vol. 100, no. 3, pp. 2859–2876, 2020.

[42] F. Yu, L. Liu, S. Qian et al., "Chaos-based application of a novel multistable 5D memristive hyperchaotic system with coexisting multiple attractors," *Complexity*, vol. 2020, Article ID 8034196, 19 pages, 2020.

[43] W. Yao, C. Wang, Y. Sun, C. Zho, and H. Lin, "Exponential multistability of memristive Cohen-Grossberg neural networks with stochastic parameter perturbations," *Applied Mathematics and Computation*, vol. 386, Article ID 125483, 2020.

[44] C. Wang, H. Xia, and L. Zhou, "A memristive hyperchaotic multiscroll jerk system with controllable scroll numbers," *International Journal of Bifurcation and Chaos*, vol. 27, no. 6, Article ID 1750091, 2017.

[45] H. R. Lin, C. H. Wang, Q. H. Hong, and Y. C. Sun, "A multistable memristor and its application in a neural network," *IEEE Transactions on Circuits and Systems-II: Brief Papers*, vol. 67, no. 12, pp. 3472–3476, 2020.

[46] N. A. B. N. Hashim, F. A. B. Hamid, J. Teo et al., "Analysis of Memristor based ring oscillators for hardware security," in *Proceedings of the 2016 IEEE International Conference on Semiconductor Electronics (ICSE)*, pp. 181–184, Kuala Lumpur, Malaysia, August 2016.

[47] N. A. B. N. Hashim, J. Teo, M. S. A. Hamid et al., "Implementing memristor in ring oscillators based random number generator," in *Proceedings of the 2016 IEEE Student Conference on Research and Development (SCOReD)*, pp. 1–5, Kuala Lumpur, Malaysia, December 2016.

[48] 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.

[49] B. Stoyanov and K. Kordov, "Novel secure pseudo-random number generation scheme based on two tinkerbell maps," *Advanced Studies in Theoretical Physics*, vol. 9, no. 9, pp. 411–421, 2015.

[50] M. Franois, T. Grosges, D. Barchiesi et al., "Pseudo-random number generator based on mixing of three chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 4, pp. 887–895, 2014.

[51] N. K. Pareek, V. Patidar, and K. K. Sud, "A random bit generator using chaotic maps," *International Journal of Network Security*, vol. 10, no. 1, pp. 32–38, 2010.

[52] V. Patidar, K. K. Sud, and N. K. Pareek, "A pseudo random bit generator based on chaotic logistic map and its statistical testing," *Informatica*, vol. 33, pp. 441–552, 2009.

[53] D. Lambi, A. Jankovi, and M. Ahmad, "Security analysis of the efficient chaos pseudo-random number generator applied to video encryption," *Journal of Electronic Testing*, vol. 34, no. 6, pp. 709–715, 2014.

[54] S. C. Wang, C. H. 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.

[55] C. Xu, J. Sun, and C. Wang, "An image encryption algorithm based on random walk and hyperchaotic systems," *International Journal of Bifurcation and Chaos*, vol. 30, no. 4, Article ID 2050060, 2020.

[56] 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.

[57] P. Ayubi, S. Setayeshi, and A. M Rahmani, "Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application," *Journal of Information Security and Applications*, vol. 52, Article ID 102472, 2020.

[58] C. Xu, J. Sun, and C. Wang, "A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems," *Multimedia Tools and Applications*, vol. 79, no. 9-10, pp. 5573–5593, 2020.

[59] G. Chen, C. Wang, and C. Xu, "A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing," *Multimedia Tools and Applications*, vol. 79, no. 39-40, pp. 29243–29263, 2020.

[60] J. Sun, M. Peng, F. Liu, and C. Tang, "Protecting compressive ghost imaging with hyper-chaotic system and DNA encoding," *Complexity*, vol. 2020, Article ID 8815315, 13 pages, 2020.

[61] S. M. Ismail, L. A. Said, A. G. Radwan et al., "A novel image encryption system merging fractional-order edge detection and generalized chaotic maps," *Signal Processing*, vol. 167, Article ID 107280, 2020.

[62] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. Abd EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Information Sciences*, vol. 515, pp. 191–217, 2020.

[63] B. A. Mezatio, M. T. Motchongom, B. R. Wafo Tekam, R. Kengne, R. Tchitnga, and A. Fomethe, "A novel memristive 6D hyperchaotic autonomous system with hidden extreme multistability," *Chaos, Solitons & Fractals*, vol. 120, pp. 100–115, 2019.

[64] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proceedings of the National Academy of Sciences*, vol. 88, no. 6, pp. 2297–2301, 1991.
[65] A. D. Matteis and S. Pagnutti, "Long-range correlations in linear and non-linear random number generators," *Parallel Computing*, vol. 14, no. 2, pp. 207–210, 1990.
[66] C. Chen, K. Sun, and S. He, "A class of higher-dimensional hyperchaotic maps," *The European Physical Journal Plus*, vol. 134, no. 8, p. 410, 2019.
[67] D. Peng, K. Sun, S. He, L. Zhang, and A. O. A. Alamodi, "Numerical analysis of a simplest fractional-order hyperchaotic system," *Theoretical and Applied Mechanics Letters*, vol. 9, no. 4, pp. 220–228, 2019.
[68] S. He, N. A. A. Fataf, S. Banerjee, and K. Sun, "Complexity in the muscular blood vessel model with variable fractional derivative and external disturbances," *Physica A: Statistical Mechanics and Its Applications*, vol. 526, Article ID 120904, 2019.
[69] S. He, K. Sun, and Y. Peng, "Detecting chaos in fractional-order nonlinear systems using the smaller alignment index," *Physics Letters A*, vol. 383, no. 19, pp. 2267–2271, 2019.
[70] 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*, vol. 73, pp. 146–164, 2019.
[71] D. Peng, K. H. Sun, and A. O. A. Alamodi, "Dynamics analysis of fractional-order permanent magnet synchronous motor and its DSP implementation," *International Journal of Modern Physics B*, vol. 33, no. 6, Article ID 1950031, 2019.
[72] 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.
[73] D. Zhang, Q. Li, G. Yang, L. Li, and X. Sun, "Detection of image seam carving by using weber local descriptor and local binary patterns," *Journal of Information Security and Applications*, vol. 36, pp. 135–144, 2017.
[74] J. Zhang, J. Sun, J. Wang, and X.-G. Yue, "Visual object tracking based on residual network and cascaded correlation filters," *Journal of Ambient Intelligence and Humanized Computing*, 2020.
[75] 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.
[76] J. Zhang, Z. Xie, J. Sun, X. Zou, and J. Wang, "A cascaded R-CNN with multiscale attention and imbalanced samples for traffic sign detection," *IEEE Access*, vol. 8, pp. 29742–29754, 2020.
[77] 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.
[78] R. C. Gonzalez, R. E. Woods, and S. L. Eddins, *Digital Image Processing Using MATLAB*, Publishing House of Electronics Industry, Beijing, China, 2nd edition, 2009.
[79] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.
[80] Z.-l. Zhu, W. Zhang, K.-w. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.
[81] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, 2016.
[82] A. Awad and D. Awad, "Efficient image chaotic encryption algorithm with no propagation error," *ETRI Journal*, vol. 32, no. 5, pp. 774–783, 2010.
[83] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Transactions on Nanobioscience*, vol. 16, no. 8, pp. 850–858, 2017.
[84] B. Akram, B. Oussama, H. Houcemeddine, and B. Safya, "Selective image encryption using DCT with AES cipher," in *Proceedings of the NETCOM-2014*, pp. 69–74, Chennai, India, December 2014.
[85] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "A novel image encryption scheme using the composite discrete chaotic system," *Entropy*, vol. 18, no. 8, p. 276, 2016.