



New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG

Li-Hua Gong, Hui-Xin Luo, Rou-Qing Wu, Nan-Run Zhou *

Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China



ARTICLE INFO

Article history:

Received 7 May 2021

Received in revised form 8 October 2021

Available online 23 December 2021

Keywords:

Hidden attractors
Coexisting asymmetric attractors
Circuit implementation
Random number generator
Image encryption

ABSTRACT

A new 4D chaotic system with self-excited attractors or hidden attractors is designed and the generation of self-excited attractors and hidden attractors depends on the parameters of the new 4D chaotic system. The detailed dynamical properties of the designed new 4D chaotic system have been vividly demonstrated in terms of phase portraits, bifurcation diagrams, and Lyapunov exponents. When fixing the system parameters and changing the initial value, different kinds of coexisting asymmetric attractors are discovered in the new 4D chaotic system. Besides, the corresponding analog electronic circuit of the 4D chaotic system is designed and implemented to verify its feasibility, concurrently the random number generator and an image encryption algorithm based on the designed new 4D chaotic system are provided. Then the effectiveness of the image encryption system is verified by some basic security analysis.

© 2021 Elsevier B.V. All rights reserved.

1. Introduction

As a form of motion unique to nonlinear dynamic systems, chaos is widely found in nature, such as biology [1], medicine [2], geology [3], and physics [4]. It was not until Feigenbaum found the bifurcation point structure of some simple univariable nonlinear maps has some general laws from computer experiments in 1978 that chaos aroused great interest after some universal constant appeared. In the past decades, several classical chaotic systems have been discovered, such as Lorenz's system [5], Rössler's system [6], Chua's system [7], Sprott's systems [8], Chen's system [9], etc.

From a computational point of view, attractors can be classified as self-excited attractors and hidden attractors. An attractor is called a self-excited attractor if its basin of attraction intersects with any small neighborhoods of a stationary state (an equilibrium). Otherwise, it is called a hidden attractor. A chameleon chaotic system was discovered where the chaotic attractor can vary between self-excited attractors and hidden attractors according to different parameter values [10]. The first hidden attractor was found in the generalized Chua's circuit [11,12]. The chaotic systems with hidden attractors are mainly divided into three types: systems without equilibrium points [13,14], systems with a line of equilibrium points [15,16], and systems with a stable equilibrium point [17,18]. As a new type of attractors, hidden attractors have received more and more attention. Sambas et al. found hidden attractors in a new chaotic system can generate a peanut-shaped closed equilibrium curve [19]. A fractional-order chaotic system with hidden attractors and self-excited attractors was implemented by DSP [20]. Compounding self-excited and hidden attractors could be generated

* Corresponding author.

E-mail address: nrzhou@ncu.edu.cn (N.-R. Zhou).

from the Sprott D system with a pulse control approach [21]. The graphical structure of hidden attractors was explored in the Rabinovich–Fabrikant system [22].

In recent years, the phenomenon of multiple attractors coexisting in chaotic systems has been investigated widely [23–26]. If different initial values are selected while the system parameters remain unchanged, the motion trajectory of the system may be progressively oriented to different states, such as points, periods and chaos. A fractional-order microscopic chaotic system was invented from a set of microscopic chemical reactions to produce multiple coexisting attractors [27]. The multi-stability property was found in the new 3D chaotic system equipped with a butterfly-like curve of equilibrium points [28]. A simple fourth-order memristive twin-T oscillator with coexisting attractors and antimonotonicity was reported [29]. Coexisting attractors and hidden attractors were discovered in a new chaotic system without equilibrium [30]. In a Lorenz-like system with two saddle-foci, hidden and self-excited coexisting dynamical behaviors were discussed [31]. It is worthy to notice that all the above chaotic systems generate symmetric coexisting attractors instead of coexisting asymmetric attractors, which are difficult to discover. What is more, engineering applications based on these new chaotic systems were also discussed rapidly, especially in the fields of control [32,33], image encryption [34–37], and random number generator [38–40].

Motivated by the wide focus on the hidden attractors and few discoveries about coexisting asymmetric attractors, a new 4D chaotic system with coexisting asymmetric attractors and its practical chaos-based application are provided. The proposed chaotic system is then analyzed from phase portrait, bifurcation diagram, and Lyapunov exponent. To verify the feasibility of the new 4D chaotic system, a hardware circuit is designed and realized successfully. Then it is applied into the random number generator (RNG) and image encryption algorithm.

The rest of this paper is organized as follows. In Section 2, the mathematical model of the new 4D chaotic system is described. In Section 3, some basic dynamical properties and coexisting asymmetric attractors of the new chaotic system are analyzed in detail. The designed circuit with simulation results and hardware experiment is presented in Section 4. The RNG and the image encryption algorithm are introduced in Section 5 and Section 6, respectively. Lastly, a conclusion is given in Section 7.

2. Model of the new 4D chaotic system

Rucklidge system with two nonlinear terms and two parameters was defined as [41]

$$\begin{cases} \dot{x} = -ax + by - yz, \\ \dot{y} = x, \\ \dot{z} = y^2 - z. \end{cases} \quad (1)$$

If $a = 2$ and $b = 7.7$, chaotic attractors appear in the system. Based on system (1), a new 4D chaotic system is described by

$$\begin{cases} \dot{x} = -ax + by - yz, \\ \dot{y} = x + cw^2 + e, \\ \dot{z} = y^2 - z, \\ \dot{w} = dy, \end{cases} \quad (2)$$

where $a = 2$, $b = 10$, $c = 0.1$, $d = 0.1$. Besides, system (2) yields the hidden attractor if $e \geq 0$ and generates the self-excited attractor if $e < 0$. Figs. 1 and 2 show the corresponding phase portraits of hidden attractor and self-excited attractor of system (2), respectively.

3. Dynamic properties of the new 4D chaotic system

3.1. Equilibrium point analysis

The equilibrium point of system (2) is obtained by solving

$$\begin{cases} -ax + by - yz = 0, \\ x + cw^2 + e = 0, \\ y^2 - z = 0, \\ dy = 0. \end{cases} \quad (3)$$

The equilibrium point of system (2) can be discussed from the following three cases.

Firstly, it is obvious that the chaotic attractor is hidden since there is no equilibrium point in the new system if $e > 0$.

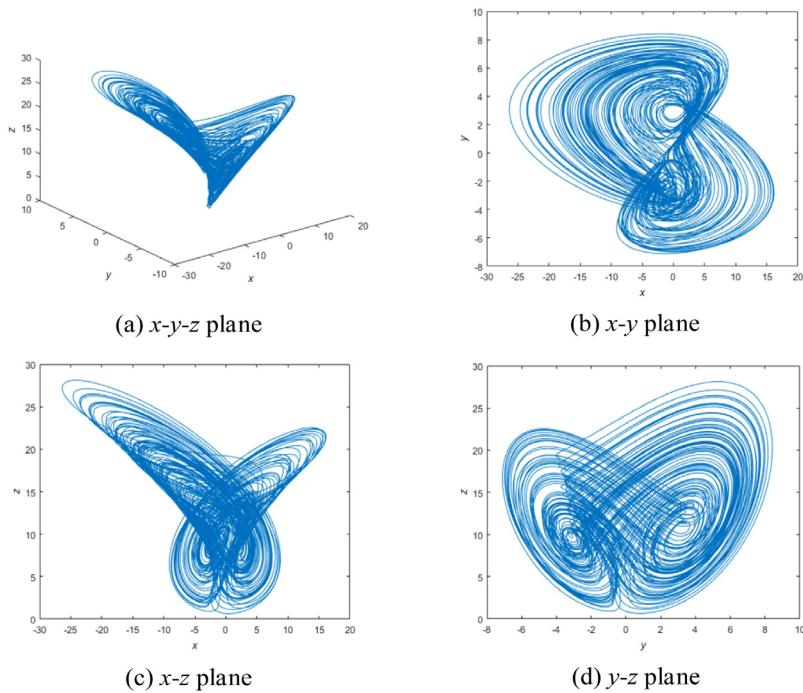


Fig. 1. Phase portraits of hidden attractors, for $a = 2$, $b = 10$, $c = 0.1$, $d = 0.1$, and $e = 0.1$.

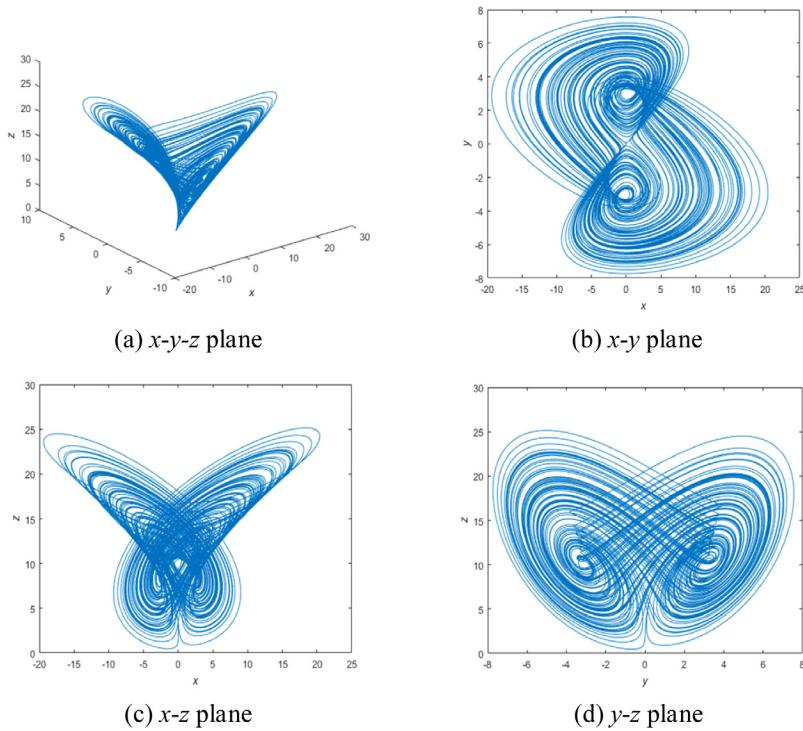


Fig. 2. Phase portraits of self-excited attractors, for $a = 2$, $b = 10$, $c = 0.1$, $d = 0.1$, and $e = -0.1$.

Secondly, the new system has only one equilibrium point $E_1(0, 0, 0, 0)$ if $e = 0$. To inspect the stability of system (2), the Jacobian matrix at the equilibrium point E_1 is expressed as

$$J = \begin{pmatrix} -a & b-z & -y & 0 \\ 1 & 0 & 0 & 2cw \\ 0 & 2y & -1 & 0 \\ 0 & d & 0 & 0 \end{pmatrix}. \quad (4)$$

Then the corresponding characteristic equation at the equilibrium point E_1 can be written as

$$\lambda [\lambda^3 + (a+1)\lambda^2 + (a-b)\lambda - b] = 0. \quad (5)$$

Eq. (5) shows that system (2) has one zero eigenvalue and three nonzero eigenvalues. If $a = 2$, $b = 10$, $c = 0.1$, and $d = 0.1$, these eigenvalues are $\lambda_1 = 0$, $\lambda_2 = -1$, $\lambda_3 = -4.3166$, and $\lambda_4 = 2.3166$. According to the Routh–Hurwitz criterion, all coefficients of the characteristic equation must be positive if the equilibrium point is stable. However, it is easy to verify that the coefficients of Eq. (5) are not all positive. Therefore, E_1 is an unstable equilibrium point.

Thirdly, system (2) has two equilibrium points $E_{2,3}(0, 0, 0, \pm\sqrt{-10e})$ if $e < 0$. The characteristic equations at the equilibrium points E_2 and E_3 are expressed as Eqs. (6) and (7), respectively.

$$\lambda^4 + (a+1)\lambda^3 + (a-b-2cd\sqrt{-10e})\lambda^2 - [b+2cd\sqrt{-10e}(a+1)]\lambda - 2acd\sqrt{-10e} = 0, \quad (6)$$

$$\lambda^4 + (a+1)\lambda^3 + (a-b+2cd\sqrt{-10e})\lambda^2 - [b-2cd\sqrt{-10e}(a+1)]\lambda + 2acd\sqrt{-10e} = 0. \quad (7)$$

If the parameters a , b , c , d and e take 2, 10, 0.1, 0.1, -1, respectively, the four eigenvalues λ_1 , λ_2 , λ_3 and λ_4 at the equilibrium point E_2 are -4.3182, 2.3222, -1 and -0.0040, respectively. It is observed that only λ_2 is positive. Thus, the equilibrium point E_2 is unstable according to the Lyapunov stability theory. At the same time, if the four eigenvalues at the equilibrium point E_3 are -4.3150, 2.3110, -1, and 0.0040, respectively, the equilibrium point E_3 is unstable.

In summary, the proposed new 4D chaotic system shows whether the attractor is self-excited or hidden depends on the parameter e . In this paper, the main focus is on the case where there is no equilibrium point in system (2).

3.2. Dissipation analysis

The vector form of the new 4D chaotic system is described as

$$\dot{\mathbf{X}} = \mathbf{f}(X) = [-ax + by - yz, x + cw^2 + e, y^2 - z, dy]^T. \quad (8)$$

Then the divergence of the new 4D chaotic system can be calculated as

$$\nabla \cdot \mathbf{f}(X) = \text{div}\mathbf{f}(X) = \frac{\partial f_1}{\partial x} + \frac{\partial f_2}{\partial y} + \frac{\partial f_3}{\partial z} + \frac{\partial f_4}{\partial w} = -a - 1, \quad (9)$$

where $a = 2$. Therefore, it is obvious to find that $\nabla \cdot \mathbf{f}(X)$ is negative.

At the time t , the volume element $V(t)$ converges to $V_0 e^{-(a+1)t}$, which means that the volume element $V(t)$ converges to zero exponentially as t approaches ∞ . Therefore, system (2) is dissipative.

3.3. Lyapunov exponent spectrum and bifurcation diagram

The Lyapunov exponent is usually used to quantitatively describe the dynamic characteristics of the chaotic attractors. For chaotic attractors, the maximal Lyapunov exponent is positive. Then two cases that the parameter e is equal to 0.1 or -0.1 are discussed.

The Lyapunov exponent spectrum versus b when $a = 2$, $c = 0.1$, $d = 0.1$, $e = 0.1$ is shown in Fig. 3(a). If $a = 2$, $b = 10$, $c = 0.1$, $d = 0.1$, $e = 0.1$, and the initial values are (0.01, 0, 0, 0.01), the Lyapunov exponents of system (2) can be calculated with Wolf's algorithm [42] as: $L_1 = 0.2629$, $L_2 = 0$, $L_3 = -0.0039$, and $L_4 = -3.2630$. The Kaplan–Yorke dimension of a chaotic system is defined as [43]

$$D_L = k + \frac{1}{|L_{k+1}|} \sum_{j=1}^k L_j, \quad (10)$$

where k is the largest number to satisfy $\sum_{j=1}^k L_j \geq 0$. According to Eq. (10), the corresponding Kaplan–Yorke dimension of the new 4D chaotic system is 3.0794.

Bifurcation diagram is a useful tool to analyze the dynamic characteristics of a chaotic system. To demonstrate the dynamic behaviors of system (2), the bifurcation diagram versus parameter b is shown in Fig. 3(b). Apparently, that the bifurcation diagram is consistent with the analysis results of the Lyapunov exponent spectrum. If the parameter b is between 4.7 and 15, the system will be in a chaotic state.

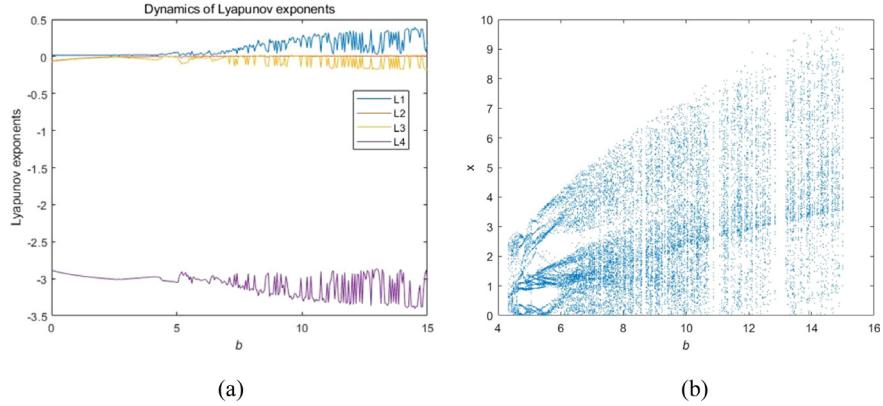


Fig. 3. Dynamics of hidden attractors versus b : (a) Lyapunov exponent spectrum (b) corresponding bifurcation diagram.

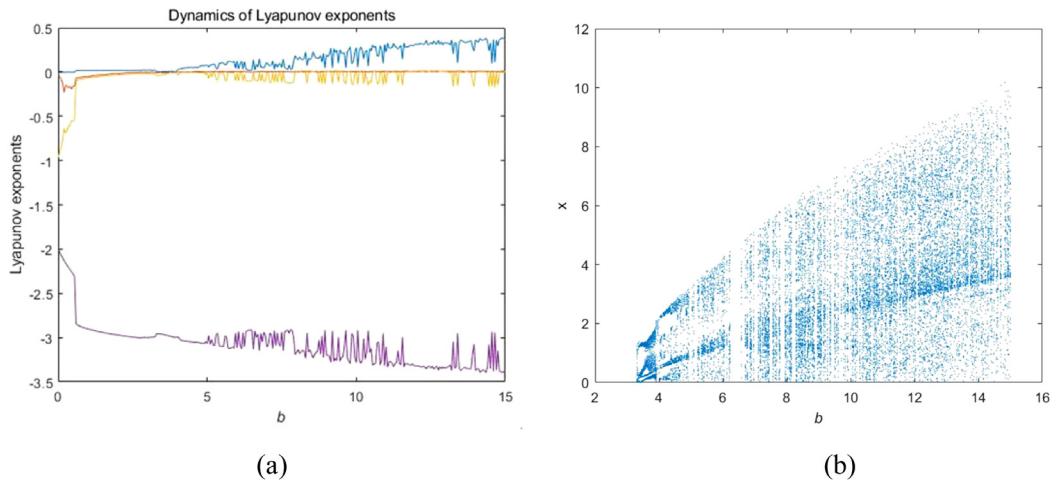


Fig. 4. Dynamics of self-excited attractors versus b : (a) Lyapunov exponent spectrum (b) corresponding bifurcation diagram.

When the parameter b varies from 4 to 15 under the case that $a = 2$, $c = 0.1$, $d = 0.1$, $e = -0.1$, the Lyapunov exponent spectrum is shown in Fig. 4(a). For $a = 2$, $b = 10$, $c = 0.1$, $d = 0.1$, $e = -0.1$, and the initial values are $(0.01, 0, 0, 0.01)$, the Lyapunov exponents of system (2) are $L_1 = 0.2757$, $L_2 = 0.0058$, $L_3 = 0$, and $L_4 = -3.2840$. What is more, the corresponding Lyapunov dimension of the new 4D chaotic system is 3.0857 in this case. The bifurcation diagram is given in Fig. 4(b). From the Lyapunov exponent spectrum and the bifurcation diagram, one can see that system (2) will be in a chaotic state at the same value of parameter b under the same condition.

In short, according to the definition of chaotic attractors, the new 4D chaotic system in two cases is both chaotic since there exists one positive Lyapunov exponent and the Lyapunov dimension is fractional.

3.4. Coexisting asymmetric attractors

The coexistence of attractors means that different initial values make the system enter different tracks and generate different chaotic attractors when the system parameters are fixed. Therefore, the trajectories of different attractors do not overlap on the plane of phase portraits. Most coexisting attractors generally have symmetry, and some coexisting attractors are left and right or up and down symmetric. However, coexisting asymmetric attractors are rarely found or often ignored, since they appear in a narrow regions of the parameter space.

Under different initial values, the bifurcation diagram of the new 4D chaotic system is shown in Fig. 5(a), where the blue and the red color correspond to initial values $(0, 0, 0, 1)$ and $(0, 0, 0, -1)$, respectively. It means that there exist coexisting attractors. What is more, the basins of attraction of the 4D chaotic system are exhibited in Fig. 5(b). It can be observed that system (2) has different kinds of the basins of attractions when the initial conditions are different.

To observe this phenomenon in system (2), one sets five parameters $a = 2$, $b = 4.8$, $c = 0.1$, $d = 0.1$, $e = 0.1$, and initial values $IV_1 = (0, 0, 0, 1)$, $IV_2 = (0, 0, 0, -1)$, respectively. The phase portraits of diverse coexisting

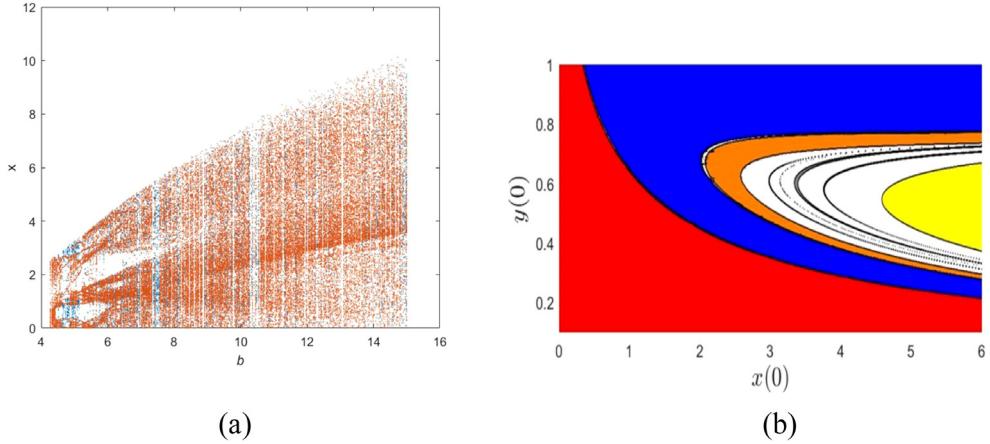


Fig. 5. (a) Bifurcation diagram of system (2) when fixing the initial value $(0, 0, 0, 1)$, $(0, 0, 0, -1)$ and changing the parameter b (b) basins of attraction on the plane $x(0) - y(0)$ of system (2) when $z(0) = 0$, $w(0) = -1$.

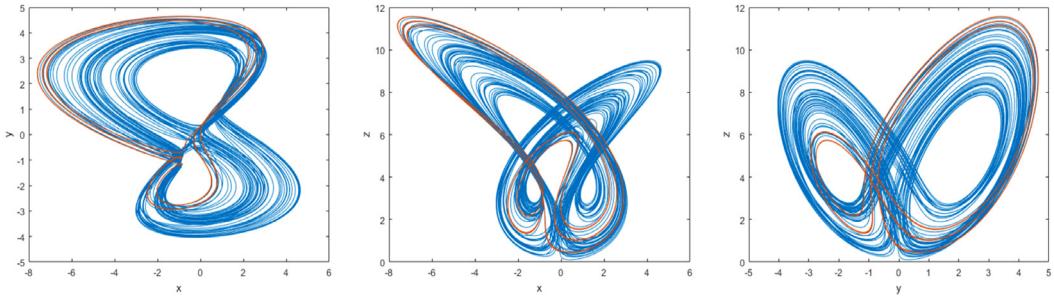


Fig. 6. Coexisting attractors and limit cycle in system (2) for $a = 2$, $b = 4.8$, $c = 0.1$, $d = 0.1$, $e = 0.1$, and two different initial values $\text{IV}_1 = (0, 0, 0, 1)$ (blue) and $\text{IV}_2 = (0, 0, 0, -1)$ (red).

asymmetric attractors are shown in Fig. 6. It can be observed that a limit cycle coexists with an attractor and they have different shapes and sizes. These two attractors have different Lyapunov exponents $(0.0366, 0, -0.0134, -3.0145)$ and $(0.0110, 0, -0.0206, -2.9775)$, respectively. In addition, the time-domain waveforms corresponding to the coexisting asymmetric attractors are shown in Fig. 6 are presented in Fig. 7. As shown in Fig. 8, there are still two coexisting attractors in system (2) and they are different from those in Fig. 6, if one fixes $a = 2$, $c = 0.1$, $d = 0.1$, $e = 0.1$ while changes initial values and parameter b . It is clear that system (2) has plentiful dynamics, especially coexisting asymmetric attractors, which are rarely found in other chaotic systems. It can be seen from Figs. 6 and 8 that there are two coexisting attractors in the new 4D chaotic system, which is very sensitive to the system parameters and the initial conditions. The existence of two coexisting attractors verifies that the multistability property is associated with the occurrence of hidden attractors.

3.5. Comparison between proposed 4D chaotic system and Rucklidge system

Some dynamical properties of the new 4D chaotic system and the Rucklidge system are shown in Table 1. It demonstrates that the new 4D chaotic system has a more complex structure and it is obviously easy to find the chaotic state. What is more, the coexisting asymmetric attractors never discovered in the Rucklidge system [41] can be generated by the new 4D chaotic system. Therefore, the designed 4D chaotic system meets the publication standards of a new chaotic system defined by Sprott [44].

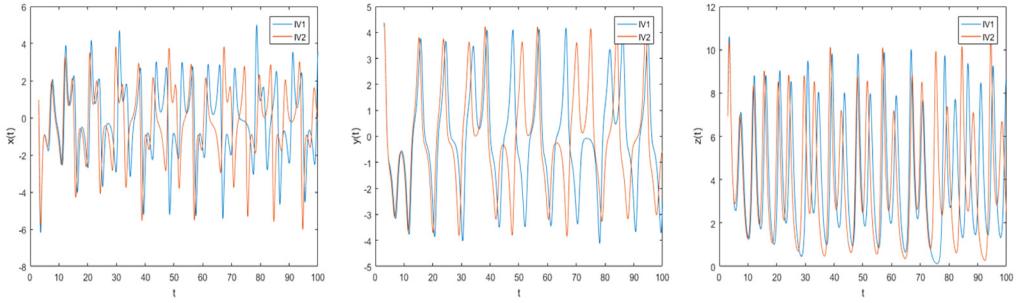


Fig. 7. The corresponding time-domain waveforms.

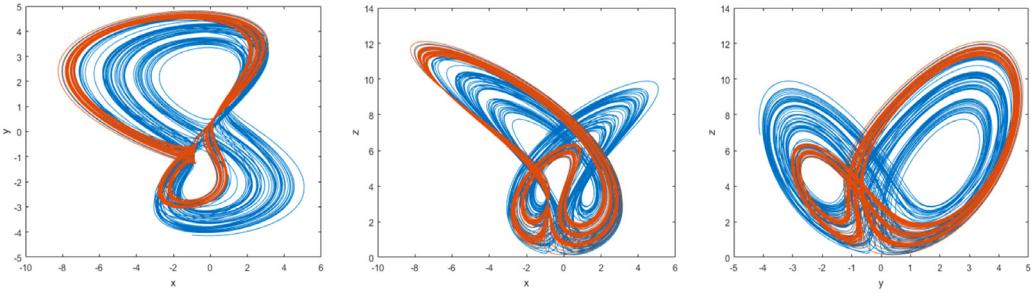
Fig. 8. Coexisting asymmetric attractors in system (2) for $a = 2$, $b = 4.88$, $c = 0.1$, $d = 0.1$, $e = 0.1$, and two different initial values $\text{IV}_1 = (0, 2, 0, 1)$ (blue) and $\text{IV}_2 = (0, -2, 0, -1)$ (red).

Table 1
Comparison of the proposed 4D chaotic system and the Rucklidge system.

System	Number of terms		Maximal Lyapunov exponents
	Linear terms	Nonlinear terms	
Proposed	6	3	0.2629
Ref. [41]	4	2	0.0643

4. Circuit implementation and experimental results

4.1. Electronic circuit design and simulation

The physical realization of a mathematical chaotic model is important in applications. Discretization may cause chaotic degradation if the chaos is generated by some digital techniques, such as FPGA and DSP. When to discuss the dynamic properties of a new chaotic system, hardware implementation is a more convincing and effective way to verify the feasibility of chaos in a true sense. Therefore, the analog electronic circuit is designed to demonstrate the feasibility of the theoretical chaotic system model.

To enhance the accuracy of the simulation and the experimental results and reduce the number of electronic components used, the improved modular circuit design method is used in this section. The power voltage of the operational amplifier is $\pm 15V$ while its saturation voltage is $\pm 13.5 V$. It can be observed that the variables in Fig. 1(c) and Fig. 1(d) have exceeded the dynamic range of $\pm 13.5 V$ for the operational amplifier. Although chaos can be simulated successfully in MATLAB, the characteristics of the operational amplifier could cause waveform distortion and a complete chaotic waveform may not be obtained. The improved modular circuit design method with compression coefficients is flexible, reliable, and straightforward to implement the physical circuit. Then it is necessary to do appropriate proportion compression transform for the dimensionless equation of system (2) first. After uniform compression of the variables by twice, for $a = 2$, $b = 10$, $c = 0.1$, $d = 0.1$, and $e = 0.1$, one can obtain

$$\begin{cases} \dot{x} = -2x - 10(-y) - 2yz, \\ \dot{y} = -(-x) - 0.2w(-w) - (-0.05), \\ \dot{z} = -2y(-y) - z, \\ \dot{w} = -0.1(-y). \end{cases} \quad (11)$$

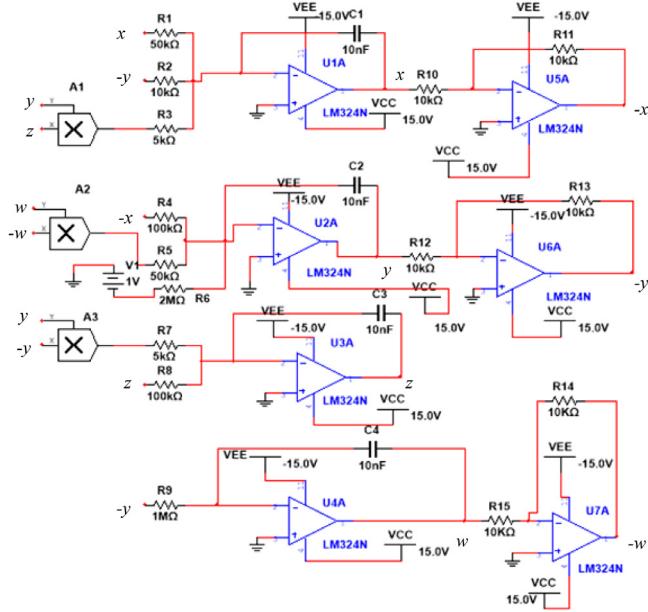


Fig. 9. Circuit schematic of system (2).

Taking the time scale transform and letting $\tau = \tau_0 t$, where $\tau_0 = 1000$ is the time scale transform factor, then Eq. (11) can be rewritten as

$$\begin{cases} \dot{x} = -2000x - 10000(-y) - 2000yz, \\ \dot{y} = -1000(-x) - 200w(-w) - (-50), \\ \dot{z} = -2000(-y) - 1000z, \\ \dot{w} = -100(-y). \end{cases} \quad (12)$$

The diagram of the chaotic circuit is shown in Fig. 9, in which the analog multipliers are AD633 with a transmission coefficient of 0.1 and the operational amplifier is LM324N. They are all supplied by $\pm 15V$ symmetric voltages. The AD633 multiplier has two inputs and one output. AD633JN versions of the AD633 four-quadrant voltage multipliers chips are adopted to implement the nonlinear terms of the mathematical model. The operational amplifiers and associated circuits perform the basic operations of subtraction, addition, integration, reverse phase. According to the schematic circuit of Fig. 9, the state equation can be expressed as

$$\begin{cases} \dot{x} = -\frac{1}{R_1 C_1}x - \frac{1}{R_2 C_1}(-y) - \frac{1}{10R_3 C_1}yz, \\ \dot{y} = -\frac{1}{R_4 C_2}(-x) - \frac{1}{10R_5 C_2}w(-w) - \frac{1}{R_6 C_2}(-V_1), \\ \dot{z} = -\frac{1}{10R_7 C_3}y(-y) - \frac{1}{R_8 C_3}z, \\ \dot{w} = -\frac{1}{R_9 C_4}(-y), \end{cases} \quad (13)$$

where the capacitor C_i is 10 nF and $V_1 = 1V$, $i = 1, 2, 3, 4$.

The whole circuit presented in Fig. 9 consists of four channels to implement the integration of the four variables x, y, z, w , respectively. In the first channel, the operational amplifiers U1 A and U5 A are used to realize the integral function and reverse phase, respectively. In the second channel, the functions of the two operational amplifiers U2 A and U6 A are also to implement the integration and inversion, respectively. In the third channel, the variable z to realize the integration function is obtained by the operational amplifier U3 A. In the last channel, the variable y is reversed and is regarded as the input of the operational amplifier U4 A to implement the integral operation. Then the output of U5 A is the inverse of the output of U4 A.

The improved modular design method does not involve the transform of the differential integral equation, while it can determine the parameters of the electronic components in the circuit by contrasting the parameters on both sides of the

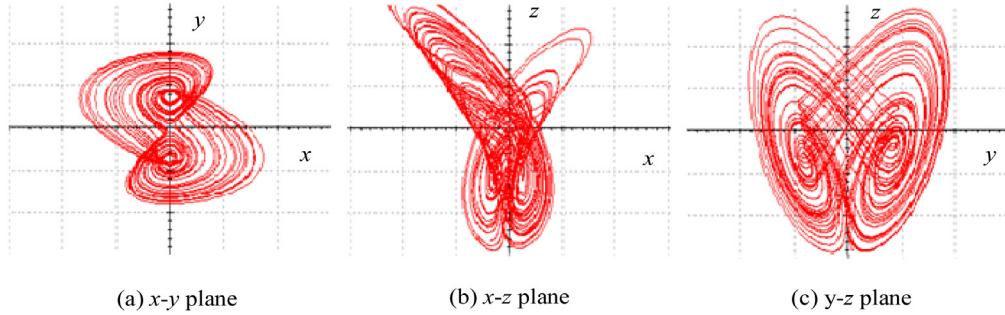


Fig. 10. Circuit simulation results on the Multisim platform.

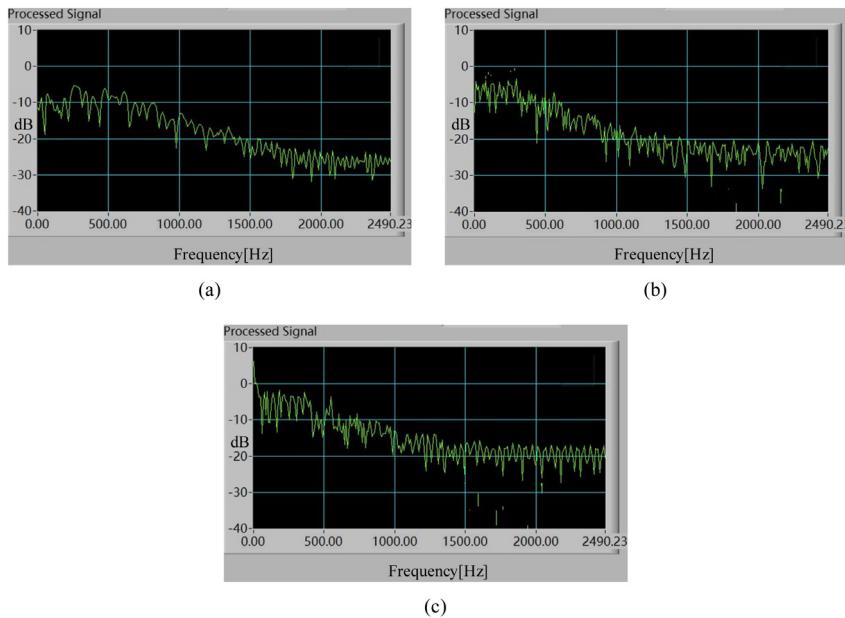


Fig. 11. Spectral distributions of the signals of the chaotic circuit: (a) signal x (b) signal y (c) signal z.

state equation. Consequently, comparing Eq. (12) with Eq. (13), one can obtain

$$\left\{ \begin{array}{l} 2000 = \frac{1}{R_1 C_1} \rightarrow R_1 = 50 \text{ k}\Omega, \quad 10000 = \frac{1}{R_2 C_1} \rightarrow R_2 = 10 \text{ k}\Omega, \\ 2000 = \frac{1}{10R_3 C_1} \rightarrow R_3 = 5 \text{ k}\Omega, \quad 1000 = \frac{1}{R_4 C_2} \rightarrow R_4 = 100 \text{ k}\Omega, \\ 200 = \frac{1}{10R_5 C_2} \rightarrow R_5 = 50 \text{ k}\Omega, \quad 50 = \frac{1}{R_6 C_2} \rightarrow R_6 = 2 \text{ M}\Omega, \\ 2000 = \frac{1}{10R_7 C_3} \rightarrow R_7 = 5 \text{ k}\Omega, \quad 1000 = \frac{1}{R_8 C_3} \rightarrow R_8 = 100 \text{ k}\Omega, \\ 100 = \frac{1}{R_9 C_4} \rightarrow R_9 = 1 \text{ M}\Omega. \end{array} \right. \quad (14)$$

The corresponding simulation phase portraits of the state variables in the circuit are shown in Fig. 10. Apparently, the simulation phase portraits in Fig. 10 are almost same as those in Fig. 1. The slight difference is caused by circuit simulation computation in Multisim. According to the definition of hidden attractors, one can infer from Fig. 10 that the new 4D chaotic system with these fixed parameters can produce hidden attractors.

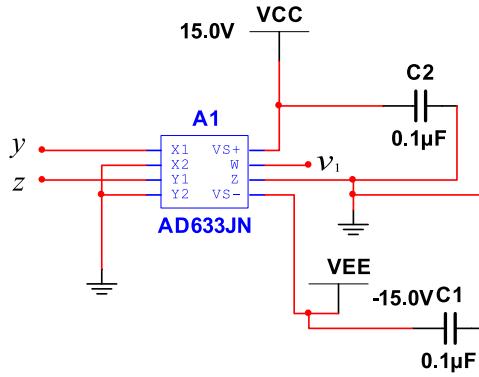


Fig. 12. Circuit implementation of v_1 .

The Fourier spectral distributions of three state variables x, y and z are shown in Fig. 11. The frequency range is 5 kHz. It is observed that the power spectra of the output signals in Fig. 11 are broadband and random, which means that the signals are chaotic.

4.2. Physical implementation

Due to the influences of element errors and other factors, the electronic simulation could not guarantee a same conclusion as the physical experiment. Therefore, it is necessary to implement the physical circuit to test the proposed chaotic system. In the realization process of the hardware circuit, to implement the state equation \dot{x} , it can be rewritten as follows:

$$\dot{x} = -\frac{1}{R_1 C_1} x - \frac{1}{R_2 C_1} (-y) - \frac{1}{R_3 C_1} \frac{yz}{10}. \quad (15)$$

For simplicity, one can define

$$v_1 \triangleq \frac{yz}{10}, \quad (16)$$

$$\dot{x} = -\frac{1}{R_1 C_1} x - \frac{1}{R_2 C_1} (-y) - \frac{1}{R_3 C_1} v_1. \quad (17)$$

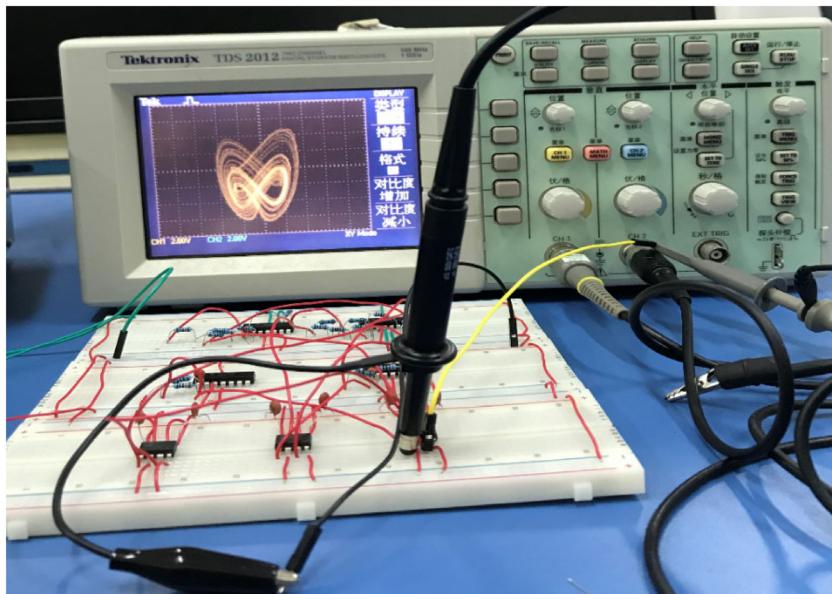
The realization of Eq. (16) is presented in Fig. 12. The output gain of AD633JN is $\frac{1}{10}$, so v_1 can be easily implemented by an AD633JN.

Eq. (17) can be implemented by one Op-Amp LM324N. LM324N is an integrated circuit with four operational amplifiers and phase compensation circuits, then two operational amplifiers of LM324N are used to perform integration and inversion, respectively. Besides, the output of one operational amplifier is variable x and the output of the other one is the opposite of variable x . The other variables y, z, w in Eq. (13) can also be obtained by the same circuit construction ideas as above.

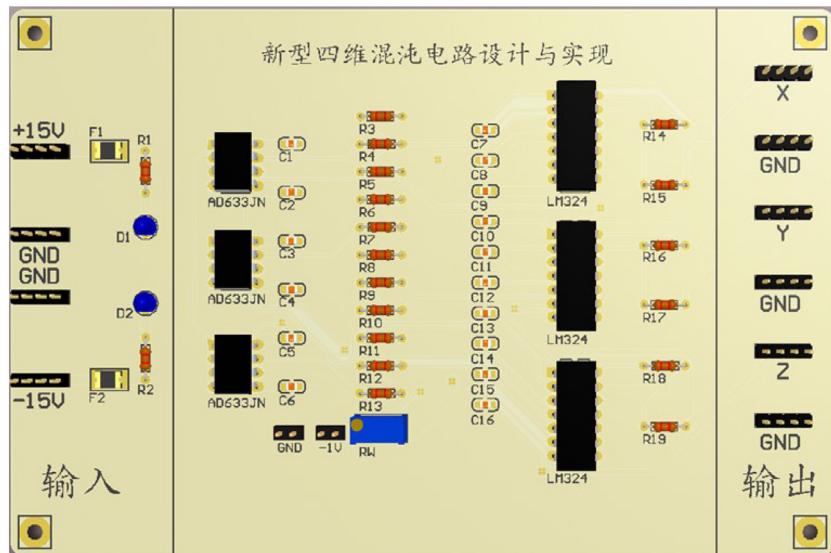
Fig. 13(a) and Fig. 13(b) show the physical implementations on the breadboard and the printed circuit board (PCB) according to the designed circuit network, as presented in Fig. 9, respectively. The hardware circuit on the breadboard consists of 3 analog multipliers AD633JN, 4 operational amplifiers LM324N, 4 capacitors with 10 nF, and 15 resistors $R_1 - R_{15}$. The resistors that met the EIA E96 standard with 1% error are adopted in the circuit building. For the chosen set of components, the parameters in system (2) are $a = 2, b = 10, c = 0.1, d = 0.1$, and $e = 0.1$.

Fig. 14 displays the experimental results observed by the digital oscilloscope (Tektronix TDS 2012) instantly with XY mode. Results in Fig. 14 are consistent with mathematical results in Fig. 1 and simulation ones in Fig. 10. Some slight differences exist in these corresponding results, since there is no initial value defined for the analog electronic circuit and the circuit is self-stimulation starting from $t = 0$ s. In addition, these differences also result from the different values of system parameters, which are determined by resistors and capacitors used in the physical circuit.

It must be pointed out that the electronic chaotic circuit is extremely sensitive to the external conditions, and will not succeed if the quality of the power supplies changes slightly. At the same time, the circuit wiring should be ensured effective and stable. Besides, it is necessary to select as few resistors as possible to form the required resistance values to reduce the circuit errors. Therefore, it is obvious that a chaotic system can be easily implemented with the help of standard circuit elements and integrated circuit connections. Then the correct results can be found immediately. In this way, the new chaotic system in Eq. (2) is implemented in the hardware circuit experiment, which matches the simulations in MATLAB and Multisim. Therefore, these results can effectively verify the feasibility and the authenticity of the new chaotic system model.



(a)



(b)

Fig. 13. Hardware circuit of system (2): (a) breadboard schematic (b) PCB schematic.

5. RNG design and NIST tests

Random number generator based on a chaotic system has many engineering applications, especially in secure communication. More importantly, these random numbers generated from chaotic systems are served as keys in the encryption process. The randomness of the generated numbers directly affects the encryption reliability. In this section, a random number generator algorithm is described.

Before being applied in digital environments, the continuous time chaotic signals must be discretized. The classical one-step fourth-order Runge–Kutta method (RK-4) is a suitable way for numerical calculation because of its high accuracy and numerical stability. Even if random numbers are generated from float values via normalization, it is quite difficult to obtain successful results and pass all the NIST tests. Therefore, the LSBs of generated binary random numbers are taken

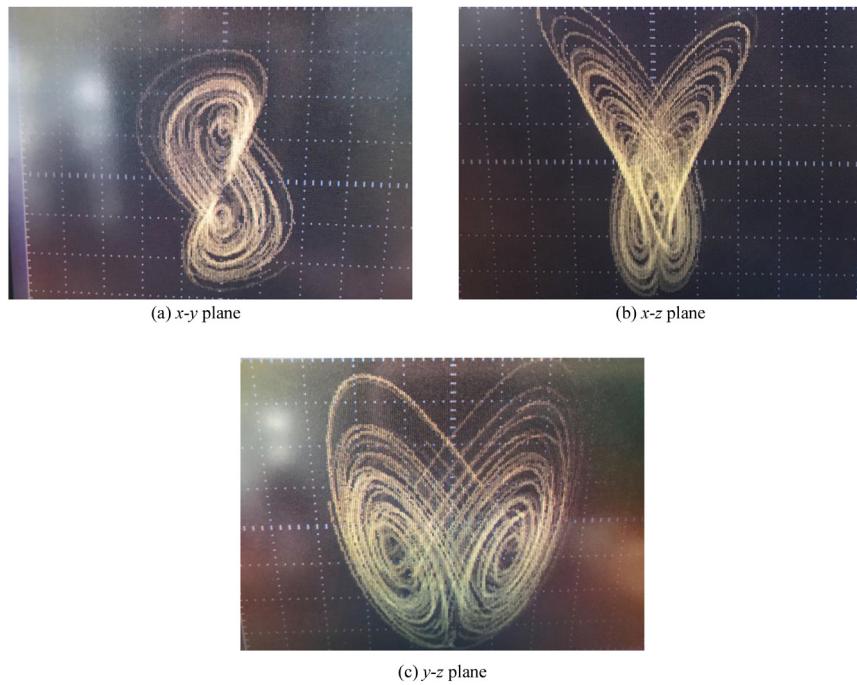


Fig. 14. Phase portraits obtained from real circuit.

and a random number generator is designed based on the new chaotic system. The pseudocode of the designed RNG is shown in Algorithm 1.

Algorithm 1 Designed RNG Algorithm Pseudocode

- 1: Start
- 2: Input the system parameters and the initial values of the new chaotic system
- 3: Determine the appropriate sampling step Δh
- 4: **while** (least 1 Mbit) **do**
- 5: Solve the new chaotic system with the RK-4 algorithm
- 6: Convert float values into 32 bits binary values
- 7: Select the 8 bits LSB from x , y , z , w phases and obtain the random number sequence

$$\text{rng+} = x(\text{LSB-8 bit}) + y(\text{LSB-8 bit}) + z(\text{LSB-8 bit}) + w(\text{LSB-8 bit})$$
- 8: **end while**
- 9: Carry out NIST tests of the obtained 1Mbit data
- 10: **if** test-results == pass **then**
- 11: Ready 1Mbit data for image encryption
- 12: **else** {test-result == fail}
- 13: Return the former steps and reset the system parameters and the initial values
- 14: **end if**
- 15: End

The results of the NIST-800-22 tests are shown in Table 2. The NIST-800-22 tests include 15 different test ways. It can be observed that the random number sequence has passed through all the NIST-800-22 tests, which implies that the sequence is random fairly.

Table 2
NIST-800-22 tests on the chaos-based RNG.

Statistical tests	Number of tests	P-value (Peppers)	P-value (Woman)	P-value (Cameraman)	Results
Frequency	1	0.18457	0.95117	0.51363	Passed
Block frequency	1	0.64515	0.65088	0.90396	Passed
Runs	1	0.74578	0.46246	0.73185	Passed
Longest-run	1	0.32962	0.59906	0.58068	Passed
Binary matrix rank	1	0.44446	0.56491	0.87301	Passed
Discrete Fourier transform	1	0.26105	0.11134	0.22339	Passed
Non-overlapping templates	148	0.99764	0.99999	0.99996	Passed
Overlapping templates	1	0.75800	0.99197	0.75801	Passed
Maurer's universal statistical	1	0.99828	0.99869	0.99476	Passed
Linear complexity	1	0.97571	0.11084	0.63850	Passed
Serial test-1	1	0.44486	0.29203	0.75506	Passed
Serial test-2	1	0.39055	0.11023	0.51342	Passed
Approximate entropy	1	0.64274	0.02039	0.86709	Passed
Cumulative sums	2	0.13852	0.94154	0.31195	Passed
Random excursions ($x = -4$)	8	0.84365	0.02093	0.14555	Passed
Random excursions variant ($x = -9$)	18	0.29104	0.20867	0.89950	Passed

6. Image encryption based on RNG

6.1. Image encryption algorithm

In this section, an image encryption algorithm based on RNG is introduced. As shown in Fig. 15, the image encryption algorithm is described as follows.

Step 1: A 256-bit hash value is generated by the SHA-256 algorithm with the sum of the first column pixel values of the original image. And then it is converted into a hexadecimal string B of length 64. There are five keys, including four initial values u_1, u_2, u_3, u_4 , and the period N of the Arnold transform. The four initial values can be obtained according to Eq. (18). The random number sequence I_1 for image encryption is obtained by substituting the initial values and the system parameters into the RNG algorithm.

$$\begin{cases} u_1 = \text{double(hex2dec}(B(1:16))/2^{65}), \\ u_2 = \text{double(hex2dec}(B(17:32))/2^{65}), \\ u_3 = \text{double(hex2dec}(B(33:48))/2^{65}), \\ u_4 = \text{double(hex2dec}(B(49:64))/2^{65}). \end{cases} \quad (18)$$

Step 2: The original image is scrambled by the Arnold transform, and the image pixel values are converted from decimal into binary values to form a scrambling image I_2 .

Step 3: The random sequence I_1 is XORed bitwise with the scrambling image I_2 . Then the obtained binary file is converted back into the decimal form, i.e., encryption image I_3 .

The operations in the decryption process are reversed from those in the encryption process.

6.2. Experimental results and analysis

The size of the images used to test the encryption algorithm is set as 256×256 . Four important initial values u_1, u_2, u_3 , and u_4 are generated by considering the pixel values of the original image as the input to the SHA-256 hash function. Therefore, the keys of the proposed image encryption algorithm with the designed 4D chaotic system are related to the original image, and the proposed image encryption algorithm can resist the known-plaintext attack and the chosen-plaintext attack effectively.

The original images, the encryption ones, and the decryption images are shown in Fig. 16. Any similar features to the original image cannot be found directly from the encryption image, while the decryption image is same as the original image visually. Thus the proposed image encryption algorithm with the designed 4D chaotic system is effective.

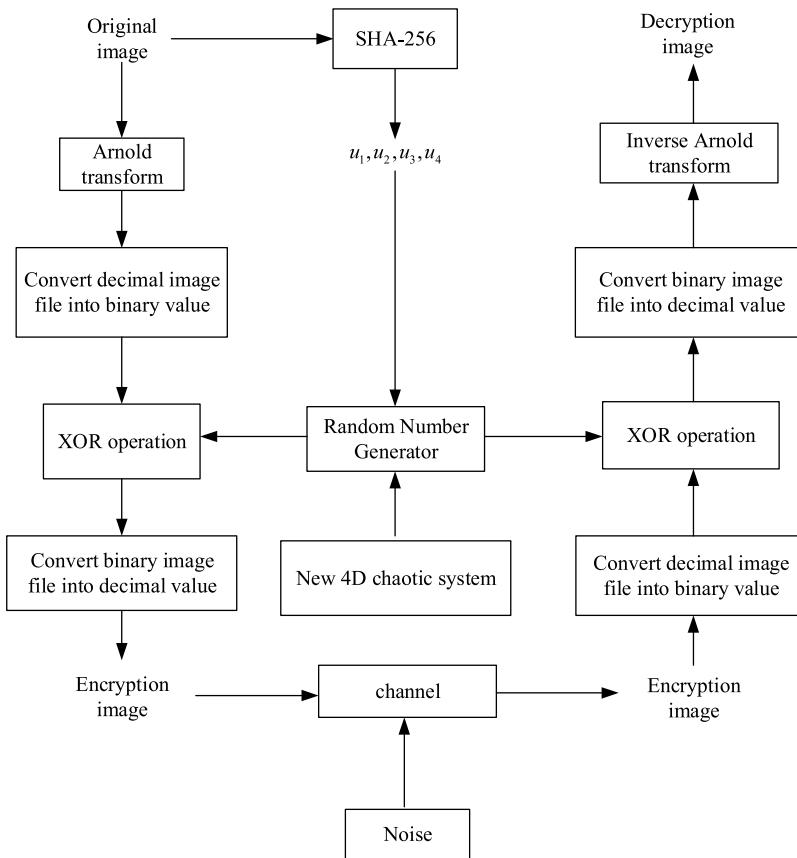


Fig. 15. Encryption and decryption processes of the proposed image encryption algorithm.

6.2.1. Histogram

An image consists of pixels of different gray values, and their distribution is an important feature of the image. And the information embodied in the encryption image can be used to analyze the ability of an image encryption algorithm to resist the statistical analysis attack. The histograms of original images (i.e., Peppers, Woman, and Cameraman) and encryption ones are shown in Fig. 17. There is no direct pixel statistical characteristic of the original images in the histograms of the encryption images, since the distributions of pixel values in encryption images are similar and almost uniform. Therefore, the proposed image encryption algorithm based on the designed 4D chaotic system can resist the statistical analysis attack effectively.

6.2.2. Correlation of adjacent pixels

Correlation coefficient is usually adopted as an important indicator to evaluate the correlation among any adjacent pixels in an image. The correlation coefficient C of adjacent pixels is defined as

$$C = \frac{\sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^N (x_i - \bar{x})^2 \times \sum_{i=1}^N (y_i - \bar{y})^2}}, \quad (19)$$

where $\bar{x} = \frac{1}{N} \sum_{i=1}^N x_i$ and $\bar{y} = \frac{1}{N} \sum_{i=1}^N y_i$, x_i and y_i are the gray values of two adjacent pixels in the same image. Table 3 shows the horizontal (H), vertical (V) and diagonal (D) correlation coefficients of different test images. It can be seen that these correlation coefficient values are small or near zero, which means that the correlation between adjacent pixels of the encryption images is weakened macroscopically. Fig. 18 shows the correlation distribution between two horizontally adjacent pixels in original image and encryption one. The horizontal distribution of any two pixels in the test images is mainly centered around the angle bisector, while the pixel distribution of the encryption images tends to be uniform. It illustrates that the presented image encryption algorithm based on the designed 4D chaotic system can counteract the statistical analysis attack effectively.

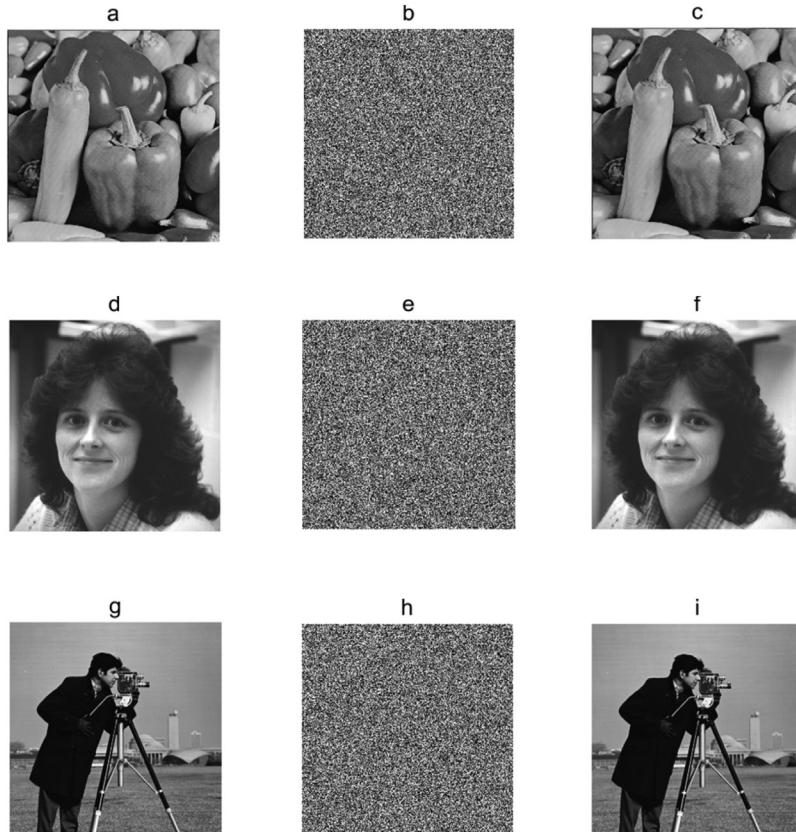


Fig. 16. Test results: (a), (d) and (g) are the original images, (b), (e) and (h) are corresponding encryption images, (c), (f) and (i) are corresponding decryption images.

Table 3
Correlation coefficients of adjacent pixels.

Image	Horizontal direction	Vertical direction	Diagonal direction
Peppers	0.0057	-0.0085	0.0026
Woman	-0.0194	-0.0103	-0.0024
Cameraman	-0.0107	0.0014	-0.0066

Table 4
Information entropy (bit).

Image	Peppers	Woman	Cameraman
Information entropy	7.9974	7.9971	7.9970

6.2.3. Information entropy

Information entropy is defined as

$$H(x) = - \sum_{i=1}^N p(x_i) \log_2 p(x_i), \quad (20)$$

where $p(x_i)$ is the occurrence probability of x_i . The information entropies of ciphertext images are shown in **Table 4**. From **Table 4**, it is easy to find that the information entropies of the encryption images are all very close to the ideal value. Therefore, the proposed image encryption algorithm is strong enough to resist the differential attack.

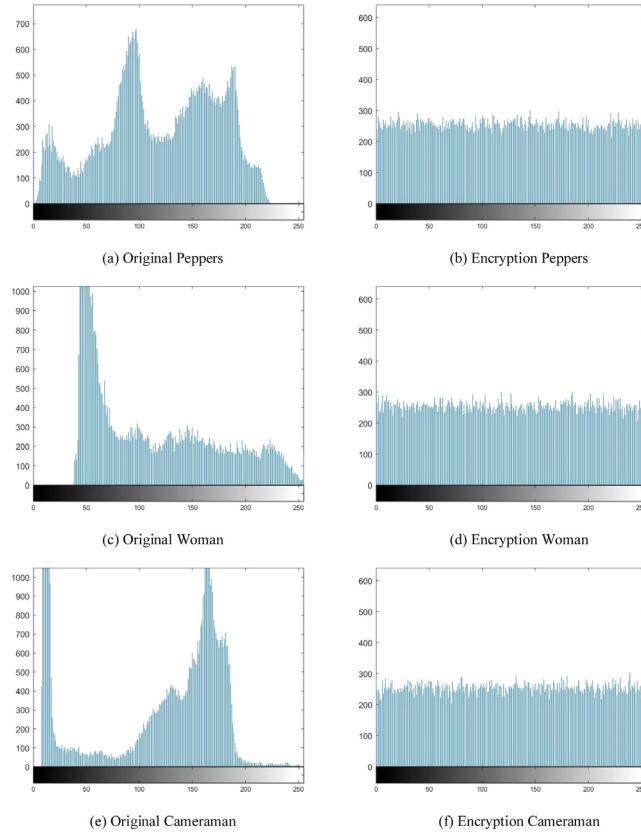


Fig. 17. Histograms of test images.

Table 5
Comparison on correlation coefficients and information entropy.

Algorithm	Correlation coefficients			Information entropy
	H	V	D	
Proposed scheme	0.0057	-0.0085	0.0026	7.9974
Ref. [35]	0.0122	0.0142	0.0139	7.9993
Ref. [37]	-0.0062	-0.0236	-0.0047	7.9971

6.2.4. Comparison

To demonstrate the effectiveness of the proposed image encryption algorithm, correlation coefficient and information entropy are compiled in [Table 5](#). Then it can be observed that the proposed image encryption algorithm has enough ability to resist the statistical analysis attack and the differential attack.

7. Conclusion

A new 4D chaotic system to generate hidden attractors or self-excited attractors depending on system parameter value is proposed. As for the hidden attractors, the designed 4D chaotic system can produce coexisting asymmetric attractors. In addition, the analog chaotic circuit is designed to realize this new system. The hardware experimental results agree with the numerical simulation results, and the feasibility of the new 4D chaotic model is verified. The random number generator and the image encryption algorithm based on the new chaotic system are presented. The random sequences generated by the random number generator with high randomness could pass the NIST tests. It is demonstrated that the image encryption algorithm suitable for gray images can resist the statistical attack and the differential attack.

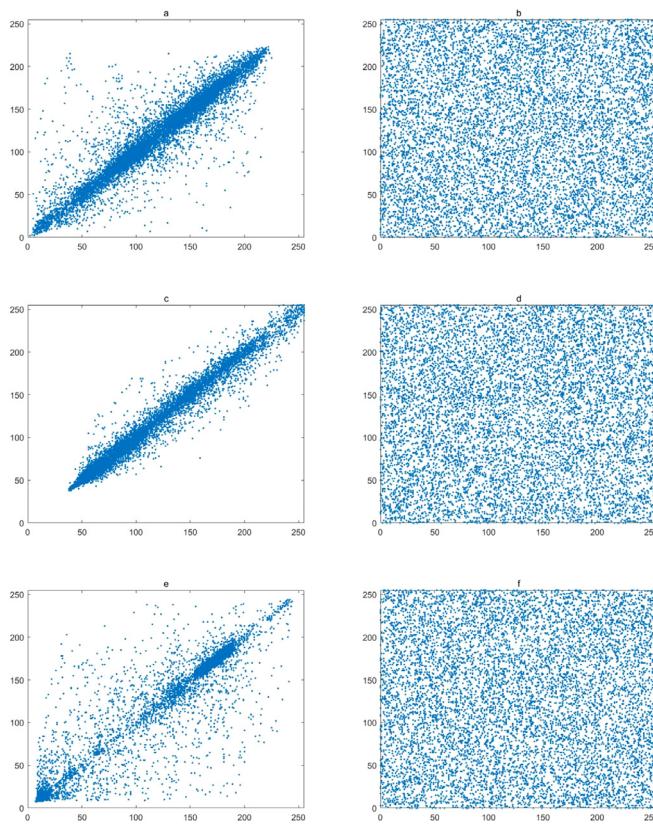


Fig. 18. Correlation distribution: (a), (b) are original “Peppers” and encryption “Peppers”, respectively. (c), (d) are original “Woman” and encryption “Woman”, respectively. (e), (f) are original “Cameraman” and encryption “Cameraman”, respectively.

In the future, a color image encryption algorithm with higher security based on the new 4D chaotic system will be discussed.

CRediT authorship contribution statement

Li-Hua Gong: Methodology, Funding acquisition, Project administration, Writing – review & editing. **Hui-Xin Luo:** Methodology, Formal analysis, Circuit design, Writing – original draft. **Rou-Qing Wu:** Methodology, Formal analysis, Validation, Writing – original draft. **Nan-Run Zhou:** Conceptualization, Resources, Supervision, Project administration, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant No. 61861029), the Major Academic Discipline and Technical Leader of Jiangxi Province, China (Grant No. 20162BCB22011), and the Natural Science Foundation of Jiangxi Province, China (Grant No. 20171BAB202002).

References

- [1] M.L. Helberg, S. Krishna, M.H. Jensen, On chaotic dynamics in transcription factors and the associated effects in differential gene regulation, *Nat. Commun.* 10 (71) (2019).
- [2] D. Dharminder, U. Kumar, P. Gupta, A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services, *Complex Intell. Syst.* 7 (3) (2021).

- [3] X.C. Li, C. Jiang, R. Xu, W. Yang, H.H. Wang, Y. Zou, Combining forecast of landslide displacement based on chaos theory, *Arab. J. Geosci.* 14 (2021) 1–10.
- [4] Y.X. Liao, A. Vikram, V. Galitski, Many-body level statistics of single-particle quantum chaos, *Phys. Rev. Lett.* 125 (2020) 250601.
- [5] E.N. Lorenz, Deterministic nonperiodic flow, *J. Atmos. Sci.* 20 (1963) 130–141.
- [6] O.E. Rössler, An equation for continuous chaos, *Phys. Lett. A* 57 (1976) 397–398.
- [7] T. Matsumoto, A chaotic attractor from Chua's circuit, *IEEE Trans. Circuits Syst.* 31 (1984) 1055–1058.
- [8] J.C. Sprott, Some simple chaotic flows, *Phys. Rev. E* 50 (1994) R647.
- [9] G. Chen, T. Ueta, Yet another chaotic attractor, *Int. J. Bifurcat. Chaos* 9 (1999) 1465–1466.
- [10] S. Mobayen, A. Fekih, S. Vaidyanathan, A. Sambas, Chameleon chaotic systems with quadratic nonlinearities: an adaptive finite-time sliding mode control approach and circuit simulation, *IEEE Access* 9 (2021) 64558–64573.
- [11] V.O. Bragin, V.I. Vagaitsev, N.V. Kuznetsov, G.A. Leonov, Algorithms for finding hidden oscillations in nonlinear systems, The Aizerman and Kalman conjectures and Chua's circuits, *J. Comput. System Sci.* 50 (2011) 511–543.
- [12] G.A. Leonov, N.V. Kuznetsov, V.I. Vagaitsev, Localization of hidden Chua's attractors, *Phys. Lett. A* 375 (2011) 2230–2233.
- [13] S. Zhang, Y. Zeng, Z. Li, M. Wang, L. Xiong, Generating one to four-wing hidden attractors in a novel 4D no-equilibrium chaotic system with extreme multistability, *Chaos* 28 (2018) 013113.
- [14] S. Zhang, X.P. Wang, Z.G. Zeng, A simple no-equilibrium chaotic system with only one signum function for generating multidirectional variable hidden attractors and its hardware implementation, *Chaos* 30 (2020) 053129.
- [15] A. Sambas, S. Vaidyanathan, S. Zhang, Y.C. Zeng, M.A. Mohamed, M. Mamat, A new double-wing chaotic system with coexisting attractors and line equilibrium: bifurcation analysis and electronic circuit simulation, *IEEE Access* 7 (2019) 115454–115462.
- [16] V.T. Pham, S. Jafari, C. Volos, L. Fortuna, Simulation and experimental implementation of a line-equilibrium system without linear term, *Chaos Solit. Fract.* 120 (2019) 213–221.
- [17] Q.L. Deng, C.H. Wang, L.M. Yang, Four-wing hidden attractors with one stable equilibrium point, *Int. J. Bifurcation Chaos* 30 (2020) 2050086.
- [18] M. Chen, C. Wang, H. Bao, X. Ren, B. Bao, Q. Xu, Reconstitution for interpreting hidden dynamics with stable equilibrium point, *Chaos Solit. Fract.* 140 (2020) 110188.
- [19] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, B. Abd-El-Atty, A.A. Abd El-Latif, O. Guillen-Fernandez, Sukono, Y. Hidayat, G. Gundara, A 3-D multi-stable system with a peanut-shaped equilibrium curve: circuit design, FPGA realization, and an application to image encryption, *IEEE Access* 8 (2020) 137116–137132.
- [20] T.M. Liu, H.Z. Yan, S. Banerjee, J. Mou, A fractional-order chaotic system with hidden attractor and self-excited attractor and its DSP implementation, *Chaos Solit. Fract.* 145 (2021) 110791.
- [21] J.L. Gao, M.J. Wang, X.N. Peng, Y.C. Zeng, Compounding self-excited and hidden attractors via a non-autonomous approach, *Eur. Phys. J.-Spec. Top.* 230 (2021) 1873–1885.
- [22] M.F. Danca, P. Bourke, N. Kuznetsov, Graphical structure of attraction basins of hidden chaotic attractors: the Rabinovich-Fabrikant system, *Int. J. Bifurcat. Chaos* 29 (2019) 1930001.
- [23] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, S. Zhang, O. Guillen-Fernandez, Sukono, Y. Hidayat, G. Gundara, A novel chaotic system with two circles of equilibrium points: multistability, electronic circuit and FPGA realization, *Electronics* 8 (2019) 1211.
- [24] C. Du, L. Liu, Z. Zhang, S. Yu, Double memristors oscillator with hidden stacked attractors and its multi-transient and multistability analysis, *Chaos Solit. Fract.* 148 (2021) 111023.
- [25] Q. Lai, Z. Wang, P.D.K. Kuata, H. Fotsin, Coexisting attractors, circuit implementation and synchronization control of a new chaotic system evolved from the simplest memristor chaotic circuit, *Commun. Nonlinear Sci. Numer. Simulat.* 89 (2020) 105341.
- [26] A. Bayani, K. Rajagopal, A.J.M. Khalaf, S. Jafari, G.D. Leutcho, J. Kengne, Dynamical analysis of a new multistable chaotic system with hidden attractor: antimonotonicity, coexisting multiple attractors, and offset boosting, *Phys. Lett. A* 383 (2019) 1450–1456.
- [27] S. He, S. Banerjee, K. Sun, Complex dynamics and multiple coexisting attractors in a fractional-order microscopic chemical system, *Eur. Phys. J. Special Top.* 228 (2019) 195–207.
- [28] A. Sambas, S. Vaidyanathan, T. Bonny, S. Zhang, Sukono, Y. Hidayat, G. Gundara, M. Mamat, Mathematical model and FPGA realization of a multi-stable chaotic dynamical system with a closed butterfly-like curve of equilibrium points, *Appl. Sci.-Basel* 11 (2021) 788.
- [29] L. Zhou, C. Wang, X. Zhang, W. Yao, Various attractors, coexisting attractors and antimonotonicity in a simple fourth-order memristive twin-T oscillator, *Int. J. Bifurcation Chaos* 28 (2018) 1850050.
- [30] Q. Lai, Z.Q. Wan, P.D.K. Kuata, Modelling and circuit realisation of a new no-equilibrium chaotic system with hidden attractor and coexisting attractors, *Electron. Lett.* 56 (2020) 1044–1046.
- [31] S. Cang, Y. Li, R. Zhang, Z. Wang, Hidden and self-excited coexisting attractors in a Lorenz-like system with two equilibrium points, *Nonlinear Dynam.* 95 (2019) 381–390.
- [32] J. Xu, N. Li, X.L. Zhang, X.L. Qin, Fuzzy synchronization control for fractional-order chaotic systems with different structures, *Front. Phys.* 8 (155) (2020).
- [33] M.A. Baloutaki, H. Rahmani, H. Moeinkhah, A. Mohammadzadeh, Non-singleton fuzzy control for multi-synchronization of chaotic systems, *Appl. Soft. Comput.* 99 (2020) 106924.
- [34] Z. Hua, Y. Zhou, H. Huang, Cosine-transform-based chaotic system for image encryption, *Inform. Sci.* 480 (2019) 403–419.
- [35] A. Shakiba, A novel randomized one-dimensional chaotic Chebyshev mapping for chosen plaintext attack secure image encryption with a novel chaotic breadth first traversal, *Multimed. Tools Appl.* 78 (2019) 34773–34799.
- [36] Y. He, Y.Q. Zhang, X.Y. Wang, A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system, *Neural Comput. Appl.* 32 (2020) 247–260.
- [37] X.Y. Wang, S.N. Chen, Y.Q. Zhang, A chaotic image encryption algorithm based on random dynamic mixing, *Opt. Laser Technol.* 138 (2021) 106837.
- [38] B. Li, X. Liao, Y. Jiang, A novel image encryption scheme based on improved random number generator and its implementation, *Nonlinear Dynam.* 95 (2019) 1781–1805.
- [39] M. Tuna, A novel secure chaos-based pseudo random number generator based on ANN-based chaotic and ring oscillator: design and its FPGA implementation, *Analog Integr. Circuits Process* 105 (2020) 167–181.
- [40] C.H. Tseng, R. Funabashi, K. Kanno, A. Uchida, C.C. Wei, S.K. Hwang, High-entropy chaos generation using semiconductor lasers subject to intensity-modulated optical injection for certified physical random number generation, *Opt. Lett.* 46 (2021) 3384–3387.
- [41] A.M. Rucklidge, Chaos in models of double convection, *J. Fluid Mech.* 237 (1992) 209–229.
- [42] A. Wolf, J.B. Swift, H.L. Swinney, J.A. Vastano, Determining Lyapunov exponents from a time series, *Phys. D Nonlinear Phenom.* 16 (1985) 285–317.
- [43] M. Cencini, F. Cecconi, A. Vulpiani, *Chaos: From Simple Models To Complex Systems*, World Scientific, Singapore, 2010.
- [44] J.C. Sprott, A proposed standard for the publication of new chaotic systems, *Int. J. Bifurcation Chaos* 21 (2011) 2391.