The Journal of Supercomputing (2024) 80:8767–8800
https://doi.org/10.1007/s11227-023-05781-4

Dynamical analysis, circuit realization, and applications of 4D hyperchaotic systems with bursty oscillations and infinite attractor coexistence

Jie Zhang[1] · Jingshun Bi[1] · Jinyou Hou[1] · Qinggang Xie[1]

Accepted: 2 November 2023 / Published online: 29 November 2023

Abstract

A new four-dimensional chaotic system with high complexity is proposed, and the analysis of its dynamics reveals that the system shows a rare topological attractor structure symmetry phenomenon. The phenomenon of inverse multiplicative bifurcation and multistability, which changes from a quadruple period to a double period and then to a single period, are found. A complex oscillatory transformation between chaos and period can be observed, highlighting the complexity of the system. The transient hyperchaos and burst oscillations are found in the time series and Lyapunov exponential spectra of the system, and the rich dynamical behavior of the system is verified by the 0–1 test and complexity spectral entropy test. The analog circuitry of the system is simulated based on Multisim, and the actual digital circuitry of the system is implemented through a Field Programmable Gate Array. The experimental results and the numerical simulation results agree and prove the feasibility of the constructed system. An image encryption algorithm is designed by combining the disruption-diffusion algorithm with the DNA encoding algorithm, and the system is analyzed and verified to be highly sensitive to the chaotic sequence key and initial value. Moreover, the key space of the algorithm is large and the information entropy is close to the ideal value, so the new system proposed can contribute to play a role in the field of secure communication.

Keywords Chaotic system · Burst oscillation · Coexistence attractor · FPGA · Image encryption

✉ Jie Zhang
zhangjie@nwnu.edu.cn

[1] College of Physics and Electronic Engineering, Northwest Normal University, Lanzhou, People's Republic of China

1 Introduction

Chaos is a form of motion unique to nonlinear dynamical systems, which is widely found in nature and many scientific fields, such as biology, physics, chemistry, geology, and so on. Chaos reveals the complexity that exists universally in nature and human society: the unity of order and disorder, the unity of certainty and probability, which opens up people's horizons and deepens their understanding of the objective world. Chaos is the inherent randomness of determinism, a world in which determinism and probability are dialectically unified. Chaotic motion is one of the most fundamental forms of motion in nature. Meteorologist Lorenz first discovered chaos in the 1960s while studying the atmosphere, and this chaos is what we know as the "butterfly effect." The 1970s was a glorious era in the history of the development of chaos science, in which chaos formally began to appear as a new independent discipline, and since then chaos science has ushered in a research boom and became a research hotspot [1–4], accompanied by the rapid development of the Internet, and chaotic systems have been widely used in pattern recognition, biomedicine, neural networks, secure communications and image encryption [5–9].

Image encryption is the application of encryption algorithms to clutter the target image so that the encrypted image cannot be recognized directly. In 1998, an image encryption scheme based on a chaotic mapping "disorder and diffusion" system [10, 11] was proposed by Fridrich. Image encryption based on chaotic mapping should have the operation of disorder and diffusion processing. In the process of disruption, only the position information of the pixel is changed without changing the size of the pixel, thus changing the correlation between neighboring pixels in the image, and in the process of diffusion, the operation is just the opposite. Liu [10] et al. proposed an image encryption algorithm based on segmented linear chaotic system encryption. M. Gao et al. [11] proposed a chaos-based permutation-diffusion image encryption algorithm, and P. Fang [12] et al. proposed a grouped image encryption algorithm based on an improved two-dimensional logistic chaotic mapping combined with DNA sequence operations [13].

Existing chaotic systems, with relatively simple structures and low complexity, use encryption methods that can achieve the purpose of image encryption, but they are single encryption. Moreover, most of them use low-dimensional chaotic systems, which are applied in image encryption, have the disadvantages of limited key space, low sensitivity, and undesirable information entropy, and are less secure in image encryption applications [14–17, 35, 36].

In order to improve the complexity of chaotic systems and security in image encryption, a new four-dimensional chaotic system is proposed. The system has a symmetric topology, which not only reduces the complexity of the system of differential equations and provides a way to simplify the problem, but also provides a better understanding of the behavior of the system by analyzing the symmetry of the system and the effect of symmetry transformations to infer the stability characteristics of the system.The system is found to have special dynamical properties not found in other systems. The system has excellent properties such as inverse multiplicative periodic bifurcation, transient hyperchaos phenomenon, sudden oscillation phenomenon, and coexisting attractor symmetry, and the system is more complex and can be applied to image encryption with higher security. Meanwhile, the comparison between the proposed system and the system shown in Table 1 also demonstrates the rich dynamic characteristics of the system. Compared with the chaotic systems in the literature [16, 17], the transient hyperchaos phenomenon demonstrates more diverse and rich dynamic behaviors of chaotic systems, and the complexity of the hyperchaos phenomenon makes it possible to be applied to data encryption and confidential transmission to provide higher security for information transmission.Bursty oscillations provide the system with different states and behavioral modes, expanding the variability and adaptability of the system to a wider range of conditions and environments. Coexisting attractor symmetries can be used to enhance the robustness of the system. Different attractors represent different signals or behavioral patterns, and by selecting specific attractors to suppress or filter noise components, the robustness of the system to noise interference can be improved. In this paper, the Longe-Kuta algorithm is used in analog circuit simulation, the Euler algorithm is used in FPGA, and in image encryption it is a combination of Arnold disruption and DNA dynamic encryption coding to design a new image encryption algorithm.

Section 2 presents a novel four-dimensional hyperchaotic system and analyzes the phase diagram of the system. Sections 3 and 4 analyze the bifurcation diagram, Lyapunov exponential spectrum, complexity, and coexisting attractors, and find that the system has special dynamical properties not found in other systems. The system has excellent properties such as inverse multiplicative periodic bifurcation, transient hyperchaos phenomenon, sudden oscillation phenomenon, and coexisting attractor symmetry. The design and simulation of the analog circuit is carried out in Sect. 5. The chaotic circuit is constructed and simulated using Multisim circuit simulation software and the simulation results are consistent with the system phase diagram. Sect. 6 designs and implements the chaotic circuit using Field Programmable Gate Array (FPGA). Section 7 performs the image encryption analysis the new system is very sensitive to the image key and the information entropy and correlation are close to ideal values. Section 8 concludes that the new system has high complexity and excellent security performance in image encryption applications.

2 Chaotic system construction

The Lorenz system is a nonlinear dynamical model proposed by American meteorologist Edward Lorenz in 1963 to describe fluid motion in the atmosphere. It is a simplified three-dimensional dynamical system represented by three variables: x, y, and z. The Lorenz system has chaotic behavior, i.e., small changes to the initial conditions may cause the system to evolve completely different trajectories. The equations of the Lorenz system are expressed as:

Table 1 Comparison of the dynamic behavior of other systems

References	The system dimension	Number of terms	Chaos or hyperchaos	Maximum Lyapunov Index	Circuit structure	Dynamic behavior
Literature [10]	4D chaotic system	4	Chaos	$LE_1=0.6790$ $LE_2=0.0063$ $LE_3=-0.0327$ $LE_4=-22.1846$	Complex	Chaotic bursting, multiple attractors coexist
Literature [11]	4D chaotic system	6	Chaos	$LE_1=0.1282$ $LE_2=0.01399$ $LE_3=-0.7456$ $LE_4=-1.0918$	Complex	multiplicative cycle bifurcation
The proposed system	4D chaotic system	5	hyperchaos	$LE_1=3.2699$ $LE_2=2.2760$ $LE_3=0.2772$ $LE_4=-11.0299$	Simple	oscillation outburst, intermittent chaos, multi-attractor coexistence, inverse doubling period bifurcation

$$\begin{cases} \frac{\mathrm{d}x}{\mathrm{d}t} = a(y - x) \\ \frac{\mathrm{d}y}{\mathrm{d}t} = bx - y - xz \\ \frac{\mathrm{d}z}{\mathrm{d}t} - cx + xy \end{cases} \tag{1}$$

We propose to introduce a nonlinear term and a sinusoidal function to present a new four-dimensional hyperchaotic system that consists of five parameters and four variables as follows:

$$\begin{cases} \frac{\mathrm{d}x}{\mathrm{d}t} = y - ax + yz \\ \frac{\mathrm{d}y}{\mathrm{d}t} = by - xz - u \\ \frac{\mathrm{d}z}{\mathrm{d}t} = xy - cz + yu \\ \frac{\mathrm{d}u}{\mathrm{d}t} = dy + e\sin(x) \end{cases} \tag{2}$$

where, x,y,z,u are the state variables of the system and $a = 3.04$, $b = 1.02$, $c = 9.02$, $d = 1$, $e = 2.02$ are the system parameters. When the system parameters are $a = 3.04$, $b = 1.02$, $c = 9.02$, $d = 1$, $e = 2.02$ when the initial value is (1,1,0,0), the system will have a complex chaos phenomenon, and at this time, the Lyapunov exponent is $LE_1 = 0.0552$ $LE_2 = 0.0114$ $LE_3 = -0.415$ $LE_4 = -10.67$, respectively. Simulation was carried out using Matlab keeping the parameters as $a = 3.04$, $b = 1.02$, $c = 9.02$, $d = 1$, $e = 2.02$ constant. The initial values are for are (1,1,0,0) Relative error tolerance and absolute error tolerance are set to le^{-7} after iteration 1000 times to get the 2D mapping of the system in four planes (x,y), (x,z), (x,u) and (y,z) as shown in Fig. 1a, b, c, and d. It can be observed that has a complex stretching and twisting structure, and from the overall view, the system is again very stable. The orbits in the figure have complex paths of vortices and the trajectories are very rich and dense with a relatively regular and simple form.

3 Analysis of the dynamics of the system

3.1 Equilibrium point

Find the equilibrium point of the system so that the right-hand side of the system equation is equal to zero. When the parameters $a = 3.04$, $b = 1.02$, $c = 9.02$, $d = 1$, $e = 2.02$, the equilibrium point of the system is (0,0,0,0). The Jacobi matrix obtained by linearizing the system:

$$J = \begin{bmatrix} -3.04 & 1 + z & y & 0 \\ -z & 1.02 & -x & -1 \\ y & x + u & -9.02 & y \\ e\cos(x) & 1 & 0 & 0 \end{bmatrix} \tag{3}$$

Let det(J − λ I) = 0, where I is the unit matrix, and find the eigenvalues $\lambda_1 = -9.0200$, $\lambda_2 = -3.1807$, $\lambda_3 = 0.5803 + 1.1199\mathrm{i}$, $\lambda_4 = 0.5803 – 1.1199\mathrm{i}$, at the

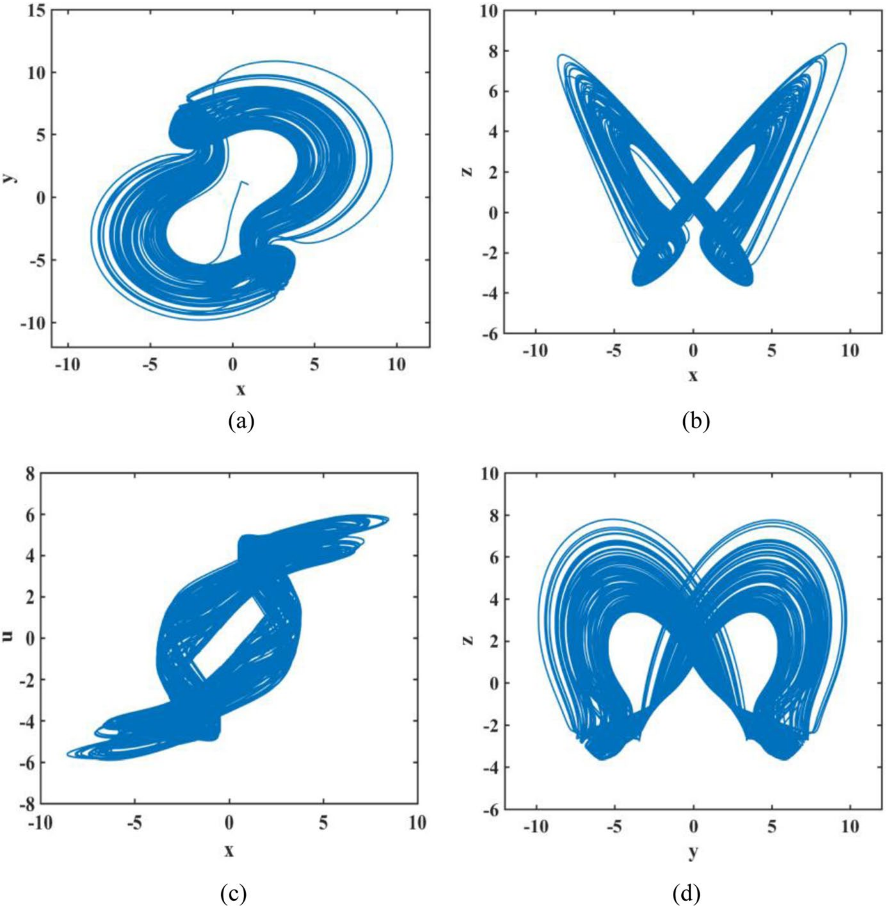


Fig. 1 Phase diagram of the system in each direction: **a** the *x*–*y* plane **b** the *x*–*z* plane **c** the *x*–*u* plane **d** the *y*–*z* plane

equilibrium point S_1(0,0,0,0). Eigenvalue analysis shows that the system has two positive eigenvalues and two negative eigenvalues, which means that the equilibrium point S_1(0,0,0,0) is an unstable saddle focus.

3.2 Dissipative nature of the system

The dispersion of the system is derived from the system equation:

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{u}}{\partial u} = -a + b - c \tag{4}$$

Substituting $a=3.04$, $b=1.02$, and $c=9.02$, gives $\nabla V=-11.04$, so the system scatter is less than 0. The system is dissipative and converges according to the exponential form $dv/dx=\mathrm{e}^{-11.02\mathrm{t}}$. As $t\rightarrow\infty$ there is a trajectory of the system that will finally be restricted to a volume of zero limit point set and its dynamical behavior will be fixed on an attractor, which is sufficient evidence for the existence of the attractor.

3.3 Lyapunov exponential spectrum and dimensionality

The Lyapunov exponent can quantitatively characterize the state of motion of a system and graphically describe the degree of mutual attraction and repulsion between neighboring trajectories of the system, which is one of the most important physical quantities to characterize chaotic systems. Therefore, using the Lyapunov exponential spectrum, it can be observed when the parameters of the system change, the motion state of the system changes accordingly can be observed. The bifurcation is that when the initial values of the variables of the state or the parameters of the system change, the dynamic state of the system changes as well. The system is a four-dimensional chaotic system. The curves shown in Fig. 2 are represented as LE_1, LE_2, LE_3, and LE_4 in order from top to bottom. When the parameters of the system are set to $a=3.04$, $b=1.02$, $c=9.02$, $d=1$, and $e=2.02$, the Lyapunov exponents of the system are calculated as $LE_1=3.26986$, $LE_2=2.27603$, $LE_3=0.277269$ and $LE_4=-11.0299$, and it can be clearly observed that the system is in a state of hyperchaos. The Lyapunov dimension of the new system is:

$$D_L = j + \frac{1}{\left|\lambda_{Lj} + 1\right|} \sum_{i=1}^{j} \lambda_{Li} = 3 + \frac{\lambda_{L1} + \lambda_{L2} + \lambda_{L3}}{\left|\lambda_{L4}\right|} = 3.5279 \tag{5}$$

The maximum Lyapunov exponent of the four-dimensional hyperchaotic system is calculated. Since the system is four-dimensional, $j=3$, the maximum Lyapunov exponent is obtained as greater than 0 and the order is not an integer, indicating that the system is chaotic. The curve of this chaotic system as the parameter changes for $a=$ [0, 5] can be seen in Fig. 6a. Observing the curves, it can be seen that when $a\in$ [0.72,0.78], [1.2,1.26], [2.85,3.1], it can be observed that there exist two Lyapunov exponents greater than zero and the system is in a hyperchaotic state. When $a=3.02$,

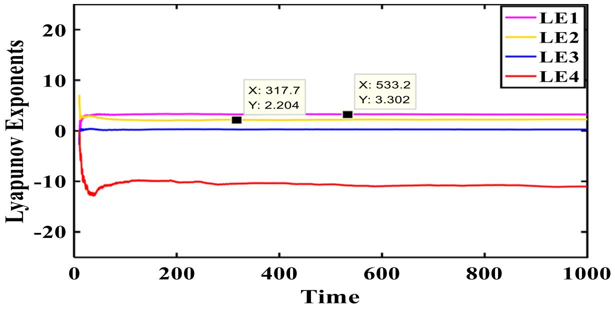


Fig. 2 Lyapunov exponent chart

it is in a hyperchaotic state. The super-mixing state has randomness and high unpredictability, making its encryption more effective and secure. There is a positive *LE* index maintained in the interval of variation of *a*. Chaotic attractors exist and are always in complex chaotic systems.

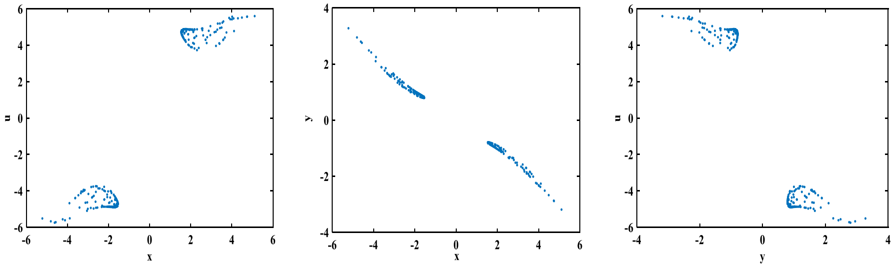
3.4 Poincaré cross section, power spectrum, 0–1 tests analysis

3.4.1 Poincaré cross section

The acyclic properties of chaotic systems can be well described by the Poincaré cross section. This observation highlights the disorderly and unpredictable behavior of the system. It is very effective for analyzing multivariate systems, where the motion is periodic when there is only one immobile point or few discrete points on the Poincaré cross section. When the Poincaré cross-section is a closed continuous curve, the motion is quasi-periodic. When the Poincaré section is a continuous curve or a patchwork of dense points, the motion is chaotic. The 2-dimensional Poincaré cross-sections in phase space are made as in (a), (b), and c in Fig. 3 to obtain in the *x*-*u*, *x*–*y*, and *y*-*u* planes, respectively. By looking at the cross-sectional view of the system, it can be found that the system is chaotic. It can also be observed that Fig. 3a and c are symmetric about the *u*-plane and Fig. 3b is symmetric about the origin. The symmetry of the Poincaré cross-section diagram allows a simpler understanding and analysis of the dynamical behavior of the system.

3.4.2 0–1 tests analysis

The basic idea of the "0–1 test" [18, 19] is to create a stochastic dynamic process for the data and then study how the size of the stochastic process varies over time. The system is observed to show an unconstrained trajectory in the (*p*, *s*) plane similar to Brownian motion, and an algorithm is used to test whether the output is close to 1 to distinguish the creation of chaos. The system is proved to be chaotic by calculating the final value of *K* (*K* = 0.9798), and the trajectory maps are drawn with *p*(n) and



(a) (b) (c)

Fig. 3 Cross-section of Poincaré in different directions: **a** *x*-*u* direction with $z = 0$ **b** *x*–*y* direction with $z = 0$ **c** *y*-*u* direction with $z = 0$

s(n) as the horizontal and vertical axes, respectively, and the steps of the algorithm whose maps produce the Brownian specific algorithm are as follows.

Define the following two equations:

$$p(n) = \sum_{j=1}^{n} \varphi(j)\cos(\theta(j)), n = 1, 2... \tag{6}$$

$$s(n) = \sum_{j=1}^{n} \varphi(j)\sin(\theta(j)), n = 1, 2... \tag{7}$$

When $\theta(j) = jc + \sum_{i=1}^{j} \varphi(j), j = 1, 2...$

The diffusion behavior of p(n) and s(n) can be analyzed by calculating the displacement mean square error M(n), which is calculated as follows.

$$M(n) = \lim_{N\to+\infty} \frac{1}{N}\sum_{j=1}^{N} \left[p(j+n) - p(j)\right]^2, n = 1, 2... \tag{8}$$

The convergence of M(n) can be used to measure the convergence of p(n) and s(n). If the discrete time series is ordered, M(n) is a bounded quantity, however, if the time series is chaotic, M(n) grows linearly in n. The convergence of M(n) is a measure of the convergence of p(n) and s(n).

Finally, the linear growth rate K, the linear regression coefficient of M(n) with n, is calculated. The asynchronous growth rate is:

$$K = \lim_{n\to+\infty} \frac{\lg M(n)}{\lg n} \tag{9}$$

By analysis, Fig. 4b shows that the motion of the system in the (p, s) plane exhibits an unbounded trajectory similar to Brownian motion, which proves that the system is a chaotic dynamical system.For example, Fig. 4a is the 0–1 test plot with

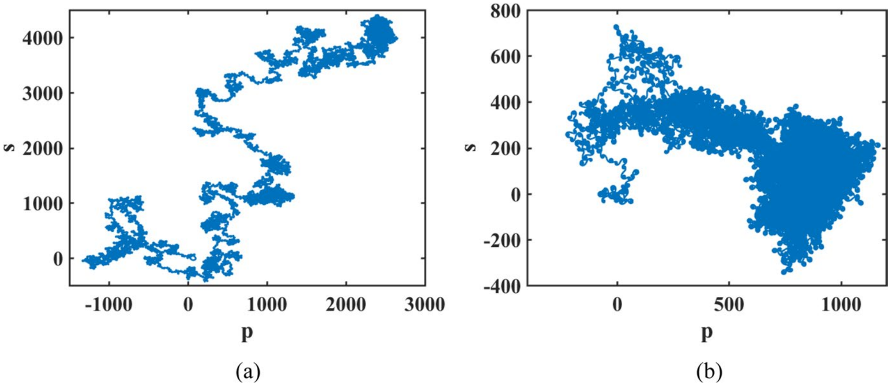


Fig. 4 Different initial values: **a** Initial values of (x_1, y_1, z_1, u_1) = (0, 1, 0, 0), **b** Initial values of (x_2, y_2, z_2, u_2) = (1, 1, 0, 0)

initial values of (x_1, y_1, z_1, u_1) = (0, 1, 0, 0), and Fig. 4b is the 0–1 test plot with initial values of (x_2, $y_{2,}$ z_2, u_2) = (1, 1, 0, 0), and the comparison between the two plots shows that (1, 1, 0, 0) is more suitable to be the initial value of this system.

3.4.3 Power spectrum

The power spectrum is a common method to analyze the chaotic behavior of a system, because chaotic systems produce chaotic signals that are non-periodic, so the power spectrum is also continuous. Figure 5 is obtained with initial values of (1, 1, 0, 0) parameters a = 3.04, b = 1.02, c = 9.02, d = 1, e = 2.02. From Fig. 5, it can be seen that the power spectrum is continuous, which indicates that the system is non-periodic, and therefore the system is chaotic.

4 Dynamical behavior of chaotic systems with changing parameters

4.1 Bifurcation diagram and Lyapunov exponential spectrum with parameters

Put *an* as a variable, and with initial values of (1,1,0,0) and step size of 0.01, only the parameter a is changed, and the rest is kept constant to observe the change of the system state. For parameters $a \in$ [0,5], keeping b = 1.02, c = 9.02, d = 1, and e = 2.02, the Lyapunov exponential spectrum and bifurcation diagram of the system are shown in Fig. 6a and b. When the parameter a is changed, periodic and chaotic regions are evident in the system. When $a \in$ [0, 0.66], the system is in a periodic state, at $a \in$ [0.7, 1.48], the system is chaotic, at $a \in$ [1.5, 2.35], the system appears again in a periodic state, when the parameter $a \in$ [2.4, 4], the system appears in a chaotic state, there are alternating chaotic and periodic changes, making its system more complex. When the parameter $a \in$ [4.2,5], the system state changes as shown in Fig. 6, it is obvious that the bifurcation diagram of the system undergoes a bifurcation where the quadruple period becomes a double period and then a bifurcation where the double period becomes a period. The emergence of multiplicative bifurcation is an important phenomenon of chaotic

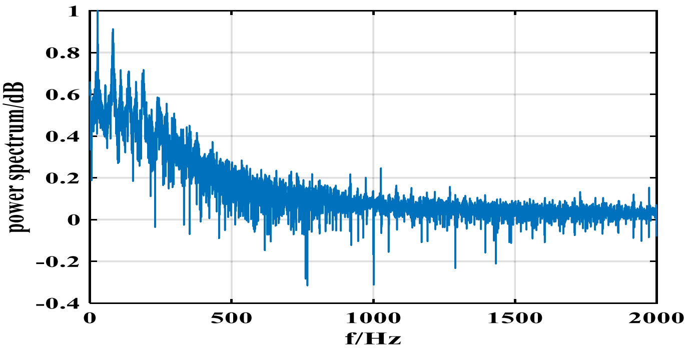
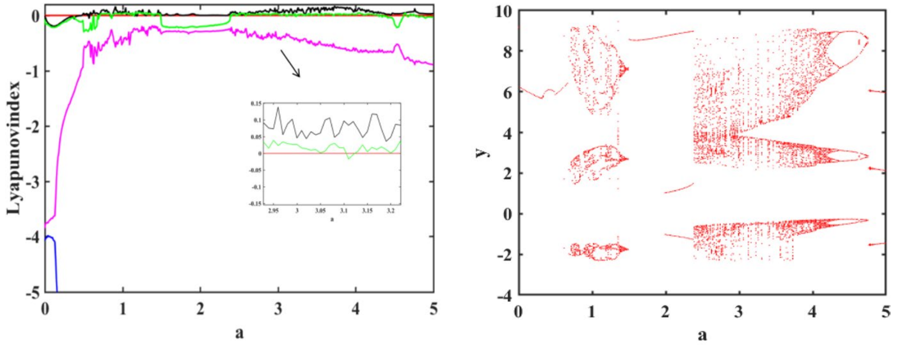


Fig. 5 Power spectrum of the system

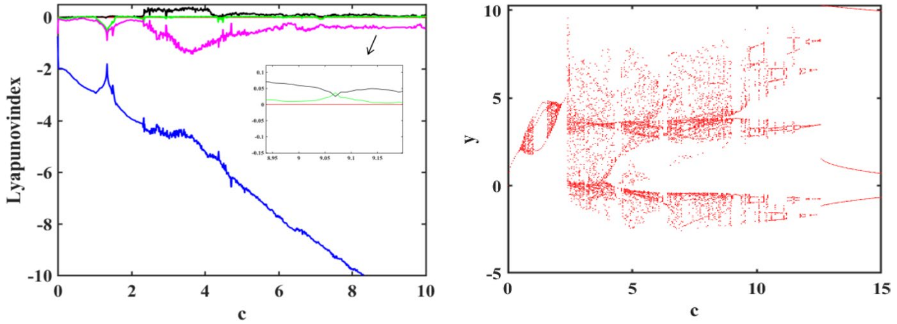


(a) (b)

Fig. 6 Lyapunov index spectrum and bifurcation diagram: **a** The Lyapunov index spectrum for parameter *a* **b** Bifurcation diagram for parameter *a*

systems, and the appearance of multiplicative bifurcation will enrich the dynamical behavior of chaotic systems and make them more diverse and complex.

For parameter c, take the parameter $c \in$ [0, 10] and set $a = 3.04$, $b = 1.02$, $d = 1$, $e = 2.02$, and the initial values of $(x_0,y_0,z_0,u_0) = (1,1,0,0)$, the bifurcation diagram and Lyapunov exponential spectrum of the system is shown in Fig. 7a and b. When $c \in$ [2.4,4.2], the system maintains a chaotic state accompanied by a transient hyperchaotic state, and when the parameter $c = 9.02$, the system has two Lyapunov exponents greater than 0, which is also hyperchaotic at this moment. The hyperchaotic state is more complex than the chaotic state, with better encryption performance and higher security. In the corresponding bifurcation diagram, in which chaos and cycles alternate with each other, the chaotic state of the system is distributed in a larger parameter space, from which it can be concluded that the system has strong randomness and a larger key space, which should be better for image encryption.

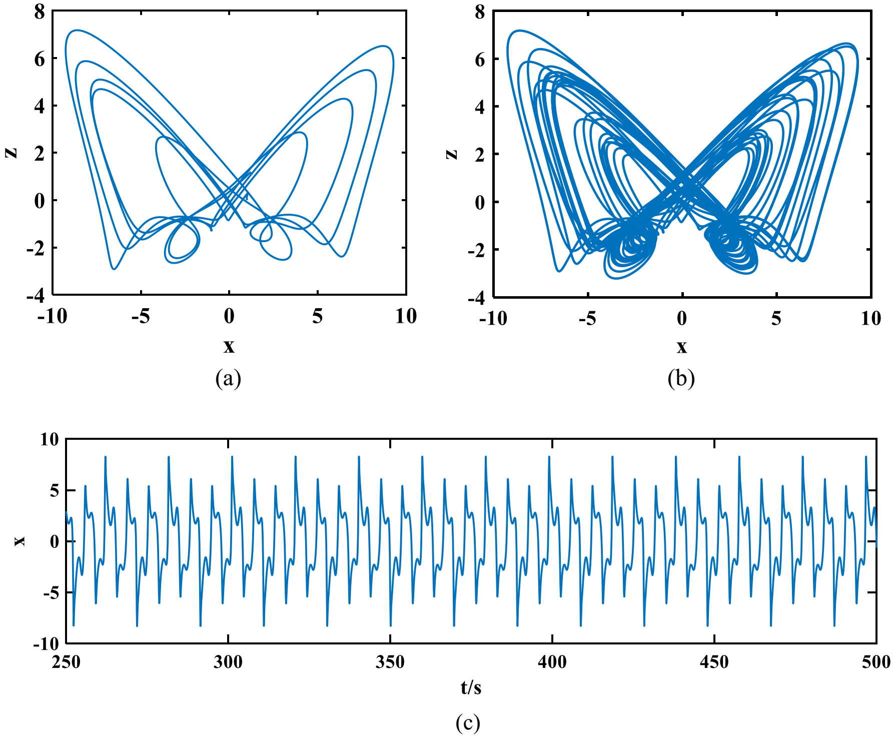


(a) (b)

Fig. 7 Lyapunov index spectrum and bifurcation diagram: **a** The Lyapunov index spectrum for parameter *c* **b** Bifurcation diagram for parameter *c*

4.2 Burst oscillations and intermittent chaos

Keeping $b = 1.02$, $c = 9.02$, $d = 1$, $e = 2.02$, when $a = 1.22$, the timing waveform is obtained for the selected time [250,500]s as shown in Fig. 8c. In Fig. 8, we can find that the attractor appears to burst oscillation, which is not easy to appear in chaotic systems. The burst oscillation can change the flatness and monotony of the timing diagram and make it more vivid and complex. Figure 8a and b show the phase diagrams when changing the time diagrams, and it can be seen that the phase diagrams change from periodic to chaotic with rich dynamical behavior. The Lyapunov exponents at this point in Fig. 8a are $LE_1 = 0$, $LE_2 = -0.0143$, $LE_3 = -0.3313$, $LE_4 = -8.5195$, and in Fig. 8b the Lyapunov exponents at this point in time are $LE_1 = 0.081$, $LE_2 = 0.0599$, $LE_3 =$-0.2723, $LE_4 = -9.0780$, respectively. Figure 9c shows the timing diagram for selected times [500,1000] s for $a = 3.3$. It can be observed that the timing diagram changes from periodic to chaotic and back to periodic, with periodic and chaotic states alternating with intermittent chaotic states. Figure 9a and b show the phase diagrams that change from periodic to chaotic. The Lyapunov exponents of Fig. 9a are $LE_1 = -0.1363$, $LE_2 = 0$, $LE_3 = -0.2617$, $LE_4 = -9.9137$. The Lyapunov exponents of Fig. 9b are



(a)

(b)

(c)

Fig. 8 Outbreak: **a** Attractor diagram of the cycle **b** Attractor diagram of the chaos **c** Timing waveform at parameter $a = 1.22$

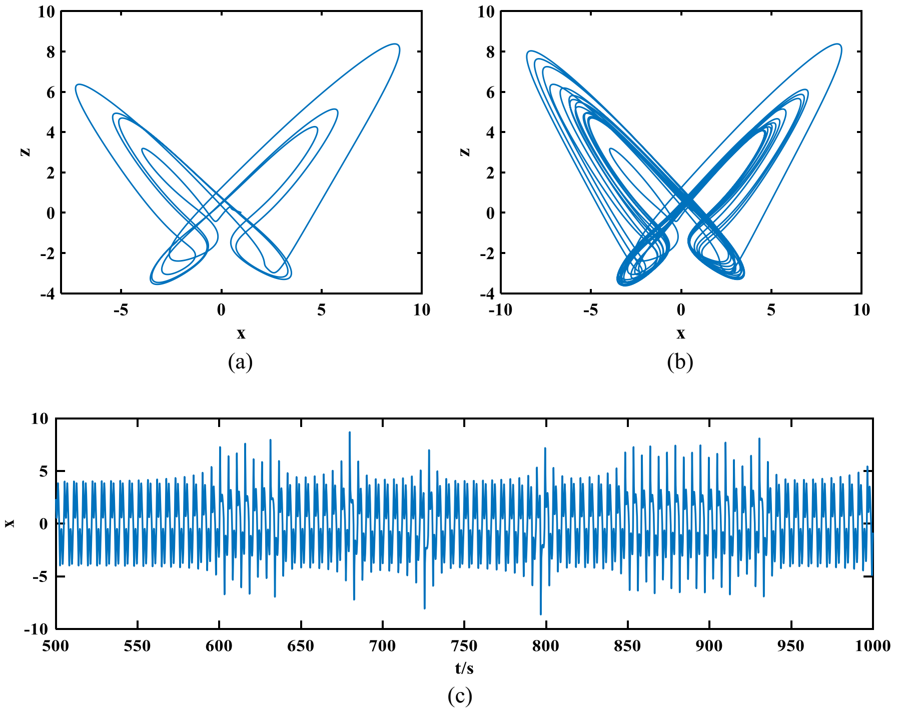


Fig. 9 Intermittent oscillation: **a** Attractor diagram of the cycle **b** Attractor diagram of the chaos **c** Timing waveform at parameter $a=3.3$

$LE_1=0.0781$, $LE_2=0.0206$, $LE_3=-0.4490$, $LE_4=$-10.9200. It is thus observed that the phase and timing diagrams of the system are very sensitive to the parameters. As the parameter changes, the topology of the attractor also changes, making the system more secure for application in image encryption.

The motion state of a system can change from one stable state to another, from an immobile point to a periodic state, and from a periodic state to a chaotic state. Keep the parameters $b=1.02$, $c=9.02$, $d=1$, and $e=2.02$, so that the parameter changes within (0, 5). When $a\in$ [0.391,0.410], the system is in the motionless point state; when a∈ [0.569,0.571], the system changes from an immobile point state to a periodic state; when $a\in$ [0.689,0. 692], the system changes from a periodic state to a chaotic state. When a∈ [2.429,2.433], the system changes from a chaotic state to a hyperchaotic state. The system exists in the form of jumps between immobile points, cycles, non-cycles, chaos, and hyperchaos, and has a rich dynamical behavior. As shown in Fig. 10a, b, c, and d are the phase diagrams of the different states of the system when the parameter a is varied.As shown in Fig. 10a, b, c and d the Liapunov exponents for the states are shown in Table 2.

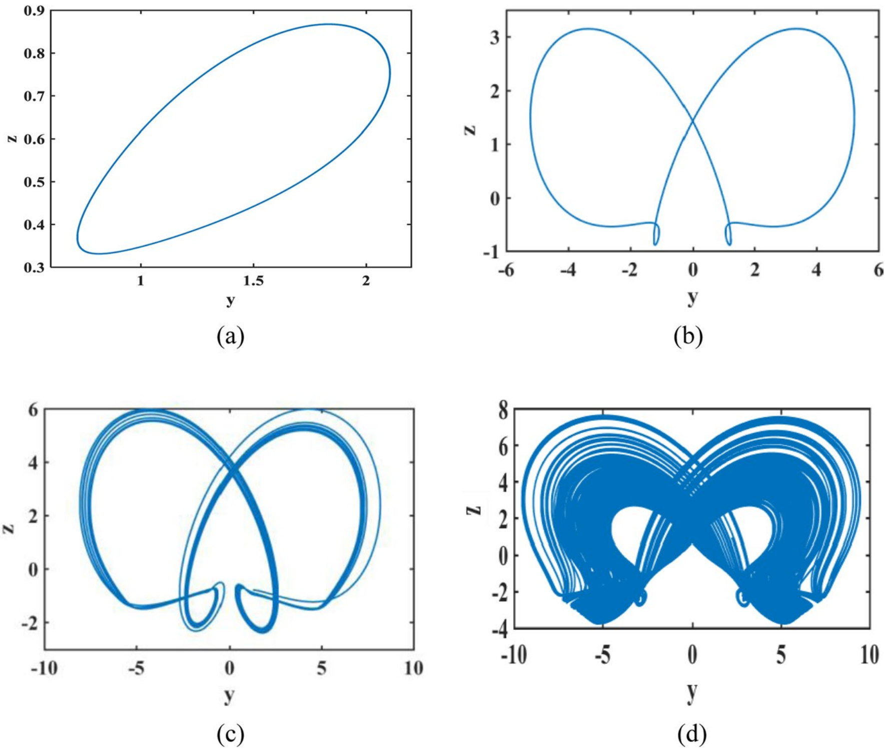


Fig. 10 Phase diagram of the system in different states: **a** *y*–*z* plane at $a=0.4$ **b** *y*–*z* plane at $a=0.57$ **c** *y*–*z* plane at $a=0.69$ **d** *y*–*z* plane at $a=2.43$

Table 2 Lyapunov index in different states

Phase portrait	Lyapunov exponent	Current state
Figure 10a	$LE_1=-0.0215$, $LE_2=-0.0711$, $LE_3=-1.2860$, $LE_4=-7.0200$	Immobile point state
Figure 10b	$LE_1=0$, $LE_2=-0.2451$, $LE_3=-0.4673$,$LE_4=-7.7970$	Periodic state
Figure 10c	$LE_1=0.0426$, $LE_2=-0.1949$, $LE_3=-0.7447$, $LE_4=-8.1500$	Chaotic state
Figure 10d	$LE_1=0.0536$, $LE_2=0.0270$, $LE_3=-0.2910$,$LE_4=-10.1900$	Hyperchaotic state

4.3 Sensitivity to initial conditions

Initial value sensitivity means that a relatively small change in the initial state of the system can lead to a large difference in the trajectory of the system. As shown in Fig. 11, the solid blue line has an initial value of [1,1,0,0] for time-series, and the solid purple line has an initial value of [1,1,0,1] for the time-series. It can be seen

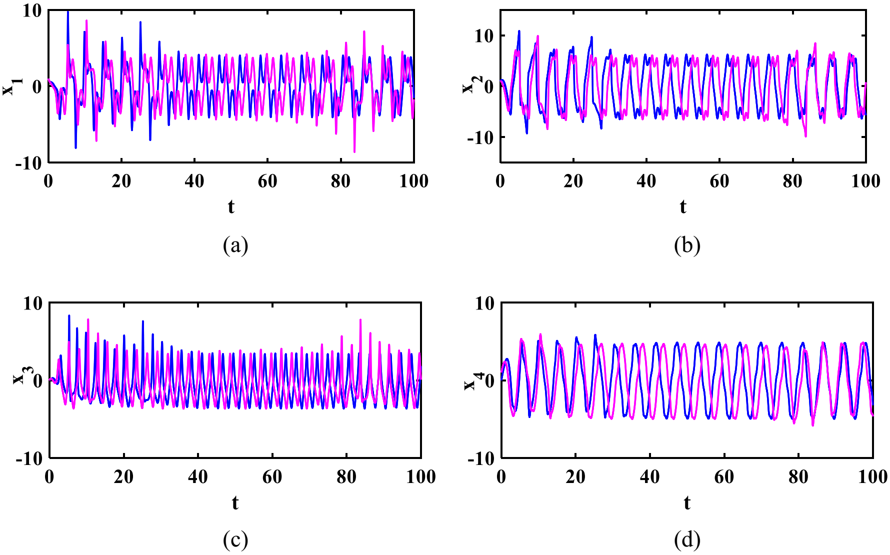
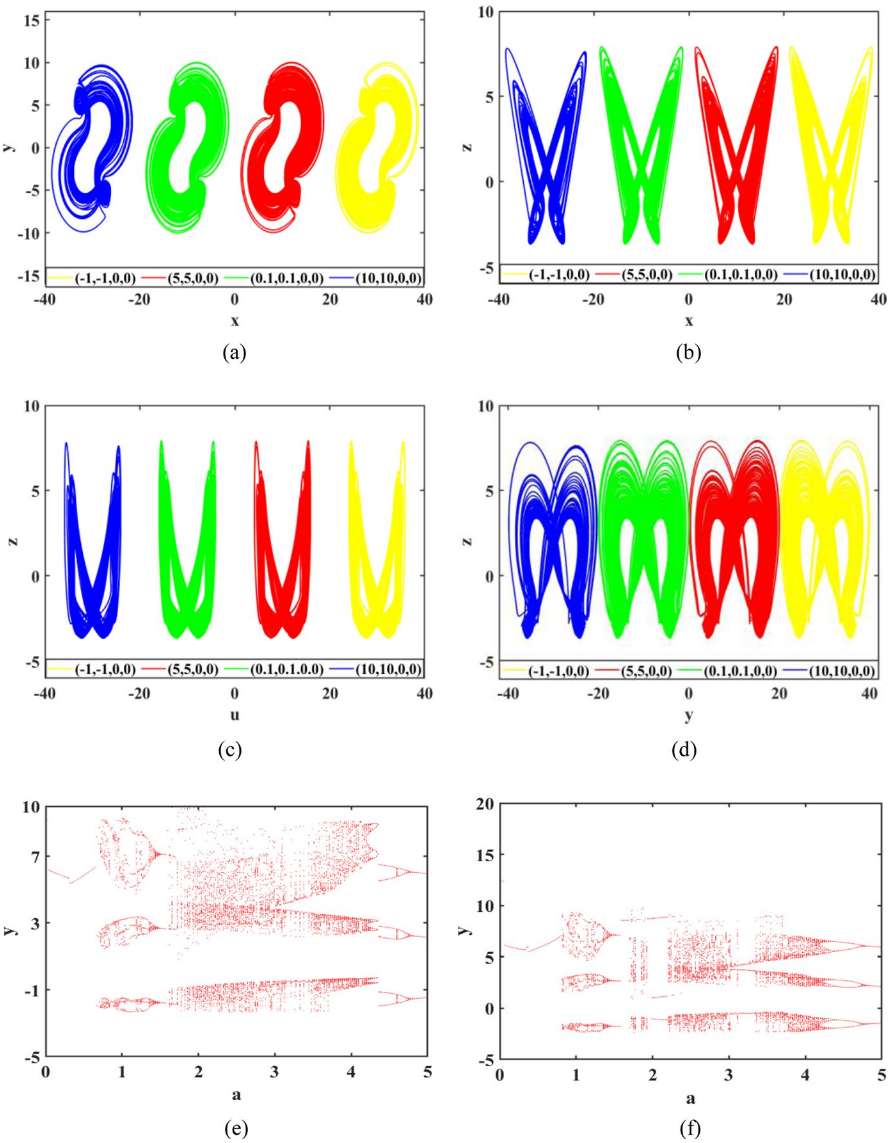


Fig. 11 Time-series of state variables with different initial values: **a** Time-series of x_1 **b** Time-series of x_2 **c** Time-series of x_3 **d** Time-series of x_4

that the system has a high sensitivity to initial values, and this excellent feature can be applied to confidential communications, such as image encryption.

4.4 System coexistence attractor analysis

Chaotic systems are sensitive to changes in initial values, keeping the parameters of the system unchanged. Changing the initial values of the system will cause the system trajectories to change, with some trajectories eventually converging on the same attractor and some trajectories clustering on other attractors. These attractors are called coexisting attractors. To better analyze the state of the hyperchaotic system, the existence of multiple coexisting attractors of the system can be found by changing the initial state of the system with well-defined system parameters. When the initial parameters $a=3.04$, $b=1.02$, $c=9.02$, $d=1$, and $e=2.02$, Fig. 12a, b, c, d show the attractor coexistence diagram in the x–y plane, the x–z plane, the u-z plane, and the y–z plane, respectively. When they change their initial value, their behavior changes. The initial value of the yellow track line is (-1,-1,0,0), the initial value of the red track line is (5,5,0,0), the initial value of the green track line is (0.1,0.1,0,0), and the initial value of the blue track line is (10,10,0,0). The bifurcation diagrams of the system for initial values (5,5,0,0) and (10,10,0,0) are shown in Fig. 12 in e and f, respectively, and the computation results of the coexisting attractors show that the phase diagrams and the Liapunov exponential spectra remain consistent when the initial values are changed. The initial values are the same as in the bifurcation diagram.



(a) (b)

(c) (d)

(e) (f)

Fig. 12 Coexistence of attractors in different directions: **a** *x*–*y* coexistence attractor **b** *x*–*z* coexistence attractor **c** *u*-*z* coexistence attractor **d** *y*–*z* coexistence attractor **d** System Bifurcation Diagram **e** System Bifurcation Diagram

4.5 Complexity analysis

The complexity of chaotic systems is an important part of the analysis of the dynamics of the studied systems. The depth of the image color represents the complexity of the chaotic system within the parameter range, if the color is darker then it means that the complexity value of the system is higher and the corresponding sequence randomness is better, on the contrary, the lighter the color means that the complexity value of the system is lower and the random sequence of the system is worse. The results of the complexity analysis show that the complexity corresponds precisely to the randomness of the system it has the same effect as the Poincaré mapping, the bifurcation diagram, and the Lyapunov exponent. The complexity is the degree to which the chaotic sequence is close to the random sequence. The method is mainly to make the chaotic sequence close to the random sequence by using the correlation algorithm, and the closer it is to the random sequence, the greater the complexity and thus the higher the security of the system will be. This good feature can then be utilized for image encryption. There are two main types of complexity in chaotic systems, one is the *SE* complexity and the other is the *C0* complexity, and it is verified that in continuous chaotic systems, the trends of both remain the same [33, 34].*SE* complexity is a measure of complexity in chaotic systems. It is often used to describe how sensitive the system is to initial conditions.*C0* complexity is another measure of complexity in chaotic systems. It describes the entropy growth rate of the system's trajectory in phase space. The connection between the two is that both *SE* complexity and *C0* complexity are used to measure the complexity of chaotic systems. They both reflect the unpredictability and nonlinear characteristics of the system behavior. The difference between the two is that *SE* complexity mainly focuses on the sensitivity of the system behavior to the initial conditions, while *C0* complexity pays more attention to the chaotic degree of the system behavior complexity emphasizes the effect of small perturbations, while *C0* complexity takes into account the entropy growth rate of the trajectories in the whole phase space.

The present analysis is based on the fixed parameters $a=3.04$,$b=1.02$,$c=9.02$,$d=1$, and $e=2.02$. Figure 13a shows the 3D *SE* complexity of the system for the initial values (1,1, x(0),z(0)). Figure 13b shows the 3D C_0 complexity of the system for the initial values (1,x(0),0,z(0)). It can be observed that a large area of black is mixed with a small area of white and yellow, the darker the color indicates a higher complexity of the system, and the only remaining small amount of yellow and red in the darker area represents the state transfer phenomenon that exists in a chaotic system, and thus the

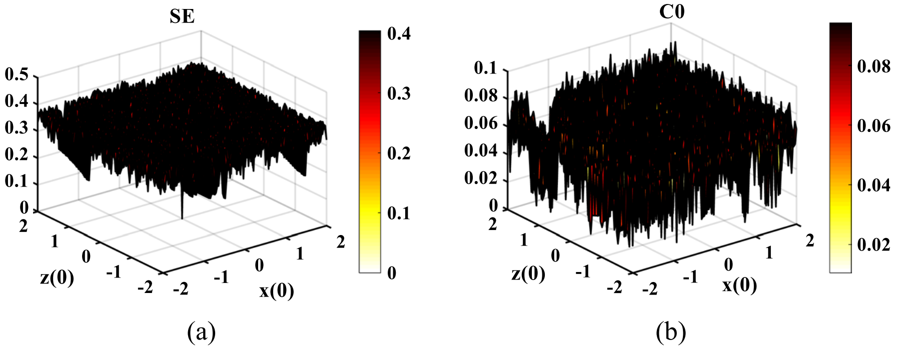


Fig. 13 Three-dimensional complexity of the system at different initial values: **a** *C0* complexity with x(0)-z(0) as variables **b** *SE* complexity with x(0)-z(0) as variables

state complexity of the hyperchaotic system. The system is more complex and its application in the field of image encryption will have higher security.

As shown in Fig. 14a and b plots of SE and C_0 single-parameter complexity with parameter d, respectively, it can be seen that the complexity is higher at $d = 1$, indicating that chaos is more pronounced. Compared to the literature [34], this system has high complexity and high security and has good properties when applied to confidential communication.

5 Analog circuit design and simulation

In order to verify the dynamical behavior of the chaotic system, the results will be analytically verified in this section by designing a simulation circuit. It can be observed through Fig. 1 that the variable dynamic range of the phase diagram does not exceed ± 13.5 V, therefore no scaling compression transformation of the system is required. If the system exceeds ± 13.5 V, a variable proportional compression transformation must be performed. Perform proportional transformation of Eq. (2), set $\tau_0 = 1/(R_0C_0) = 1/(R_3C_1) = 1/(R_8C_2) = 1/(R_{14}C_3) = 1/(R_{20}C_4)$ to derive Eq. (10):

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}(\tau_0 t)} = y - ax + \mathrm{yx} \\ \dfrac{\mathrm{d}y}{\mathrm{d}(\tau_0 t)} = by - xz - u \\ \dfrac{\mathrm{d}z}{\mathrm{d}(\tau_0 t)} = xy - cz + -yu \\ \dfrac{\mathrm{d}u}{\mathrm{d}(\tau_0 t)} = dy + e\sin(x) \end{cases} \tag{10}$$

Based on the use of an inverse adder, Eq. (11) is obtained after the evolution and transformation of the equation:

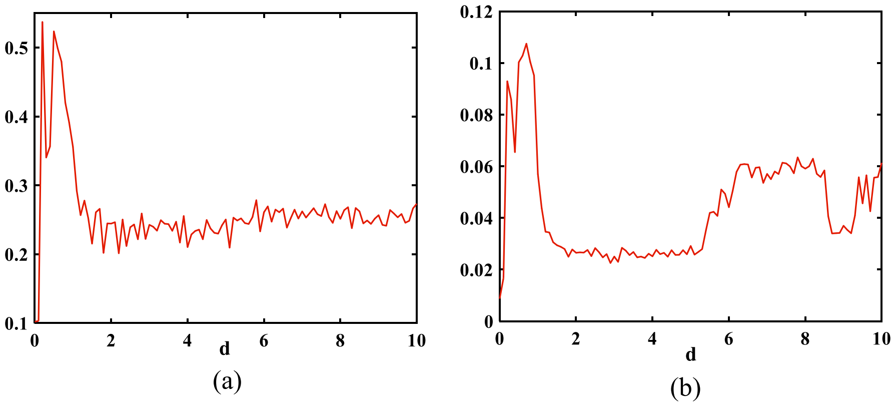


Fig. 14 Complexity: **a** SE complexity when $d = 1$ **b** $C0$ complexity when $d = 1$

$$\begin{cases} x = \dfrac{1}{R_0 C_0} \displaystyle\int \left[-(-y) - ax - x(-y)\right] \mathrm{d}t \\ y = \dfrac{1}{R_0 C_0} \displaystyle\int \left[-b(-y) - xz - u\right] \mathrm{d}t \\ z = \dfrac{1}{R_0 C_0} \displaystyle\int \left[-x(-y) - cz - (-y)u\right] \mathrm{d}t \\ u = \dfrac{1}{R_0 C_0} \displaystyle\int \left[-d(-y) - e\sin(-x)\right] \mathrm{d}t \end{cases} \tag{11}$$

By introducing resistance values, the circuit system equation can be derived based on the differential equation of the system circuit:

$$\begin{cases} x = \dfrac{1}{R_3 C_1} \displaystyle\int (\dfrac{R_4}{R_{30}} y - \dfrac{R_4}{R_{23}} x + \dfrac{R_4}{R_5} yz) \mathrm{d}t \\ y = \dfrac{1}{R_8 C_2} \displaystyle\int (\dfrac{R_9}{R_{24}} y - \dfrac{R_9}{R_{10}} xz - \dfrac{R_9}{R_{11}} u) \mathrm{d}t \\ z = \dfrac{1}{R_{14} C_3} \displaystyle\int (\dfrac{R_{15}}{R_{25}} xy - \dfrac{R_{15}}{R_{17}} \mathrm{z} + \dfrac{R_{15}}{R_{16}} yu) \mathrm{d}t \\ u = \dfrac{1}{R_{20} C_4} \displaystyle\int (\dfrac{R_{21}}{R_{33}} y - \dfrac{R_{21}}{R_{22}} \sin(x)) \mathrm{d}t \end{cases} \tag{12}$$

Set $C_1 = C_2 = C_3 = C_4$, by comparing (10) and (12), we can get the following parameters $R_3 = R_8 = R_{14} = R_{20} = 15\mathrm{K}\Omega$, $R_5 = R_{10} = R_3 = R_{25} = R_{16} = 1\mathrm{K}\Omega$, $R_{23} = 3.3\mathrm{K}\Omega$, $R_{24} = 10.5\mathrm{K}\Omega$, $R_{17} = 1.5\mathrm{K}\Omega$, $R_{22} = 4.9\mathrm{K}\Omega$, $R_4 = R_9 = R_{15} = R_{21} = R_{33} = R_{30} = R_{11} = 10\mathrm{K}\Omega$.The circuit diagram of the system is derived from the mathematical Eq. (12) as shown in Fig. 15.The quantitative relationship between Eq. (10) and Eq. (12) is for example the ratio of the coefficients R_4/R_{30} of y in Eq. (12) is the coefficient of y in Eq. (10) which is 1, and the ratio of R_4/R_{23} in Eq. (12) is the coefficient a of Eq. (10). The tool used in this analog circuit is Multisim 14.0, and the models used are the AD633 multiplier, LM248 amplifier, and AD639 sine converter.

The simulation is carried out through the circuit software simulation multi-simulation and the phase diagram of the system is obtained as shown in Fig. 16. By comparing this figure with the phase diagram of the system, the attractor of the circuit agrees with the theoretical attractor, so the correctness of the system is verified by numerical analysis and experimentation, and the attractor exists in the system.

6 Hardware circuit implementation

Field programmable gate arrays (FPGA) are the ideal solution we chose for building chaotic circuits. Conventional chaotic circuits are constructed using analog electronic components, but the performance of these components is affected by

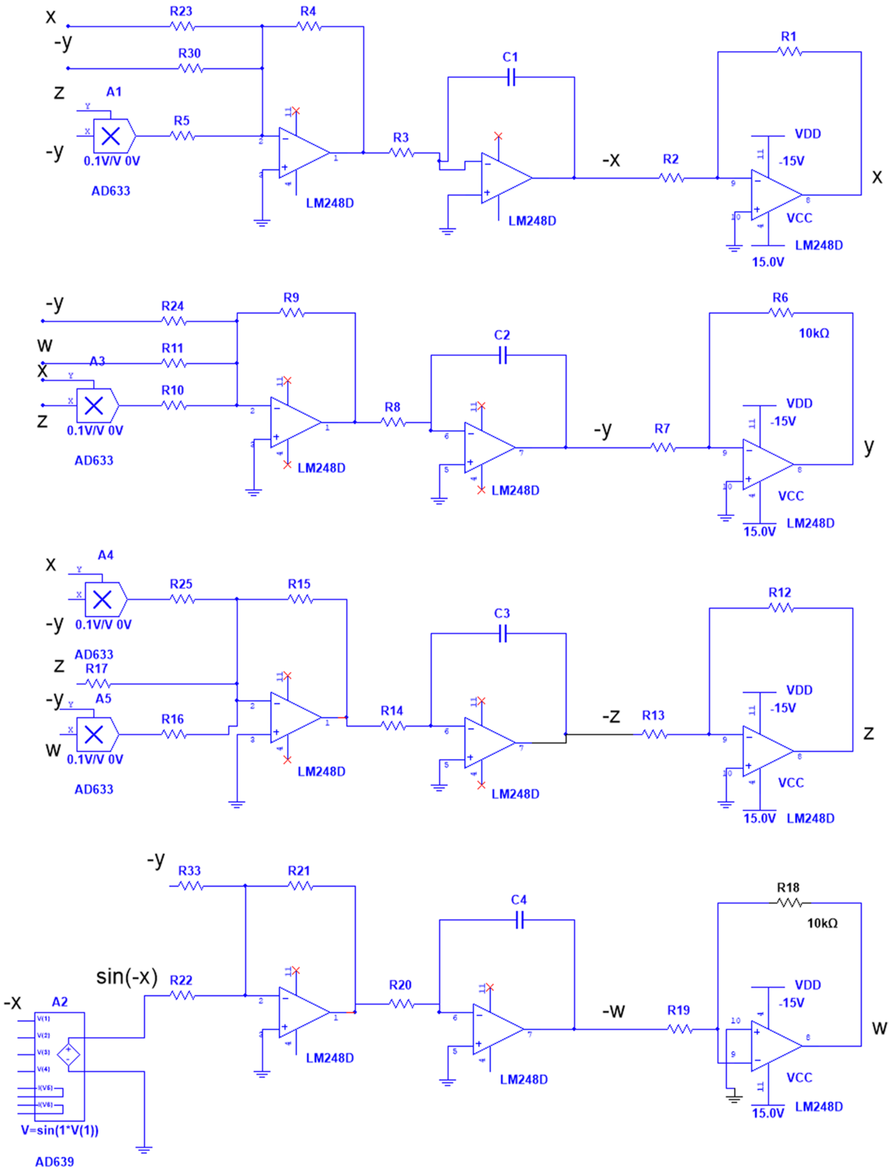


Fig. 15 System circuit schematic

aging and other factors, and long-term performance stability cannot be guaranteed. FPGA are used exclusively in the field of integrated circuits, successfully addressing the shortcomings of custom circuits and overcoming the shortcomings of the limited number of gates in the original programmable devices. By designing circuits using FPGA, you can reduce printed circuit board area, shorten design time, and significantly improve system reliability.FPGA is more flexible and programmable

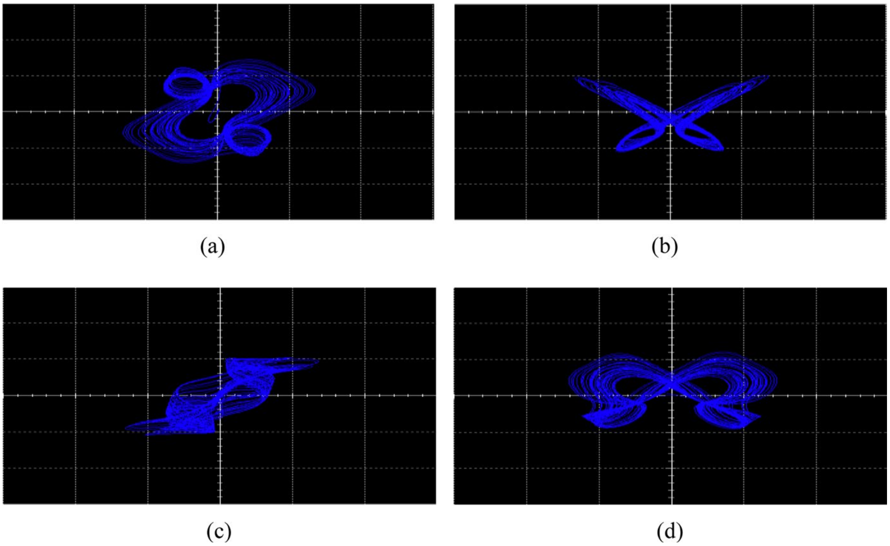


Fig. 16 Circuit simulation diagram: **a** Phase diagram of the *x*–*y* plane **b** Phase diagram of the *x*–*z* plane **c** Phase diagram of the *x*-*u* plane **d** Phase diagram of the *y*–*z* plane

than DSP. Compared to DSP, FPGA can configure hardware circuits on demand to accommodate a variety of complex chaotic systems and different algorithms.

The XC6SLX16-2FTG256I chip is selected as the FPGA and the Texas Instruments PROGRAMMED 12-bit dual-channel TLC5618A is used as the digital-to-analog converter (DAC). The main parameters of the XC6SLX16-2FTG256I chip are the number of logic cells: 16,256, the capacity of internal memory: 49,152 bits, the number of I/O pins: 148, the internal clock management resources: 4 global clock line networks. The main parameters of the XC6SLX16-2FTG256I chip are the number of logic cells: 16,256, internal memory capacity: 49,152 bits, the number of I/O pins: 148, and the internal clock management resources: 4 global clock line networks. Quartus 15.0 was used as the development environment, and an oscilloscope with a bandwidth of 20 Hz was used to output the images with a MATRIX MOS-620 model.The XC6SLX16-2FTG256I chip offers a number of outstanding features including low static and dynamic power consumption, a maximum clock frequency of 667.0 MHZ, adjustable I/O slew rate for improved signal integrity, rich logic resources and higher logic capacity, and a highly efficient 6-input LUT that improves performance and reduces power consumption. Compared with other FPGA chips, the XC6SLX16-2FTG256I's advantageous features are more conducive to realizing chaotic digital circuits. The digital implementation circuit flow is shown in Fig. 17.

The specific operation is as follows. First, connect the FPGA development board to the computer, you can generally use the USB interface to connect. Install the appropriate FPGA development tool Quartus II 15.0 on the computer to write, synthesize, and download the FPGA design. Open the FPGA development tool and create a new project, set appropriate pin constraints in the project to ensure that the

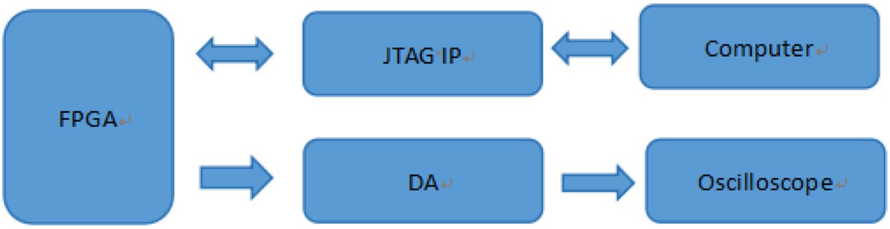


Fig. 17 Block diagram of hardware implementation of FPGA platform

input and output pins on the FPGA development board correspond to the inputs and outputs of the chaotic system phase diagram.The design is synthesized and implemented using the FPGA development tool and binary files are generated that can be burned onto the FPGA. Connect the computer to the FPGA development board and the FPGA development tool downloads the generated binary file to the FPGA development board via JTAG. Convert the input signals (initial conditions or parameters) of the chaotic system into analog signals via DA and input them to the FPGA development board.Finally, run the chaotic system design on the FPGA development board and use an oscilloscope connected to the output pins of the chaotic system to observe and record the waveforms on the oscilloscope.

Considering that the Runge Kutta algorithm would take up a lot of logic resources in the FPGA, we chose the Eulerian algorithm to convert the system to C code and discretization to obtain Eq. (13), where the step size is h = 0.001 and the parameters are $a=3.04$, $b=1.02$, $c=9.02$, $d=1$, and $e=2.02$. The utilization of the chip resources in the FPGA in implementing the digital hardware circuit of the new system is shown in Table 3. Finally, the planar phase diagram of the system is obtained by a digital oscilloscope, as shown in Fig. 18, which is basically consistent with the numerical simulation results and Multisim circuit simulation results. The RTL diagram of the system is shown in Fig. 19.

$$\begin{cases} x(n+1) = x(n) + h(y(n) - ax(n) + y(n)z(n)) \\ y(n+1) = y(n) + h(by(n) - x(n)z(n) - u(n)) \\ z(n+1) = z(n) + h(x(n)y(n) - cz(n) + y(n)u(n)) \\ u(n+1) = u(n) + h(dy(n) + e\sin(x(n)) \end{cases} \tag{13}$$

Table 3 Resource utilization in the design of new four-dimensional ultra chaotic hardware

Resource	Estimation	Available	Utilization (%)
IO	47	150	31.33
FF	16,300	112,010	14.55
BUFG	1	32	3.12
LUTRAM	16,215	589,824	2.74
LUT	13,021	47,800	27.24

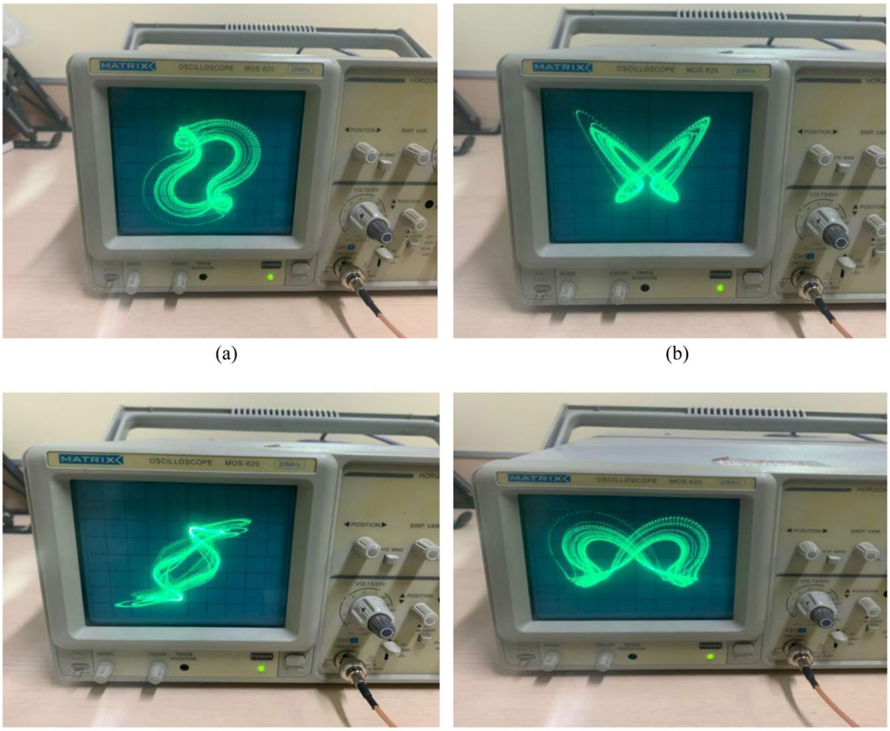

(a)
(b)
(c)
(d)

Fig. 18 Oscilloscope phase diagram: **a** *x*–*y* plane **b** *x*–*z* plane **c** *x*-*u* plane **d** *y*–*z* plane

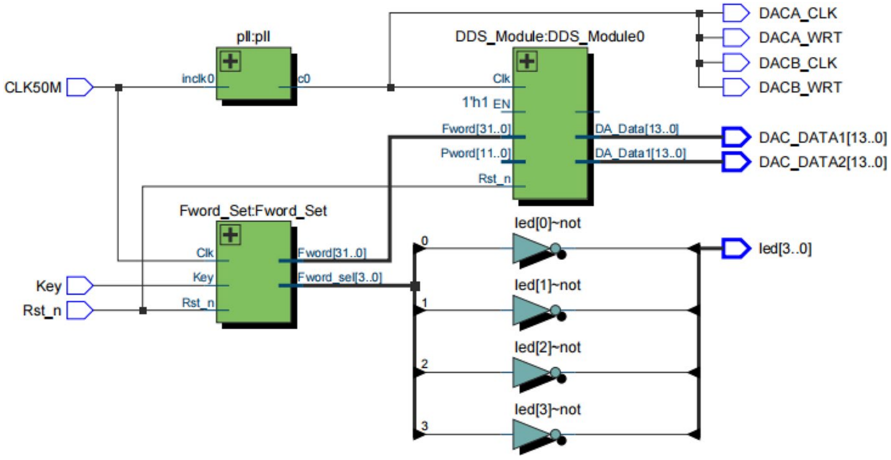


Fig. 19 RTL schematic diagram

7 Application in image encryption

With time, image encryption algorithms based on chaotic systems have achieved rapid development [19–23]. Chaotic systems have the good properties of unpredictability and sensitivity to initial values, as well as the randomness of the generated sequences, so chaotic systems are widely used in image encryption. Early chaotic image encryption mainly uses some simple low-dimensional chaotic systems or only performs a single encryption. However, the image encryption algorithm proposed in this paper adopts multiple encryption strategies. Taking a grayscale image with the size of $M \times N$ as an example, Arnold transformation [24–27] was performed on the original image first, and then DNA encryption operation was performed on the transformed image. The framework diagram of the image encryption algorithm is shown in Fig. 20 [28–32].

7.1 Arnold Disruption

The Arnold permutation is a transformation proposed by Russian mathematician Vladimir I. Arnold, whose transformation matrix equation is:

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 1 & A \\ B & AB+1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} (\mathrm{mod} N) \tag{14}$$

$$X = (x + By) \mod N \tag{15}$$

$$Y = \left[Bx + (AB+1)y\right] \mod N \tag{16}$$

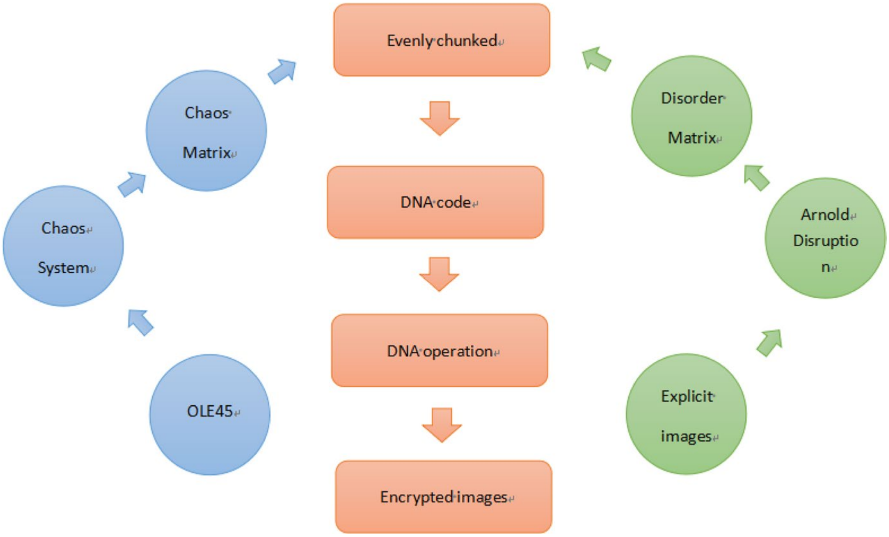


Fig. 20 Encryption process

Table 4 DNA coding rules

Rules	1	2	3	4	5	6	7	8
00	A	A	C	T	T	G	G	C
01	C	G	C	G	T	A	T	A
10	G	C	G	C	A	T	A	T
11	T	T	A	A	C	C	G	G

Table 5 DNA addition and subtraction rules

Addition					Subtraction				
+	A	C	G	T	−	A	C	G	T
A	A	C	G	T	A	A	T	G	C
C	C	G	T	A	C	C	A	T	G
G	G	T	A	C	G	G	C	A	T
T	T	A	C	G	T	T	G	C	A

x, $y=\{0,1\ \ldots,\ N\text{-}1\}$ denotes the position before the transformation, and (X, Y) denotes the transformation position. a, b are the parameters of Arnold's transformation. $a=x_{\mathrm{i}}$, $b=y_{\mathrm{i}}$ $(i=1, 2, 3\ldots, MN)$, N denotes the side length of the square image, and mod denotes the modulus operation.A and B are pseudo-random sequences generated by vector generation X, both of size $M\times N$, and the transformation between pixel points can be realized by pseudo-random variables A and B.

7.2 DNA encoding encryption

Watson and Crick jointly proposed the double helix structure of the DNA strand, in which each DNA sequence consists of four bases: adenine (A), cytosine (C) and guanine (G), and thymine (T), and the two DNA sequences are bonded together by the complementary pairing laws of A-T and C-G. The four bases are encoded by 00, 01, 10 and 11, and then eight coding rules can be obtained according to the principle of DNA complementarity. These four bases are encoded with 00, 01, 10 and 11, and then eight encoding rules can be obtained according to the principle of DNA base complementarity. To realize image encryption, the image data should first be converted into binary numbers, and then a DNA coding rule is randomly selected to encode two binary numbers into one base, and decoding is the inverse process of this process. Tables 4, 5 and 6 show the complete DNA algorithm.

As shown in Table 4, the so-called DNA computation refers to the "different-or" or "same-or" operation between DNA codes, as well as the complementary operation of DNA codes, such as the eight DNA coding modes shown in Table 4, where DNA computation is still essentially a binary The DNA calculation here is still essentially a binary arithmetic operation.

The definition of addition and subtraction of DNA follows traditional binary addition and subtraction operations. Since there exist 8 DNA coding rules, there also

Table 6 DNA coding rule 1 when the DNA heterodyning rule

XOR	A	T	G	C
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

exist 8 corresponding DNA rules. When using DNA coding rule 1, for example, the DNA addition and subtraction rules shown in Table 5 are obtained.

The definition of DNA dissimilarity rules follows the traditional binary dissimilarity operation. Because there are 8 DNA coding rules, there are also 8 corresponding DNA dissimilarity rules. For example, when using DNA coding rule 1, the DNA dissimilarity rules shown in Table 6 are obtained.

Using the ode45 algorithm to calculate the initial value of the chaotic system and iterate the chaotic system, four keys are obtained. To improve security and obtain better randomness, the first 3001 terms are removed to obtain four chaotic sequences, x_{i}, y_{i}, z_{i}, $u_{\mathrm{i},}$ where ($i = 1, 2, 3 \ldots M \times N$), the $\{u_{\mathrm{i}}\}$ chaotic sequence is converted to an integer between 0 and 255, and then u_{i} is converted into a random matrix R with M rows and N columns. Next, the binary matrix transformation will be performed on the matrix A and matrix R after Arnold permutation, and then every two binary numbers will be converted into a DNA base according to the DNA coding rules, and the corresponding DNA sequence matrix will be obtained, and the matrix H will be represented by DNA calculation.

7.3 Pixel-level diffusion

Firstly, the matrix H is decoded according to the rules of DNA decoding. A binary matrix is obtained, and then it is converted into a binary matrix notated as F. The pseudo-matrix sequences u_{i}', D_{i}, and L_i are the sequences after diffusion. Then the diffusion is performed, the diffusion is performed by using two-way diffusion with heterogeneous operations, and the forward and reverse diffusion are each diffused once, and the formulas for the forward and reverse operations are (17) and (18), respectively.

$$\begin{cases} L_i = L_{i-1} \oplus D_i \oplus F_i \\ F_i = L_{i-1} \oplus L_i \oplus D_i \end{cases} \tag{17}$$

$$\begin{cases} L_i = L_{i+1} \oplus D_i \oplus F_i \\ F_i = L_{i+1} \oplus L_i \oplus D_i \end{cases} \tag{18}$$

The standard 512×512 Lena image and the baboon image are chosen for the experiments of the images, and the encrypted results are shown in Fig. 21b and e, where the image features of the original image are no longer observed.

7.4 Image security analysis

7.4.1 Histogram analysis

Histogram is a statistical method to describe the distribution of images smoothly, usually, the encrypted histogram has the characteristics of uniform distribution, and the image histogram of plain text is not uniform, the implementation of this part selects the classical image Lena and orangutan image of size 512 × 512 as shown in Fig. 22. Figure 22 b and e are the histogram before encryption, Fig. 22c and f are the histograms after encryption, it can be observed that the encrypted histogram presents an overall uniform distribution, which makes it difficult for an attacker to use the statistical characteristics of the sample values to recover the original image. Therefore, it is verified that the algorithm has an excellent ability to prevent statistical analysis.

7.4.2 Keyspace and sensitivity analysis

The set of valid keys becomes the key space, and the key space is large enough to be effective against attacks. A new four-dimensional chaotic system is proposed in this paper, the initial value of the system is $k=(x_0,y_0,z_0,u_0)$ and the parameters of the system are a, b, c, d, and e. The computational accuracy

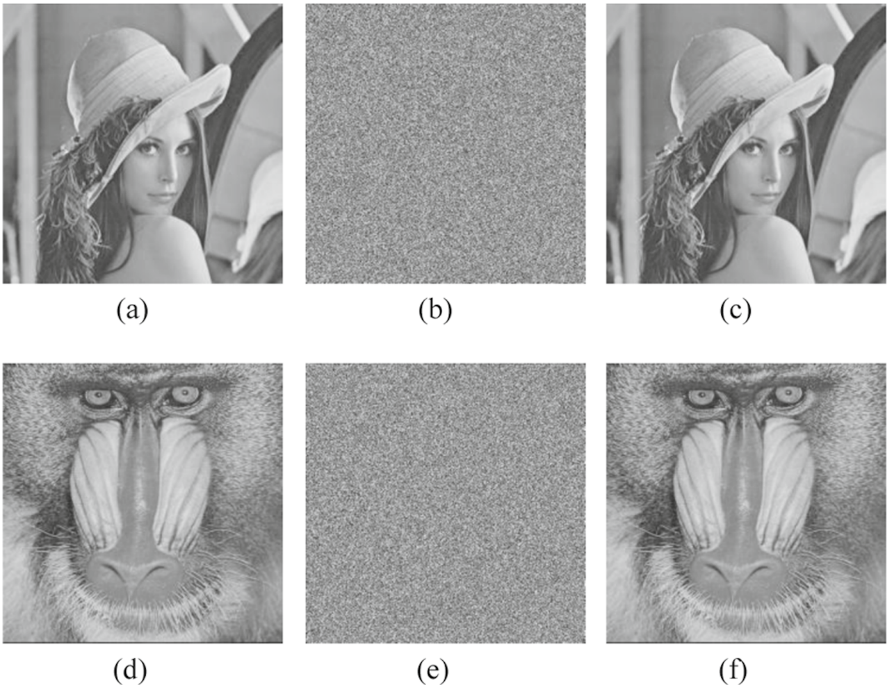


Fig. 21 Encrypted rendering: **a** Lena Original image **b** Lena Encrypted images **c** Lena Decrypting the image **d** Baboon Original image **e** Baboon Encrypted images **f** Baboon Decrypting the image

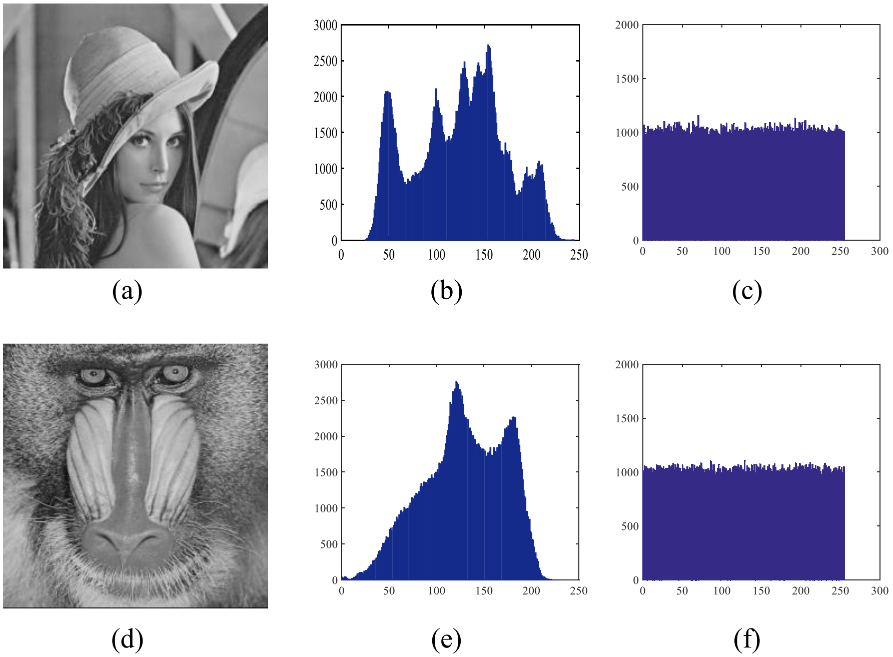


Fig. 22 Image histogram: **a** Lena Original image **b** Lena Original image histogram **c** Lena Histogram of the encrypted image **d** Baboon Original image **e** Baboon Original image histogram **f** Baboon Histogram of the encrypted image

of the computer is 10^{-16}, so the key space of the chaotic system in this paper is $10^{-16}\times 10^{-16}\times 10^{-16}\times 10^{-16}\times 10^{-16}\times 10^{-16}\times 10^{-16}\times 10^{-16}\times 10^{-16}\times 10^{-16}\approx 2^{478}$. It is generally stipulated that the reliability of an encryption system is guaranteed only when the key space is greater than 2100. According to this standard, it is obvious that the key space of the system in this paper is much larger than this requirement.

Key sensitivity is the ratio of the difference between two ciphertext images obtained by observing the encryption of the same plaintext image when the key is changed. If the difference between the two cipher images is small, it proves that the sensitivity of the key is poor. If the difference between two cipher images is large then the sensitivity of the key is proved to be good. When the key sensitivity test is performed in this paper, the key K is changed to K_1 and it is found that the image could not be decrypted as shown in (a) and b in Fig. 23, which shows that the image encryption algorithm in this paper has good key sensitivity.

7.4.3 Correlation analysis

One of the important factors to measure the effectiveness of image encryption is the correlation property. Digital images have a strong correlation between adjacent pixel points in horizontal, vertical, diagonal, and anti-diagonal directions, close to 1. The correlation between adjacent pixels of the encrypted image becomes very small,

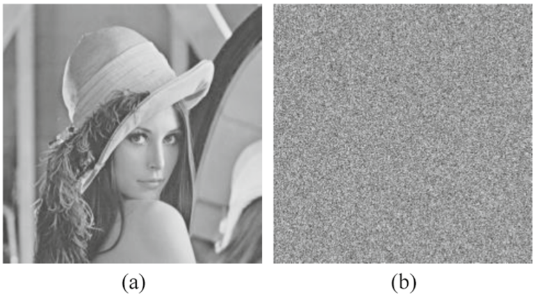


Fig. 23 Key sensitivity test: **a** Original image **b** Decrypted image after key replacement

so breaking the correlation between adjacent pixels of the image is the meaning of image encryption. The formula to calculate the correlation is as follows:

$$\begin{cases} E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \\ D(x) = \frac{1}{n}\sum_{i=1}^{n} (x_i - E(x))^2 \\ \operatorname{cov}(x, y) = \frac{1}{n}\sum_{i=1}^{n} (x_i - E(x))(y_i - E(y) \\ \tau = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)D(y)}} \end{cases} \tag{19}$$

x and y are pixel values representing adjacent pixels, E(X) is representing expectation, and D(X) is representing variance. In this paper, a classic 512×512 Lena image is selected to calculate the correlation coefficients before and after encryption, and the correlation coefficients are calculated from four directions. The correlation coefficients of the images before and after encryption are shown in Fig. 24, and it can be observed that the correlation of the encrypted images is evenly distributed compared with the images before encryption, thus verifying that the algorithm in this paper destroys the correlation of the original images.

As shown in Table 7, the unencrypted image has a strong correlation close to 1 in 4 directions and the image has a dense pixel distribution, while the encrypted image has a small correlation close to 0 in 3 directions and the image has a uniform pixel distribution. It can also be seen from Table 5 that the correlation coefficients of all three directions of the encrypted images of the system in this paper are closer to 0 than the other compared with other methods, which indicates that the encryption effect of the new system algorithm proposed in this paper is very effective (Table 8).

7.4.4 Analysis of information entropy

Information entropy can be used to measure the random distribution of image information, which is an important indicator of the random distribution. The better the

Fig. 24 The correlation coefficient of images: **a** Plaintext horizontal direction **b** Plaintext vertical direction **c** Plaintext diagonal direction **d** Plaintext anti-diagonal direction **e** Ciphertext horizontal direction **f** Ciphertext vertical direction **g** Ciphertext diagonal direction **h** Ciphertext anti-diagonal direction ▸

random distribution, the greater the value of information entropy, which is calculated by the formula:

$$G(s) = -\sum_{i=0}^{2^n-1} p(s_i)\log_2 p(s_i) \tag{20}$$

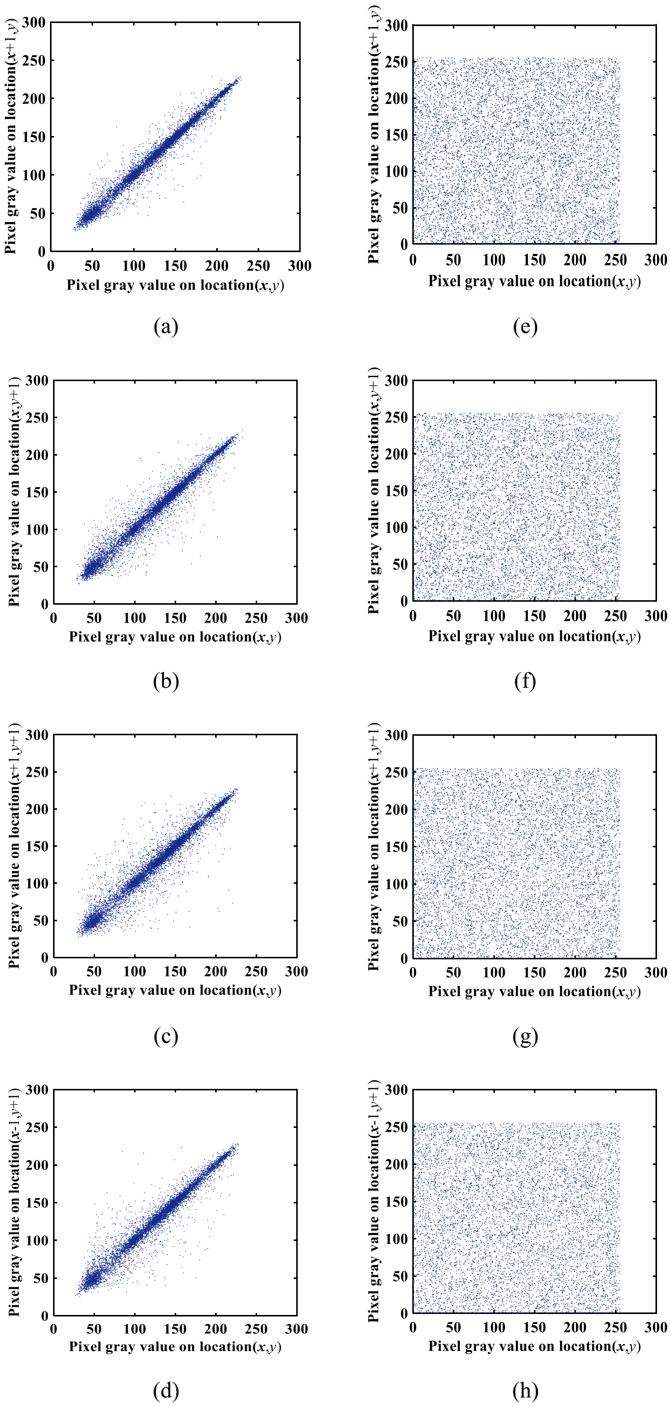
All states of pixel values in the image are denoted by 2^n and the probability of pixel values in the image is denoted by $p(s_\mathrm{i})$, which has the information of 256 states in this paper, so the ideal information entropy is 8. The image information entropy after encryption is 7.9994, which is very close to 8. The comparison with other systems after encryption is given in the chart, and it is found that the encryption effect of this paper is better.

7.4.5 Robustness analysis

Robustness is the most important characteristic to measure the resistance of an encryption algorithm to interference. In this paper, we choose to test the robustness of the encryption algorithm by cropping attack and noise attack. After cropping a part of the image, the image is then decrypted, and the result of decryption is shown in Fig. 25c. Applying 0.03 times pretzel noise to the encrypted image, the decrypted image is shown in Fig. 26c. It is found that the key information of the graphics can still be identified using the encryption algorithm in this paper. It can be verified that this algorithm can resist the cropping attack and noise attack to a certain extent and has good robustness.

8 Conclusion

In this paper, a novel four-dimensional hyperchaotic system is proposed and the dynamical properties of the system are analyzed. It is found that burst oscillations appear on the time series, intermittent chaos, and inverse multiplicative period bifurcations appear in the Lyapunov exponential spectrum and bifurcation diagram. The coexisting attractor appears to have a rare symmetric structure, indicating that the system has a rich dynamical behavior and a very good topology. In addition, in the aspect of system design and verification, Multisim circuit simulation software and FPGA digital hardware circuits are used. The experimental results show that the system exhibits excellent chaotic generation capability and verifies its feasibility and effectiveness. Finally, the new image encryption algorithm is designed by combining the new chaotic system proposed in this paper and DNA encryption algorithm, and the security performance such as information entropy and correlation after image encryption is analyzed, and the system is found to have good encryption cryptographic effect. Therefore, the novel


Pixel gray value on location(x+1,y)
Pixel gray value on location(x,y+1)
Pixel gray value on location(x+1,y+1)
Pixel gray value on location(x-1,y+1)
Pixel gray value on location(x,y)
0
50
100
150
200
250
300

(a) (e)

(b) (f)

(c) (g)

(d) (h)

Table 7 Correlation coefficient comparison

Method	Horizontal correlation	Vertical correlation	Diagonal correlation
Original Lena image	0.9855	0.9711	0.9623
Literature [28]	0.01022	0.02141	0.00562
Literature [29]	0.00270	0.01520	0.00711
Literature [30]	− 0.0034	− 0.0060	0.0063
Algorithm of this paper	0.0019	−0.0032	−0.0053

Table 8 Information entropy comparison

Method	Information entropy
Original Lena image	7.0211
Algorithm of this paper	7.9994
Literature [24]	7.9964
Literature [25]	7.9978
Literature [26]	7.9975
Literature [27]	7.9380

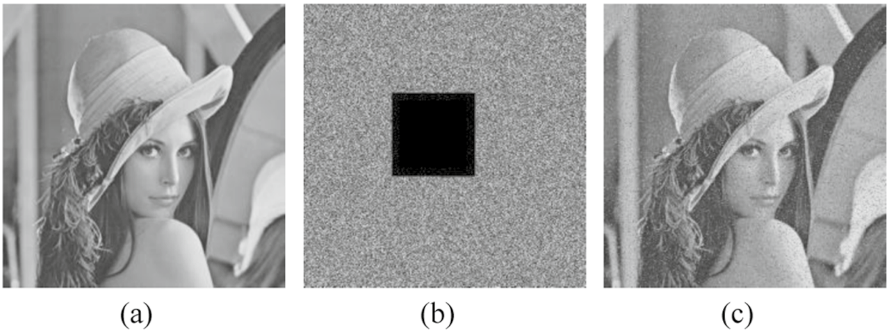


Fig. 25 Key trimming test: **a** Original image **b** Trimming test **c** Decrypting the image

four-dimensional hyperchaotic system and encryption algorithm proposed in this paper have good prospects for application in digital image communication.

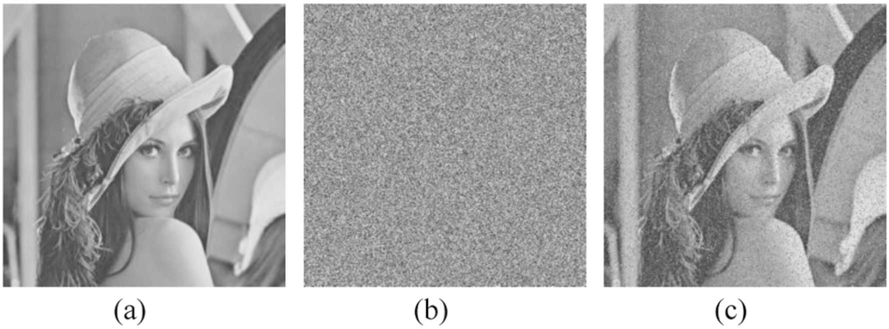


Fig. 26 Noise Attack Test: **a** Original image **b** 0.03 times pretzel noise was applied **c** Decrypting the image

Author contributions Jie Zhang is responsible for the revisions; Jingshun Bi is responsible for all the manuscript writing; Jinyou Hou and Qinggang Xie is responsible for the guidance.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Joshi M, Ranjan A (2020) An autonomous simple chaotic jerk system with stable and unstable equilibria using reverse sine hyperbolic functions. Int J Bifurcation Chaos 30(05):2050070
2. Joshi M, Ranjan A (2019) New simple chaotic and hyperchaotic system with an unstable node. AEU-Int J Electron C 108:1–9
3. Joshi M, Ranjan A (2019) An autonomous chaotic and hyperchaotic oscillator using OTRA. Analog Integr Circ Sig Process 101:401–413
4. Joshi M, Ranjan A (2022) Low power chaotic oscillator employing CMOS. Integration 85:57–62
5. Lai Q, Zhang H, Kuate PDK et al (2022) Analysis and implementation of no-equilibrium chaotic system with application in image encryption. Appl Intell 52:11448–11471
6. Wang SM, Peng QQ, Du BX (2022) Chaotic color image encryption based on 4D chaotic maps and DNA sequence. Opt Laser Technol 148:107753
7. Hu CY, Tian Z, Wang Q, Zhang XF, Liang B, C.l. Jian, X.M. Wu, (2022) A memristor-based VB2 chaotic system: Dynamical analysis, circuit implementation, and image encryption. Optik 269:169878
8. Haq TU, Shah T (2021) 4D mixed chaotic system and its application to RGB image encryption using substitution-diffusion. Journal of Information Security and Applications 61:102931
9. Hagras EAA, Saber M (2020) Low power and high-speed FPGA implementation for 4D memristor chaotic system for image encryption. Multimed Tools Appl 79:23203–23222
10. Huang LL, Yao WJ, Xiang JH et al (2022) Study on super-multistability of a four-dimensional chaotic system with multisymmetric homogeneity Attractor . J Electron Inf Technol 44(1):10
11. Manal M, Karim K, Lazaros M (2023) Christos Volos, A new 4D Memristor chaotic system: analysis and implementation. Integration 88:91–100
12. Fang PF, Huang LG, Lou M et al (2021) An image encryption algorithm based on combing two-dimensional Logistic chaotic map and DNA sequence operation. China Sciencepaper 16(3):248–252
13. Sprott JC (2011) A proposed standard for the publication of new chaotic systems. Int J Bifurcation Chaos 21(09):2391–2394
14. Yan SH, Ren Y, Song ZL, Shi WL, Sun X (2022) A memristive chaotic system with rich dynamical behavior and circuit implementation. Integration 85:63–75
15. Munir, N., Khan, M., Wei, Z.et al. Circuit implementation of 3D chaotic self-exciting single-disk homopolar dynamo and its application in digital image confidentiality.Wireless Netw (2020).

16. Sun J, Zhao X, Fang J et al (2018) Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization. Nonlinear Dyn 94:2879–2887
17. Wang B, Zou FC, Cheng J (2018) A memristor-based chaotic system and its application in image encryption. Optik 154:538–544
18. Hu CY, Tian Z, Wang Q, Zhang XF, Liang B, Jian CL, Wu XM (2022) A memristor-based VB2 chaotic system: dynamical analysis, circuit implementation, and image encryption. Optik 269:169878
19. Zhang J, Guo Y, Xu LH, Zhu XP, Yang J (2022) Hyperchaotic circuit design based on memristor and its application in image encryption. Microelectron Eng 265:111827
20. Guo Q, Wang N, Zhang GS (2021) A novel current-controlled memristor-based chaotic circuit. Integration 80:20–28
21. Ponuma R, Amutha R (2018) Compressive sensing based image compressionencryption using novel 1D-chaotic map. Multimedia Tools Appl 77(15):19209–19234
22. Lai Q, Wan ZQ, Kuate PDK, Fotsin H (2020) Coexisting attractors, circuit implementation and synchronization control of a new chaotic system evolved from the simplest memristor chaotic circuit. Commun Nonlinear Sci Numer Simul 89:105341
23. Kumar M, Mohapatra RN, Agarwal S, Sathish G, Raw S (2019) A new RGB image encryption using generalized Vigenére-type table over symmetric group associated with virtual planet domain. Multimedia Tools Appl 78(8):10227–10263
24. Doubla IS, Njitacke ZT, Ekonde S, Tsafack N, Nkapkop JDD, Kengne J (2021) Multistability and circuit implementation of Tabu learning two-neuron model: application to secure biomedical images in IoMT. Neural Comput Appl 33(21):14945–14973
25. Kamell Mohamed F (2014) A parallel block-based encryption schema for digital images using reversible cellular automata. Eng Sci Techno Int J 17(2):85–94
26. Ping P, Feng X, Zhijian W (2014) Image encryption based on non-affine and balancedcellular automata. Signal Process 105:419–429
27. Li W, Chang XY, Yan AM, Zhang HB (2021) Asymmetric multiple image elliptic curve cryptography. Opt Lasers Eng 136:106319
28. Li FP, Liu JB, Wang GY, Wang KT (2020) An Image encryption algorithm based on chaos set. J Electron Inf Technol 42(4):981–987
29. Li L, Kong LY (2018) A new image encryption algorithm based on chaos. J Syst Simul 30:54–96
30. Min FH, Wang ZL, Wang ER (2016) New memristor chaotic circuit and its application to image encryption. J Electron Inf Technol 38:2681–2688
31. Zhu CX, Hu YP, Sun KH (2012) New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern. J Electr Info Technol 34(7):1735–1743
32. N. Pratyusha, S. Mandal. Design and Implementation of a Novel Circuit-Based Memristive Non-autonomous Hyperchaotic System with Conservative and Offset Boosting for Applications to Image Encryption, Circuits Syst Signal Process (2023).
33. Yan SH, Li L, Gu BX, Cui Y, Wang JJ, Song JC (2023) Design of hyperchaotic system based on multi-scroll and its encryption algorithm in color image. Integration 88:203–221
34. Rech PC (2022) Self-excited and hidden attractors in a multistable jerk system. Chaos Solitons Fractals 164:112614
35. Longhao Xu, Zhang J (2022) A Novel four—Wing chaotic system with multiple attractors based on hyperbolic sine: application to image encryption. Integration 87:313–331
36. Yan SH et al. (2022) Multi-scroll fractional-order chaotic system and finite-time synchronization. Phys Scripta, 97
37. Lola M, Kengne R, Pelap F (2023) Bursting phenomenon and chaos phase control in plant dynamics. Complexity

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