

# **A novel asymmetrical double-wing hyperchaotic system with multiple diferent attractors: application to fnite-time synchronization and image encryption**

**Jie Zhang1,2  [·](http://orcid.org/0000-0001-8690-4307) Longhao Xu1,2**

Received: 16 December 2021 / Revised: 2 September 2022 / Accepted: 12 March 2023 / Published online: 22 March 2023 © The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

## **Abstract**

In this paper, a novel asymmetrical double-wing third order hyperchaotic system is humbly proposed. The dynamic behavior of the system is greatly abundant after properly analyzing the phase diagram, bifurcation diagram, Lyapunov exponents spectrum, Poincare section diagram, and complexity. In addition, chaotic attractors under diferent parameters of the system are analyzed. In the dynamic analysis of the new system, it is found that the new system has some characteristics, like multi-stability, multi-state transition phenomenon, multiple attractors coexist. These features possess the value of in-depth analysis compared to previous systems and can make it promising for more applications. It is extraordinary attention for this new chaotic system, due to exist on multi-state transition phenomenon. The circuit diagram of the system is designed and implemented. Simultaneously, the circuit of the system is engineered and accomplished by using Multisim circuit simulation software. Furthermore, the limited time synchronization for the system is studied and carried out by an appropriate controller. Ultimately, algorithm of image encryption, novel and efficient, is designed by combining DNA dynamic encryption. The chaotic sequence of the current system is used to encrypt the image, and the key space, encrypted histogram, adjacent pixel correlation, robustness and information entropy are analyzed. The excellent performance analysis results further indicate that this hyperchaotic system has important reference value in the chosen feld of chaotic image encryption and synchronization.

**Keywords** Hyperchaotic system · Dynamical analysis · Circuit implementation · Finitetime synchronization · DNA dynamic coding

 $\boxtimes$  Jie Zhang zhangjie@nwnu.edu.cn

> Longhao Xu xlh1998666@foxmail.com

<sup>&</sup>lt;sup>1</sup> School of Physics and Electronic Engineering, Northwest Normal University, Lanzhou 730070, China

<sup>&</sup>lt;sup>2</sup> Gansu Province Intelligent Information Technology and Application Engineering Research Center, Lanzhou 730070, China

### **1 Introduction**

Over the past three decades, the chaos theory and its application have attracted frequently of consideration [\[25,](#page-23-0) [36,](#page-23-1) [42\]](#page-23-2). It is extremely rapid for chaotic systems, multifarious dissipative and conservative, to design and come true [\[28,](#page-23-3) [29](#page-23-4), [44,](#page-23-5) [53](#page-23-6)–[55](#page-24-0)]. In 2021, Han Xin-tong et al. designed a new fractional order system and implemented it with DSP [[21](#page-22-0)]. Yang Yan et al. proposed and designed a multidimensional system with multiple equilibrium points [[59](#page-24-1)]. In 2022, Bao Bo-cheng et al. designed no-argument memristive hyper-jerk system and its coexisting chaotic bubbles boosted by initial conditions [[5\]](#page-22-1). Chen Ming-shu et al. found a novel memristive chaotic system without any equilibrium point [\[14](#page-22-2)]. These works have contributed considerably to the aspect of chaos, both in terms of system construction methods and applications of the system. However, the dynamical representation of some of the systems has remained up until now relatively less in terms of dynamics and lacks some properties. This paper refers to some classical systems, like Chen system [[11](#page-22-3)], Lü system [[39](#page-23-7)], Sprott system [\[47\]](#page-23-8), Rucklidge system [[62](#page-24-2)], etc. After understanding a variety of methods to construct the system, a novel asymmetric two-wing hyperchaotic system with multiple attractors is proposed, which contains some basic dynamical manifestations. In addition, it has some properties such as multistability, attractor coexistence, multiple state transitions.

Since hyperchaotic systems exhibit the following characteristics: autonomous systems with at least four-dimensional phase space are dissipative and possess at least two or more positive Lyapunov exponents. Therefore, hyperchaotic systems have higher unpredictability, greater randomness, more key parameters, and more complex topology and evolutionary behavior than low-dimensional chaotic systems [\[17\]](#page-22-4). On the other hand, their phase space is more difficult in reconstruction due to the existence of multiple positive Lyapunov exponents, and thus they are reliably secure in use for signal encryption, confdential communication and system synchronization. There is still a little less research on the aspect of hyperchaotic systems than chaotic systems, so there is a need for more research on hyperchaotic systems. After considering the comparative methods in some literatures [\[6](#page-22-5), [7,](#page-22-6) [9](#page-22-7)], this paper also compares the systems in much literature. Moreover, the asymmetric double-wing system proposed in this paper obtains a hyperchaotic system, which can be studied more.

Chaotic synchronization is one of the considerable felds of chaotic systems. Synchronization methods are principally known in the following categories, for instance, adaptive synchronization [[37](#page-23-9)], intermittent feedback synchronization [[51](#page-23-10)], state observer synchronization [\[20\]](#page-22-8), chaos observer synchronization [[60](#page-24-3)], projective synchronization [\[63\]](#page-24-4). However, the aforementioned studies are all involved asymptotic synchronization and infnite convergence time [\[34\]](#page-23-11). Sun Jun-wei et al. realized fnite time synchronization of two sophisticated systems by using sliding mode control method [[48](#page-23-12)]. Shi Lei, Wang Lei-min et al., studied the finite time synchronization between multidimensional systems  $[4, 45, 52]$  $[4, 45, 52]$  $[4, 45, 52]$  $[4, 45, 52]$  $[4, 45, 52]$  $[4, 45, 52]$  $[4, 45, 52]$ . However, there are few related research, so it is of considerable value to further study the synchronization method of chaotic system. In this paper, the novel hyperchaotic system is combined with a fnite time synchronization method to realize its fnite time synchronization.

Chaotic systems have various real-world applications, like random number generators, communication, synchronization, and image encryption [\[16,](#page-22-10) [50\]](#page-23-15). Digital images are characterized by large amount of data and direct correlation between pixels and chaotic system has randomness, so it has certain advantages to apply chaotic system to image encryption [[35](#page-23-16)]. Cun Qi-qi et al. proposed an innovative alternative method of DNA encryption [[15](#page-22-11)]. Uzair Aslam Bhatti has delivered many contributions to image encryption algorithms, such as the

hybrid watermarking algorithm using Cliford algebra, Arnold perturbation and chaotic encryption [[8](#page-22-12)], and hyperspectral image classifcation based on spatial and spectral fusion of local similarity [\[10\]](#page-22-13). Gurpreet Kaur et al. studied fractional and based color image encryption algorithm [\[31\]](#page-23-17). Tanveer et al. discovered and studied 4D chaotic system and successfully developed it in the feld of image encryption [[22](#page-22-14)]. These works represent enormous contributions to chaotic digital image encryption. However, some of them still need continuing to optimize their image encryption methods, and some literature does not provide a comprehensive analysis of the encrypted images.

Based on the foregoing considerations, we present a novel asymmetrical double-wing third order hyperchaotic system in this paper. There are many special dynamics phenomena in this new system, like multi-stability, control of diferent initial values, high complexity, polymorphic transition. At the same time, this system has multiple equilibrium points, which means it has good homogeneous multiple stabilities and multiple attractors. This has been unobserved before in other hyperchaotic systems. In addition, the physical circuit of the system is designed and implemented. Last but not the least, a new image encryption algorithm is designed by combining the sequence of hyperchaotic system with DNA dynamic coding.

The rest of the paper is organized as follows. In the Section [2](#page-2-0), the equation model, phase diagram and sequence diagram of the new system are introduced. Section [3](#page-3-0) analyzes in detail the dynamical properties of the system and the state changes of the attractor of the chaotic system. Section [4](#page-6-0) implements the physical circuit of the hyperchaotic system. In the Section [5,](#page-9-0) finite-time synchronization of the chaotic system is designed and implemented. Section [6](#page-12-0) is the complete image encryption algorithm for the new system. Section [7](#page-17-0) is the performance analysis of the encrypted images and the comparison with other algorithms. Finally, the results of the study are summarized, and conclusions are drawn.

### <span id="page-2-0"></span>**2 New hyperchaotic system**

The three-dimensional hyperchaotic system is designed in this paper which has good chaotic behavior, and its system equation is as follows:

<span id="page-2-1"></span>
$$
\begin{cases}\n\frac{dx}{dt} = -ax + by - yz - c \\
\frac{dy}{dt} = dx + y \\
\frac{dz}{dt} = x - z + y^2\n\end{cases}
$$
\n(1)

Where *x*, *y* and *z* are system variables, *a*, *b*, *c,* and *d* are system parameters. The choice of parameters is of immense importance for system, and nonlinear systems with independent parameters will be in diverse states. To enrich the states of chaotic systems, we combine chaotic circuits, phase diagrams, bifurcation diagrams, Lyapunov exponential spectra to determine the system parameters in a comprehensive way. The chaotic dynamics of a nonlinear system occur only at some specifc parameters. When changing the system parameters, the nonlinear system can be in a periodic, quasi-periodic or chaotic state.

When the parameters of the system are  $a=4$ ,  $b=10$ ,  $c=1$ ,  $d=1$  and the initial value is (1, 1, 0), complex hyper-chaos exists in the system. The chaotic attractor of the system is shown in Fig. [1.](#page-3-1) It can be discovered that the phase diagram of the system is asymmetric with two vortexes, one is tremendous, and the other is small. In addition, the sequence diagram of each



<span id="page-3-1"></span>**Fig. 1** Hyperchaotic systems with fxed initial values and parameters. (**a**) Spatial phase diagram of the system. (**b**) Sequence diagram of chaotic variables

variable can equally be seen. At the same instant, the system proposed in this paper is compared with other systems in some respects as shown in Table [1](#page-3-2), which also demonstrates the rich dynamic behavior of the system from the side.

## <span id="page-3-0"></span>**3 Dynamical analysis of hyperchaotic system**

### **3.1 Dissipation of attractor**

The divergence  $(\nabla V)$  for the system ([1](#page-2-1)) is obtained from the system eq. (1)

$$
\nabla V = \frac{\partial x}{\partial x} + \frac{\partial y}{\partial y} + \frac{\partial z}{\partial z} = -a + 1 - 1 = -4
$$
 (2)

The  $\nabla V < 0$ , so the system is dissipative and  $\frac{dv}{dt} = e^{-4t}$  converges exponentially. When *t*→∞, every trajectory of the system shrinks exponentially to zero. At this point, all the

References	The system dimension Circuit structure Dynamic behavior		
The literature of $[27]$ 4D chaotic system		Complex	Chaotic bursting, multiple attractors coexist
The literature of $[57]$ 3D chaotic system		Simple	Chaotic bursting
The literature of $\left[32\right]$ 5D chaotic system		Complex	Extreme multistability
The literature of $[40]$	4D chaotic system	Complex	Attractor coexistence, multiple stability
The literature of [2]	5D chaotic system	Complex	Extreme multistability
The proposed system	4D chaotic system	Simple	Chaotic bursting, multi-stability, multiple attractors coexist, multiple state transitions

<span id="page-3-2"></span>**Table 1** Comparison of dynamic behavior of other systems

## **3.2 Equilibrium point**

To fnd the equilibrium point of the system, set system equation equal to zero. The system as follows:

$$
\begin{cases}\n-ax + by - yz - c = 0 \\
dx + y = 0 \\
x - z + y^2 = 0\n\end{cases}
$$
\n(3)

When variables for the system are  $a=4$ ,  $b=10$ ,  $c=1$ ,  $d=1$ , the equilibrium set of the system are *S*<sub>1</sub>=(3.31467, −3.31467,14.3017); *S*<sub>2</sub>=(−4.24357, 4.24357, 13.7643); *S*<sub>3</sub>= (−0.071093, 0.071093, −0.06603). The Jacobian matrix obtained by linearizing the system.

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

Let det  $(J – \lambda I) = 0$ , *I* is the identity matrix. The eigenvalues of the three equilibrium points for the system are obtained respectively, and the specifc values are shown in Table [2](#page-4-0). There is a real eigenvalues  $\lambda_1$  and a pair of complex conjugate characteristic roots  $\lambda_2$ ,  $\lambda_3$ in the equilibrium points of  $S_1$  and  $S_2$ . According to Lyapunov stability theory,  $S_1$  and  $S_2$ are saddle focal equilibrium points, which are very important for chaotic system. For many chaotic systems, such equilibrium points are the prerequisite for the generation of vortex motion. In equilibrium point  $S_3$ ,  $\lambda_1$ ,  $\lambda_3$  are negative and  $\lambda_2$  is positive, so this equilibrium point is an unstable saddle point.

### **3.3 Lyapunov exponent, dimension, and bifurcation**

Lyapunov index can quantitatively represent the motion state characteristics of the system and vividly describe the degree of attraction and repulsion between adjacent trajectories of the system, which is the most important physical quantity for describing chaotic systems. When the parameters in the system change, the curve in the Lyapunov exponential spectrum of the system describes the change of the system's motion state. When the parameters are set,  $a=4, b=10, c=1, d=1$  in the system, Lyapunov index  $(LE_i)$  is calculated by MATLAB and obtained:  $LE_1 = 0.7291$ ,  $LE_2 = 0.3993$ ,  $LE_3 = -4.12$ . The Lyapunov dimension  $(D_1)$  of the system is  $D_l$  = 2.2738, indicating that the system is in the fractal dimension. At the same time, it can also be shown that the system is in hyperchaotic state by the Lyapunov exponent.

λ	$\lambda_1$	$\Lambda$	$\Lambda_3$
$S_1$	$-5.0186$	$0.5093 + 2.199i$	$0.5093 - 2.199i$
$S_2$	$-4.1449$	$0.0725 + 2.7574i$	$0.0725 - 2.7574i$
$S_3$	$-5.5269$	2.5351	$-1.0083$

<span id="page-4-0"></span>**Table 2** Eigenvalues of each equilibrium point

$$
D_L = j + \frac{1}{|LE_{j+1}|} \sum_{i=1}^{j} LE_i = 2 + \frac{LE_1 + LE_2}{LE_3} = 2.2738
$$
 (5)

Bifurcation refers to the phenomenon that the dynamic state of the system will change with the change of the system parameters or the initial value of the state variable. Lyapunov exponential spectrum and bifurcation diagram of the system change with the change of different parameters. When other parameters of the system remain unchanged, parameter *c* is selected to analyze the dynamic behavior. Figure [2](#page-5-0) shows the Lyapunov exponential spectrum and bifurcation diagram of the system with  $c$  as a variable. The curves in the Fig. [2](#page-5-0) are downward as  $LE_1$ ,  $LE_2$  and  $LE_3$ .

In addition, diferent periodic bifurcation also appears in the variation of system parameter *c*. The various variations of the chaotic attractor (x-y plane) are shown in Fig. [3.](#page-8-0) It can be seen from the observation of the curves that when  $c\in(-10,-5.5)$ , the curves  $LE_1$ and 0 are basically in coincidence state, and  $LE_1$ ,  $LE_2$  and  $LE_3$  are both less than 0. When  $c\in(-5.2,-2.95)$ , the curve *LE*<sub>1</sub> continues to rise, the curve *LE*<sub>2</sub> tends to be flat, but both are still greater than 0,  $LE_3$  less than 0, the system is hyperchaotic. When  $c \in [-2.95, -2.9]$ , the curve  $LE_1$  is still greater than 0, and the curve  $LE_2$  drops rapidly and less than 0,  $LE_3$ is less than 0, the system is chaotic. Furthermore, when  $c \in [1.65,1.7]$ , or  $c \in [3.3,3.4)$ , or *c*∈ [6.55,7.05], the system is chaotic. When *c* = −7.5, the system is in the period state (Fig. [3a](#page-8-0)). When  $c = -5.5$ , single wing transient chaotic state (Fig. [3](#page-8-0)b) is observed in the system. When  $c = -5.3$ , The system changes from single wing transient chaotic state to double wing transient chaotic state (Fig. [3c](#page-8-0)). When the value of  $c$  increases to −1, the system becomes double wing hyperchaotic state (Fig. [3](#page-8-0)d). When  $c=3.5$ , the system is in a double wing periodic state (Fig. [3e\)](#page-8-0). When increasing  $c=6$ , single wing periodic oscilla-tion (Fig. [3](#page-8-0)f) is observed in the system. When  $c=10$ , single wing periodic state (Fig. [3g](#page-8-0)) appears in the system. Continue to increase parameter  $c$  to  $c = 15$ , the system evolves into quasi-periodic state (Fig. [3](#page-8-0)h). When  $c \in [15.1, 20]$ , the curve  $LE_1$  tends to a flat straight-line state, and curve  $LE<sub>2</sub>$  drops gently. The system gradually enters a limit period state. As the parameter *c* changes, it is found that the system exhibits various chaotic attractors.



<span id="page-5-0"></span>**Fig. 2** System bifurcation diagram and Lyapunov exponential spectrum with parameter *c*. (**a**) Bifurcation diagram, (**b**) Lyapunov exponents spectra

#### **3.4 System complexity**

The study of the complexity of chaotic systems is regarded as an important part of system dynamics analysis. The complexity algorithm is used to try out the closeness between chaotic sequence and random sequence. The higher the complexity, the better the system. According to the complexity of correlation algorithm, the more similar it is to a random sequence, the higher the complexity of the system. The complexity of chaotic sequences can be divided into behavior complexity and structure complexity. Among them,  $C_0$  and *SE* algorithms belong to structural complexity, and their results have global statistical signifcance compared with behavior complexity.

In Fig. [4,](#page-8-1) the system complexity under a single parameter is frst tested. On the premise that other system parameters remain unchanged, the complexity of  $C_0$  and *SE* of the system can be obtained by changing system parameter *b*, as shown in Fig. [4](#page-8-1)a and b respectively. As can be seen from the figure, when  $b = 10$ , the  $C_0$  complexity of the system is 0.06410, and the *SE* complexity is 0.397. Similarly, when we change the system parameter  $c$ , we can see that its complexity is not as high as that of  $b$ , but the complexity of  $C_0$  is generally above 0.04, and the complexity of *SE* fuctuates greatly, but it is also above 0.25. The complexity of the system was also tested for diferent initial values, when the system parameters were  $a = 4$ ,  $b = 10$ ,  $c = 1$ , and  $d = 1$ . The test values are shown in Table [3](#page-9-1). It is found that no matter how the initial value of the system changes, the  $C_0$  complexity of the system is stable above 0.06400. In addition, after comparing the complexity of other literature systems, it is found that the complexity of this system is greater than that of other systems, indicating that the complexity of other systems is higher.

Moreover, two system parameters are selected to calculate the complexity of the system. In the Fig. [5](#page-9-2), the darker the color, the more complex the system. In addition,  $C_0$  complexity and *SE* complexity have good consistency in the same parameter variation. In the Fig. [5](#page-9-2)a and b, when the system parameters  $c \in (8, 10)$  and  $d \in (8, 9)$ , the highly complex region is mainly on *c*∈(8, 9.8), *d*∈(8.1, 9). According to the multivariable complex chaos diagram, the change of the system can be seen more concretely. When other parameters remain unchanged and system parameters  $b$  and  $c$  are changed, the complexity of  $C_0$  and  $SE$  of the system is shown in Fig. [5c](#page-9-2) and d. It can be observed that the complexity graph of system parameters *b* and *c* is darker than that of parameters *c* and *d*, indicating that the complexity of *b* and *c* is higher.

### <span id="page-6-0"></span>**4 Circuit design and realization**

After the theoretical analysis and numerical simulation, the circuit design is typically started in this completed the section to further observe the dynamic behavior of the complex system. When properly designing the independent circuit, the system eq. ([1\)](#page-2-1) is frstly transformed by proportional compression. Set  $R_X \rightarrow X$ ,  $R_Y \rightarrow Y$ ,  $R_Z \rightarrow Z$ , R is the variable proportional compression factor. Correctly assuming *R*=0.5, the changed equation in common is eq.  $(6)$  $(6)$  $(6)$ .

<span id="page-6-1"></span>
$$
\begin{cases}\n\frac{dX}{dt} = -ax + by - eyz - c \\
\frac{dy}{dt} = dx + y \\
\frac{dz}{dt} = x - z + fy^2\n\end{cases}
$$
\n(6)





<span id="page-8-0"></span>**Fig. 3** System attractor diagram with parameter *c*. (**a**) Single-wing period state attractor for *c*=−7.5, (**b**) ▸ Single-wing transient chaos state attractor for  $c = -5.5$ , (**c**) Transient transition attractor for  $c = -5.3$ , (**d**) Hyperchaotic attractor for  $c=-1$ , (**e**) Double-wing periodic state attractor for  $c=3.5$ , (**f**) Single-wing periodic attractor for  $c = 6$ , (**g**) Periodic attractor for  $c = 10$ , (**h**) Quasi-periodic state attractor for  $c = 15$ 

The system parameters are  $a=4$ ,  $b=10$ ,  $c=1$ ,  $d=1$ ,  $e=2$ ,  $f=2$ , respectively. Time scale trans-formation is performed on eq. [\(6\)](#page-6-1), let  $T = \tau_0 t$  and  $\tau_0 = \frac{1}{R_5 C_1} = \frac{1}{R_{11} C_2} = \frac{1}{R_{18} C_3}$ , where  $\tau_0$  is the time scale change factor. The transformed equation and schematic diagram are obtained.

<span id="page-8-2"></span>
$$
\begin{cases}\n\frac{dX}{dT} = \frac{1}{R_S C_1} \cdot \frac{R_2}{R_6} \left( -\frac{R_4}{R_1} X + \frac{R_4}{R_3} Y - 0.1 \frac{R_4}{R_2} Y \cdot Z - 1 \cdot \frac{R_4}{R_{21}} \right) \\
\frac{dY}{dT} = \frac{1}{R_{11} C_2} \cdot \frac{R_{13}}{R_{12}} \left( \frac{R_{10}}{R_8} X + \frac{R_{10}}{R_9} Y \right) \\
\frac{dZ}{dT} = \frac{1}{R_{18} C_3} \cdot \frac{R_{20}}{R_{19}} \left( \frac{R_{17}}{R_{16}} X - \frac{R_{17}}{R_{15}} Z + 0.1 \frac{R_{17}}{R_{14}} Y \cdot Y \right)\n\end{cases} (7)
$$

Set  $C_1 = C_2 = C_3 = 33nF$ , the following parameter values,  $R_5 = R_{11} = R_{18} = 50K\Omega$ ,  $R_3 = R_6 = R_7 = 10K\Omega$ ,  $R_{12} = R_{13} = R_{19} = R_{20} = 10K\Omega$  and  $R_4 = R_8 = R_9 = R_{10} = R_{21} = 100K\Omega$ ,  $R_{15}=R_{16}=R_{17}=100K\Omega$  and  $R_1=25K\Omega$ ,  $R_2=R_{14}=5K\Omega$ , can be obtained by comparing eqs. ([6](#page-6-1)) and [\(7\)](#page-8-2).



<span id="page-8-1"></span>**Fig. 4** System complexity. (**a**) The  $C_0$  complexity of parameter *b*. (**b**) *SE* complexity with *b*. (**c**)  $C_0$  complexity with *c.* (**d**) *SE* complexity with *c*

<span id="page-9-1"></span>

Through simulation verifcation on circuit simulation software Multisim, the phase diagram of the system is sufficiently shown in Fig.  $6$ . The theoretical attractor is similar to the circuit attractor by carefully comparing the Fig. [1](#page-3-1) and the Fig. [6](#page-10-0). Therefore, the possible existence of attractors is confrmed by numerical analysis and experimental study.

## <span id="page-9-0"></span>**5 Synchronization implementation**

In this section, system  $(8)$  $(8)$  $(8)$  is taken as the drive system and system  $(9)$  as the response system, a fnite time synchronization mode of the system is realized. The model parameters in system



<span id="page-9-2"></span>**Fig. 5** System complexity. (**a**)  $C_0$  complexity,  $c \in (8,10)$ ,  $d \in (8,9)$ . (**b**) *SE* complexity,  $c \in (8,10)$ ,  $d \in (8,9)$ . (**c**) *C*<sub>0</sub> complexity, *b*∈(0,10), *c*∈(0,2). (**d**) *SE* complexity, *b*∈(0,10), *c*∈(0,2)

 $\bigcirc$  Springer



<span id="page-10-1"></span> $(b)$ 

<span id="page-10-0"></span>**Fig. 6** System circuit schematic diagram and simulation diagram

 $\epsilon$ 

([9](#page-10-2)) are the same as those in system [\(8\)](#page-10-1), and  $U_1$ ,  $U_2$  and  $U_3$  are the control inputs. The specific synchronization method is as instantly follows:

$$
\begin{cases}\n x_1 = -ax_1 + bx_2 - x_2x_3 - c \\
 x_2 = dx_1 + x_2 \\
 x_3 = x_1 - x_3 + x_2^2\n\end{cases}
$$
\n(8)

$$
\begin{cases}\n y_1 = -ay_1 + by_2 - y_2y_3 - c + u_1 \\
 y_2 = dy_1 + y_2 + u_2 \\
 y_3 = y_1 - y_3 + y_2^2 + u_3\n\end{cases}
$$
\n(9)

In this synchronization, the error is defined as  $e_i = y_i - x_i (i = 1, 2, 3)$ , and the error dynamic system is system  $(10)$  $(10)$  $(10)$ J

$$
\begin{cases}\ne_1 = y_1 - x_1 \\
e_2 = y_2 - x_2 \\
e_3 = y_3 - x_3\n\end{cases}
$$
\n(10)

<span id="page-10-3"></span><span id="page-10-2"></span><sup>2</sup> Springer

<span id="page-11-0"></span>
$$
\begin{cases}\ne_1 = -ae_1 + be_2 - y_2y_3 + x_2x_3 + u_1 \\
e_2 = de_1 + e_2 + u_2 \\
e_3 = e_1 - e_3 + y_2^2 - x_2^2 + u_3\n\end{cases} (11)
$$

The controller design is as follows:

 $\epsilon$ 

$$
\begin{cases}\n u_1 = -k_1 e_1 - k_2 \operatorname{sgn} (e_1) |e_1|^{\mu} + (y_2 y_3 - x_2 x_3) \\
 u_2 = -k_1 e_2 - k_2 \operatorname{sgn} (e_2) |e_2|^{\mu} - (d+b)e_1 \\
 u_3 = -k_1 e_3 - k_2 \operatorname{sgn} (e_3) |e_3|^{\mu} + (x_2^2 - y_2^2 - e_1)\n\end{cases} (12)
$$

 $k_1, k_2$  is a constant,  $0 < \mu < 1$ . sgn is the step function, if the parameters satisfy  $k_1 \ge \max\{a, 0\}$ ,  $k<sub>2</sub>$  > 0, then the finite time synchronization can be fulfilled for the system through the controller. Now, using the Lyapunov function and eq. [\(11\)](#page-11-0), its derivative can be obtained.

<span id="page-11-1"></span>
$$
v = \frac{1}{2} \sum_{i=1}^{3} e_i^2
$$
  
\n
$$
v = e_1 e_1 + e_2 e_2 + e_3 e_3
$$
  
\n
$$
= e_1 [-ae_1 + be_2 - y_2 y_3 + x_2 x_3 + u_1]
$$
  
\n
$$
+ e_2 [de_1 + e_2 + u_2] + e_3 [e_1 - e_3 + y_2^2 - x_2^2 + u_3]
$$
  
\n
$$
= e_1 [-ae_1 + be_2 - y_2 y_3 + x_2 x_3] + e_2 [de_1 + e_2] +
$$
  
\n
$$
e_3 [e_1 - e_3 + y_2^2 - x_2^2] + e_1 u_1 + e_2 u_2 + e_3 u_3
$$
\n(13)

Plug  $U_1$ ,  $U_2$  and  $U_3$  into eq. [\(13](#page-11-1)), get

$$
v = -ae_1^2 + be_1e_2 - y_2y_3e_1 + x_2x_3e_1 +\nde_1e_2 + e_2^2 + e_1e_3 - e_3^2 + e_3y_2^2 - e_3x_2^2 +\n[-k_1e_1^2 + e_1y_2y_3 - e_1x_2x_3 - e_1k_2 \text{ sgn}(e_1)|e_1|^{\mu}]\n+ [-k_1e_2^2 - (d+b)e_1e_2 - e_2k_2 \text{ sgn}(e_2)|e_2|^{\mu}] +\n[-k_1e_3^2 + x_2^2e_3 - y_2^2e_3 - e_1e_3 - e_3k_2 \text{ sgn}(e_3)|e_3|^{\mu}]\n= -(k+a)e_1^2 + (1-k)e_2^2 - (1+k)e_3^2 -\nk_2(|e_1|^{\mu+1} + |e_2|^{\mu+1} + |e_3|^{\mu+1})
$$
\n(14)

Here, two lemmas are introduced as follows [\[51](#page-23-10)]:

Lemma 1

If there is a constant $t_1 > 0$ , such that  $\lim_{t \to t_1} |e_i| = 0$  and when  $t \ge t_1$ ,  $|e_i| = 0$  (*i*=1,2,3), finite time synchronization is implemented.

If there is a positive definite differential function  $V(t)$  that satisfies eq. ([15](#page-11-2)):

<span id="page-11-2"></span>
$$
V(t) \le \varepsilon V^{\theta}(t), \forall t \ge 0, V(t_0) \ge 0
$$
\n(15)

Where  $\varepsilon$  and  $\theta$  are constants, in addition  $\varepsilon > 0$ ,  $0 < \theta < 1$ , then the function  $\forall t$  satisfies.

$$
V^{1-\theta}(t) \le V^{1-\theta}(t_0) - \varepsilon (1-\theta)(t-t_0), t_0 \le t \le t_1
$$
 (16)

and when ∀ $t \geq t_1$ ,

 $\mathcal{D}$  Springer

$$
V(t) \equiv 0,\tag{17}
$$

$$
t_1 \le t_0 + \frac{V^{1-\theta}(t_0)}{\varepsilon(1-\theta)}.\tag{18}
$$

Lemma 2

For any real numbers  $\tau_1, \ldots, \tau_n$  and  $0 < \alpha < 1$ , there are the following inequalities

$$
\sum_{i=1}^{n} |\tau_i|^{\alpha+1} \ge \left(\sum_{i=1}^{n} |\tau_i|^2\right)^{\frac{\alpha+1}{2}}
$$
 (19)

According to Lemma 1 and 2

$$
\nu \le -k_2 \left( \left| e_1 \right|^{\mu+1} + \left| e_2 \right|^{\mu+1} + \left| e_3 \right|^{\mu+1} \right) \tag{20}
$$

then

$$
\left( |e_1|^{\mu+1} + |e_2|^{\mu+1} + |e_3|^{\mu+1} \right) \ge \left( |e_1|^2 + |e_2|^2 + |e_3|^2 \right)^{\frac{\mu+1}{2}}
$$
\n
$$
\dot{v} \le -k_2 \left( |e_1|^2 + |e_2|^2 + |e_3|^2 \right)^{\frac{\mu+1}{2}}
$$
\n
$$
\le -k_2 (2\nu)^{\frac{\mu+1}{2}} \le -2^{\frac{\mu+1}{2}} k_2 \nu^{\frac{\mu+1}{2}}
$$
\n(21)

then

<span id="page-12-1"></span>
$$
t_1 \le \frac{\left(v(t_0)\right)^{\frac{1-\mu}{2}}}{2^{\frac{\mu-1}{2}}k_2(1-\mu)} \le \frac{\left[\frac{1}{2}\sum_{i=1}^3 e_i^2(0)\right]^{\frac{1-\mu}{2}}}{2^{\frac{\mu-1}{2}}k_2(1-\mu)}\tag{22}
$$

Based on the lemma above, the system can achieve fnite synchronization. If constants  $(x_1, x_2, x_3) = (1, 1, 0), (y_1, y_2, y_3) = (35, 20, -1), \mu = \frac{1}{2}, k_1 = 4, k_2 = \frac{1}{4}$  are set, the synchro $n_1, n_2, n_3, \ldots, n_r, \ldots, n$ perceived from Fig. [7](#page-13-0) that the error state converges to zero in fnite time, so fnite time synchronization, the driving system ([8\)](#page-10-1) and the response system [\(9](#page-10-2)), can be achieved.

## <span id="page-12-0"></span>**6 System image encryption**

As shown in Fig. [8,](#page-13-1) the image encryption algorithm is mainly divided into three key parts in this paper: generating initial chaotic values related to chosen plaintext and generating pseudo-random sequences; Local Graph Structure (LGS) algorithm is intentionally used to select the region of the explicit image; and then fnally, DNA encryption and secondary scrambling.



<span id="page-13-0"></span>**Fig. 7** System finite-time synchronization errors  $e_1$ ,  $e_2$ ,  $e_3$ 

### **6.1 LGS selection algorithm**

LGS image selection was proposed by Eimad Abdu Abusham [[1\]](#page-22-18), and the specifc formula is as follows:

$$
\begin{cases}\nLGS(\chi_d, y_d) = \sum_{k=0}^{0} s(g_{d+1+p} - g_{d+p}) 2^{7-p} \\
s(x) = \begin{cases}\n1, x \ge 0 \\
0, x < 0\n\end{cases} \\
p = 7, ..., 0\n\end{cases}
$$
\n(23)

Where  $(x_d, y_d)$  represents any two adjacent pixel values in the picture. Since more image details can be preserved by the algorithm and there are exactly 8 binary sequences. The principle of the LGS algorithm is described below. In Fig. [9](#page-14-0)a, When the pixel value is 125, the consecutiveness



<span id="page-13-1"></span>**Fig. 8** Image encryption fowchart



<span id="page-14-0"></span>**Fig. 9** LGS algorithm selection process

begins along the red arrow path in the upper left corner. As it moves along, if the next value is greater than the current value, zero is going to represent it, otherwise one will represent it. Finally, a binary sequence is obtained, and it became decimal by converting. In addition, we set the threshold for image selection as 128. In the image selection, if last decimal value is equivalent or greater than the set value, the initial information of the image is preserved. The binary sequence '10101011' is generated at pixel 125 in Fig. [9](#page-14-0)b. It is converted to decimal to 171 greater than the threshold of 128 for this article. In this manner, the pixel value for this point should be retained. The binary sequence selected by LGS algorithm for pixel value 90 is '00101001', and the fnal decimal is 41. Since it is less than 128, zero is set to be the value at this point. This manipulation is repeated, resulting in a vivid text image of the selected region.

### **6.2 Full encryption algorithm**

Step1: According to the original image, the plaintext matrix is obtained and then converted into the corresponding plaintext sequence.

Step 2: *Ode45* algorithm is used to calculate the initial value of the chaotic system and iterate the chaotic system. For better randomness, the frst 1500 terms were removed, resulting in three chaotic sequences  $\{x_i, y_i, z_i\}$ .

Step 3: Because 0–255 is the pixel value of the image, therefore the pseudo-random sequence  $\{x_i, y_i, z_i\}$  are converted to 0–255 values. Sequence  $Z_i$  can be applied in DNA encryption operations,  $Z_i$  is converted to 1–3. The expression is shown below.

$$
\begin{cases}\nX_i = \text{mod (floor}((50 + a \sin(x_i)/\pi) \times 65536), 256) \\
Y_i = \text{mod (floor}((50 + a \sin(y_i)/\pi) \times 65536), 256) \\
Z_i = \text{mod (floor}((50 + a \sin(z_i)/\pi) \times 65536), 3) + 1\n\end{cases}
$$
\n(24)

Where *floor*() stands for taking the whole function.

Step 4: LGS algorithm and the above formula are used to process the plaintext image, which is converted into binary and then into decimal, and a matrix *H* of *M*×*N* is obtained.

Step 5: Eq. ([25\)](#page-14-1) determines the formation of *H* matrix. The matrix contains selected areas and unselected areas of the image.

$$
p(i,j) = \begin{cases} H(i,j), H(i,j) \ge 128\\ 0, H(i,j) < 128 \end{cases} \tag{25}
$$

<span id="page-14-1"></span> $\mathcal{D}$  Springer

Step 6: The matrix  $H$  is preprocessed with pseudo random sequence  $Y_i$ , and the two-dimensional matrix *E* is output. Then, formula ([25](#page-14-1)), [\(26\)](#page-15-0) and [\(27\)](#page-15-1) are used to encode the DNA of the selected region and sequence *Xi* .

$$
E_1(i,j) = \begin{cases} DNA\_code(E(i,j),code\_number), P(i,j) \neq 0\\ E(i,j), P(i,j) = 0 \end{cases}
$$
 (26)

<span id="page-15-1"></span><span id="page-15-0"></span>
$$
X'_{i}(k) = DNA\_code(X_{i}(k), code\_number'
$$
\n(27)

Where *code*\_*number*≠*code*\_*number*' , but it's all part of the eight ways DNA codes. Step 7: Sequence  $Z_i$  is used for DNA manipulation of selected regions and sequence $X_i$ .

$$
E_2(i,j) = \begin{cases} DNA\_operation(E_1(i,j), X_i(k), Z_i), P(i,j) \neq 0\\ E(i,j), P(i,j) = 0 \end{cases}
$$
(28)

The addition, subtraction, XOR and other operations are determined by sequence  $Z_i$  in DNA encryption. Tables [4,](#page-15-2) [5,](#page-15-3) [6,](#page-16-0) and [7](#page-16-1) show the detailed operation rules. Step 8: Decode according to the decoding number *decode*\_*number*.

$$
E_3(i,j) = \begin{cases} DNA\_decode(E_2(i,j), decode\_number), P(i,j) \neq 0\\ E(i,j), p(i,j) = 0 \end{cases}
$$
(29)

Where *decode*\_*number* also belongs to the eight encoding methods of DNA, but*decode*\_*number*≠*code*\_*number*, *decode*\_*number*≠*code*\_*number*' . This step is equivalent to encrypting the image for the selected region again.

Step 9: The two-dimensional matrix *R* of  $M \times N$  is obtained by transforming the sequence  $Z_i$ . Then perform XOR operations on  $E_3$  and the matrix  $Z_i$ .

$$
E_4(i,j) = E_3(i,j) \oplus R(i,j)
$$
 (30)

Step 10: Finally, the whole image is scrambled without repetition to obtain the encrypted image *H*. For encryption algorithm, its reverse process is decryption algorithm.

<span id="page-15-3"></span>

Base	$\boldsymbol{0}$	1	$\overline{2}$	3	$\overline{4}$	5	6	7
A	11	$00\,$	$00\,$	01	01	10	10	11
C	10	01	10	$00\,$	11	00	11	01
G	01	10	01	11	$00\,$	11	$00\,$	10
T	$00\,$	11	11	10	10	01	01	$00\,$
	Table 5 DNA addition rule							
			$^{+}$	А	G		$\mathcal{C}$	T
			A	A	G		$\Gamma$	T
			G	G	C		T	A
			$\mathcal{C}$	C	T		A	G

<span id="page-15-2"></span>**Table 4** DNA coding rules

<span id="page-16-0"></span>

Specific standard  $256 \times 256$  Lena, Baboon and familiar Peppers images are ordinarily used in the image encryption experiment. The encrypted image is shown in Fig. [10.](#page-16-2) Accurately compared with the original image, no image features are invariably found.

<span id="page-16-1"></span>



<span id="page-16-2"></span>**Fig. 10** Image encryption efect. (**a**), (**d**), (**g**) is the original image. (**b**), (**e**), (**h**) is encryption image. (**c**), (**f**), **i** is decrypted image

# <span id="page-17-0"></span>**7 Image security performance analysis**

# **7.1 Key space analysis**

Key space refers to the set of all legitimate keys. When the key space is large enough, exhaustive attack can be efectively resisted. Generally speaking, when the key space is larger than  $2^{100}$ , the security and adequate reliability of the encryption system will be guaranteed [[61](#page-24-7)]. In this encryption system, the private key is the initial value of the hyperchaotic system  $(X_0, Y_0, Z_0)$ , and the size for the calculated key space is  $2 \times 10^{60}$ , which is far larger than the above requirements.

# **7.2 Sensitivity analysis**

Whether the encryption algorithm is sensitive to the key is also one of the good performances. According to the encryption algorithm in this paper, the key parameter is  $(X_0, Y_0, Z_0)$ . On the premise of keeping two of them unchanged, the original image can be decrypted when  $Y_0$  becomes  $Y_0 + 10^{-16}$ . But when  $Y_0$  changes to  $Y_0 + 10^{-15}$  and is denoted as *Y*<sub>0</sub>, the plaintext image cannot be decrypted. In the same way, when  $Z_0$  becomes  $Z_0 + 10^{-15}$ , is called  $Z_0$ , the original image can't be decrypted. The results are presented Fig. [11](#page-17-1), and similar results occur when the remaining key parameters are tested. The consequences show that the proposed image encryption algorithm includes extraordinary key sensitivity.

# **7.3 Image histogram analysis**

It is a dominant statistical feature for the image. The histogram of the plaintext image is evenly undistributed, which shows the statistical features of the pixel. On the direct contrary, the histogram distribution of ciphertext image is more uniform. Figure [12](#page-18-0) of this system also conforms to the above characteristics.

# **7.4 Correlation coefficient calculation and analysis**

Correlation between images is equally signifcant for encryption algorithms. Principally, plaintext image has strong correlation between adjacent pixels in horizontal, vertical, and diagonal directions, while ciphertext image should have no correlation between adjacent pixels. The calculation formula remain as follows.



<span id="page-17-1"></span>**Fig. 11** Images decrypted with the wrong key and the right key respectively. (**a**) Decryption image of error key  $Y_0$ <sup>'</sup>, (**b**) Decryption image of error key $Z_0$ <sup>'</sup>. (**c**) Decryption image of the correct key



<span id="page-18-0"></span>**Fig. 12** Histogram of image. (**a**) Raw Lena image, (**b**) Encrypted Lena image

$$
\begin{cases}\n\gamma = \frac{\text{cov}(u, v)}{\sqrt{D(u)}\sqrt{D(v)}} \\
\text{cov}(u, v) = \frac{1}{N} \sum_{i=1}^{N} (u_i - E(u)) (v_i - E(v)) \\
D(u) = \frac{1}{N} \sum_{i=1}^{N} (u_i - E(u))^2 \\
E(u) = \frac{1}{N} \sum_{i=1}^{N} (u_i)\n\end{cases} (31)
$$

Where *U*and *V* stand for the values of any two adjacent pixels,  $E(U)$  and  $D(U)$ show the expectation and variance respectively. The previous Lena images before and after encryption are selected for correlation coefficient calculation, and the correlation coefficient diagram of the images before and after encryption is shown in Fig. [13.](#page-18-1) The plaintext images provide obvious correlation, while the corresponding ciphertext images are evenly distributed. The correlation coefficients of the image in horizontal, vertical, and diagonal directions before and after encryption were calculated. As shown in Table [8](#page-19-0), the archetypal image



<span id="page-18-1"></span>**Fig. 13** Correlation coefcient of image. (**a**) Plaintext horizontal, (**b**) Plaintext vertical direction, (**c**) Plaintext is diagonal, (**d**) Clear opposition to angular direction, (**e**) Ciphertext horizontal direction, (**f**) Ciphertext vertical direction, (**g**) The ciphertext is in the diagonal direction, (**h**) Ciphertext is opposed to angular direction

algorithm	horizontal	vertical	Positive diagonal	Negative diagonal
Lena image	0.98691	0.96872	0.96065	0.97033
Text encrypted image	0.00131	0.00075	0.00146	$-0.00117$
The literature of [43]	0.01511	0.00101	0.00403	$-0.00124$
The literature of [3]	0.00190	0.00180	0.00340	$-0.00121$
The literature of [33]	0.01022	0.02141	0.00562	$-0.00132$
The literature of [38]	0.00120	0.01530	0.00450	$-0.00122$
The literature of [41]	0.00270	0.01520	0.00711	$-0.00181$
The literature of $[18]$	0.00291	0.00412	0.00190	$-0.00194$

<span id="page-19-0"></span>**Table 8** Correlation coefficient comparison

has a strong correlation close to one in three directions, while the corresponding ciphertext image has uniformly distributed pixels and its correlation coefficient is close to zero.

### **7.5 Diference analysis**

A secure image encryption algorithm is exceptionally sensitive to any minor change in the plaintext image. That is, any change in a single pixel of the plaintext image will produce a completely diferent ciphertext image. Broadly, the sensitivity of encryption algorithm to plaintext information is measured by two indexes: pixel change rate (NPCR) and average change intensity of normalized pixel value (UACI). The calculation formula of NPCR and UACI is described as follows:

<span id="page-19-2"></span><span id="page-19-1"></span>
$$
NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%
$$
 (32)

$$
UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C'(i,j) - C(i,j)|}{255} \times 100\%
$$
 (33)

Where,  $C(i, j)$  and  $C(i, j)$  respectively represent the pixel gray values of the two ciphertext images at coordinates (*i*, *j*); *M* and *N* represent the height and width of the image, respectively.  $D(i, j)$  is defined as follows: if  $C(i, j) = C(i, j)$ ,  $D(i, j) = 1$ ; Otherwise,  $D(i, j) = 0$ .

The ciphertext image can be obtained by encrypting the image with the key in the algorithm. Subsequently arbitrarily select a pixel in the plaintext image, change its pixel value and get a new plaintext image. The similar key is used to encrypt the changed plaintext image to obtain another ciphertext image. According to eq. ([32](#page-19-1)) and eq. [\(33](#page-19-2)), a set of NPCR and UACI values can be obtained by calculating the above two ciphertext images, and the results are shown in Table [9](#page-20-0). After performing the previous method several times, the average value of NPCR and UACI can be obtained. The outstanding value of NPCR and UACI obtained by using the proposed algorithm is 99.62% and 33.43%, which is very close to the ideal expected value of NPCR and UACI.

#### **7.6 Robustness analysis**

Robustness analysis is the most essential criterion to measure the anti-interference capability of an encryption algorithm. In this paper, Lena image is selected for experimental analysis, and

<span id="page-20-0"></span>

noise attack and shear attack are used to test the robustness of the algorithm. 0.2 time and 0.05 time of salt and pepper noise were applied to the encrypted image respectively, and the decrypted image was shown in Fig. [14](#page-20-1)b and d. The decryption results of one-eighth and one-fourth encrypted images are shown in Fig. [14f](#page-20-1) and h. Compared with the experimental consequences, the encryption algorithm in this paper can still recover most of the original image information. It shows the algorithm can resist noise and shear attacks to a certain extent and has good robustness.

### **7.7 The information entropy**

The uncertainty of image is usually known by information entropy. The greater the entropy of information, the more information, the less visual information. The calculation formula of information entropy is as follows.

$$
H = -\sum_{i=0}^{2^{n}-1} p(s_i) \log_2 p(s_i)
$$
 (34)

Where,  $2^n$  shows all states for the pixel value in the image, and  $p(s_i)$  is the possibility of the pixel value in the whole image. If there are  $2<sup>n</sup>$  states of information, the entropy of information is *n*. For a standard image with 256 states, 8 would be ideal for its entropy of information. The encrypted image entropy of the system is 7.9986, which is very close to the theoretical value 8.



<span id="page-20-1"></span>**Fig. 14** Robustness analysis of image. (**a**) Apply 0.2 times salt and pepper noise, (**b**) Decrypted image, (**c**) Apply 0.05 times salt and pepper noise, (**d**) Decrypted image, (**e**) Crop 1/8 of the encrypted image, (**f**) Decrypted image, (**g**) Crop a quarter of the encrypted image, (**h**) Decrypted image

<span id="page-21-0"></span>

### **7.8 Comparison of diferent algorithms**

To compare the performance of diferent literature algorithms, Table [8](#page-19-0) shows the comparison of correlation coefficients of different literature algorithms. After comparison, it is discovered that the correlation coefficient of this algorithm is better than that of most literature algorithms. Table [9](#page-20-0) shows the comparison of the results of NPCR and UACI. The NPCR of this algorithm is the highest and the value of UACI is only lower than the UACI of the literature [[23](#page-22-21), [56\]](#page-24-8). The information entropy of this algorithm is the highest after comparing the infor-mation entropy of other literature in Table [10](#page-21-0). Therefore, the algorithm in this paper boasts an intense comprehensive performance compared with other algorithms in the literature.

## **8 Conclusion**

In this paper, a current hyperchaotic system of third order non-autonomous is constructed. The dynamic behavior of the system is analyzed by the spatial phase diagram, bifurcation diagram, Lyapunov exponential spectrum, Poincare cross section diagram and complexity. It is uncovered that the system has abundant dynamic behaviors and good topological structure. In addition, the system additionally accepts the extraordinary circumstances which asymmetrical double wing is converted to single wing, but it is affected by changes in system initialization and system parameters. When analyzing the infuence of nonlinear term *c*, we observe several phenomena of chaotic attractors. For instance, from chaos to chaos, or from chaos to period. And tested the  $C_0$  and *SE* complexity of the system with diferent initial values and parameters. Compared with the complexity of other systems, the complexity of this system is relatively high. Furthermore, the system circuit is designed and verifed in Multisim circuit simulation software. At the same instant, fnite time synchronization of the system is achieved by selecting the appropriate controller. Moreover, a new image encryption algorithm is designed based on the system, DNA encryption and LGS image selection. By comparing it with most of the other algorithms, this one can select and encrypt each region of the image accurately. At the last moment, the security performance of encrypted image is analyzed, and it is found that it has good encryption efect and can be widely used in the feld of image encryption in the future. In future work, we plan to apply the hyperbolic sine function to this hyperchaotic system. In the circuit design of the novel chaotic system, the circuit structure is optimized, and some circuit elements are reduced. In addition, it is expected that the system can be successfully applied to the feld of signal detection.

**Funding** Partial fnancial support was received from Science and Technology Project of Gansu Province.

**Data availability** All data generated or analysed during this study are included in this published article.

## **Declarations**

**Competing interests** The authors have no competing interests to declare that are relevant to the content of this article. All authors certify that they have no afliations with or involvement in any organization or entity with any fnancial interest or non-fnancial interest in the subject matter or materials discussed in this manuscript.

## **References**

- <span id="page-22-18"></span>1. Abusham EA (2014) Face verifcation using Local Graph Stucture (LGS)[C]// International Symposium on Biometrics & Security Technologies. IEEE
- <span id="page-22-15"></span>2. Ahmadi A, Rajagopal K, Alsaadi FE, Pham VT, Jafari S (2020) A novel 5D chaotic system with extreme multi-stability and a line of equilibrium and its engineering applications: circuit design and FPGA implementation[J]. Iranian J Sci Technol Trans Electr Eng 44:59–67
- <span id="page-22-19"></span>3. Banu SA, Amirtharajan R (2020) A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach[J]. Med Biol Eng Comput 58(7):1445–1458
- <span id="page-22-9"></span>4. Bao H, Cao J Finite-time generalized synchronization of nonidentical delayed chaotic systems. *Nonlinear Anal Model Control* 21:306–324
- <span id="page-22-1"></span>5. Bao B, Peol MA, Bao H et al (2022) No-argument memristive hyper-jerk system and its coexisting chaotic bubbles boosted by initial conditions. *Chaos, Solitons Fractals* 144(3):110744
- <span id="page-22-5"></span>6. Bhatti UA, Huang et al (2018) Recommendation system for immunization coverage and monitoring. *Human Vaccin Immunother* 14:165–171
- <span id="page-22-6"></span>7. Bhatti UA, Huang MX, Wu D et al (2019) Recommendation system using feature extraction and pattern recognition in clinical care systems. *Enterpr Inf Syst* 13:329–351
- <span id="page-22-12"></span>8. Bhatti UA, Yuan L, Yu Z et al (2020) Hybrid watermarking algorithm using Cliford algebra with Arnold scrambling and chaotic encryption. *IEEE Access* 8:76386–76398
- <span id="page-22-7"></span>9. Bhatti UA, Zeeshan Z, Nizamani MM et al (2022) Assessing the change of ambient air quality patterns in Jiangsu Province of China pre-to post-COVID-19. *Chemosphere* 288:132569
- <span id="page-22-13"></span>10. Bhatti UA, Yu Z, Chanussot J et al (2022) Local Similarity-Based Spatial–Spectral Fusion Hyperspectral Image Classifcation with Deep CNN and Gabor Filtering. *IEEE Trans Geosci Remote Sens* 60:1–15
- <span id="page-22-3"></span>11. Chen GR (1999) Yet another chaotic attractor. *J Bifurcation Chaos* 9:1465–1466
- <span id="page-22-16"></span>12. Chen SH, Liu J (2002) Tracking control and synchronization of chaotic systems based upon sampleddata feedback[J]. Chinese Physics 2002(3):11
- <span id="page-22-22"></span>13. Chen QQ, Zhang AQ, Lin HW et al (2018) Comput Digital Eng 46(11):2336–2341
- <span id="page-22-2"></span>14. Chen MS, Zhen W, Nazarimehr F, Jafari S (2021) A novel memristive chaotic system without any equilibrium point. *Integr VLSI J* 79:133–142
- <span id="page-22-11"></span>15. Cun QQ, Tong XJ, Wang Z, Zhang M (2021) Selective image encryption method based on dynamic DNA coding and new chaotic map. *Optik-Int J Light and Electron Optics* 243:167286
- <span id="page-22-10"></span>16. de la Fraga LG, Torres-Perez E, Tlelo Cuautle E, Mancillas Lopez C (2017) Hardware implementation of pseudo-random number generators based on chaotic maps. *Nonlinear Dyn* 90:1661–1670
- <span id="page-22-4"></span>17. Ding L, Cui L, Yu F et al (2021) Basin of attraction analysis of new memristor-based fractional-order chaotic system[J]. Complexity.<https://doi.org/10.1155/2021/5578339>
- <span id="page-22-20"></span>18. Enayatifar R, Abdull A, Isnin IF (2014) Chaos based image encryption using a hybrid genetic algorithm and a DNA sequence. *Opt Lasers Eng* 56:83–93
- <span id="page-22-17"></span>19. Gopakumar K, Premlet B, Gopchndrank G (2010) Inducing chaos in Wien-bridge oscillator by nonlinear composite devices[J]. Int J Electr Eng Res 22:489–496
- <span id="page-22-8"></span>20. Guan S, Lai CH, Wei G (2005) Phase synchronization between two essentially diferent chaotic systems. *Phys Rev E* 72:016205
- <span id="page-22-0"></span>21. Han XT, Mou J, Li X, Ma CG (2021) Coexistence of infnite attractors in a fractional-order chaotic system with two nonlinear functions and its DSP implementation. *Integr VLSI J* 81:43–55
- <span id="page-22-14"></span>22. Haq TU, Shah T (2021) 4D mixed chaotic system and its application to RGB image encryption using substitution-ffusion. *J Inf Secur Appl* 61:102931
- <span id="page-22-21"></span>23. Hu T, Liu Y, Gong LH et al (2017) Chaotic image cryptosystem using DNA deletion and DNA insertion[J]. *Signal Process* 134(May):234–243
- <span id="page-23-29"></span>24. Hua Z, Fan J, Xu B et al (2018) 2D logistic-sine-coupling map for image encryption[J]. Signal Process 149(148):161
- <span id="page-23-0"></span>25. Huang L, Feng R, Wang M (2004) Synchronization of chaotic systems via nonlinear control. *Phys Lett A* 320:271–275
- <span id="page-23-26"></span>26. Huang YJ, Xu Y, Li HR (2018) Image encryption algorithm based on DNA encoding and hyperchaotic system. J Inner Mongolia Univ Sci Technol 37(3):246–254
- <span id="page-23-18"></span>27. Huang LL, Yao WJ, Xiang JH et al (2022) Study on super-multistability of a four-dimensional chaotic system with multisymmetric homogeneity attractor[J]. J Electron Inf Technol 44(1):10
- <span id="page-23-3"></span>28. Jafari MA, Mliki E, Akgul A (2017) Chameleon: the most hidden chaotic fow. *Nonlinear Dyn* 88:2303–2317
- <span id="page-23-4"></span>29. Jafari S, Ahmadi A, Khalaf AJM (2018) A new hidden chaotic attractor with extreme multi-stability. *AEU-Int J Electron Commun* 89:131–135
- <span id="page-23-28"></span>30. Kang XB, Lin GF, Chen YJ et al (2020) Robust and secure zero-watermarking algorithm for color images based on majority voting pattern and hyper-chaotic encryption[J]. Multimed Tools Appl 79(11)
- <span id="page-23-17"></span>31. Kaur G, Agarwal R, Patidar V (2021) Color image encryption system using combination of robust chaos and chaotic order fractional Hartley transformation. *J King Saud Univ-Comput Inf Sci* 3:007
- <span id="page-23-19"></span>32. Khalaf AJM, Abdolmohammadi HR, Ahmadi A, Moysis L, Volos C, Hussain I (2020) Extreme multistability analysis of a novel 5D chaotic system with hidden attractors, line equilibrium, permutation entropy and its secure communication scheme[J]. Eur Phys J Spec Top 229:1175–1188
- <span id="page-23-23"></span>33. Li L, Kong LY (2018) A new image encryption algorithm based on Chaos. *J Syst Simul* 30:54–96
- <span id="page-23-11"></span>34. Li HL, Wang Z, Jiang YL (2017) Anti-synchronization and intermittent anti-synchronization of two identical delay hyperchaotic Chua systems via linear control. *Asian J Control* 19:202–214
- <span id="page-23-16"></span>35. Li CQ, Lin DD, Lü JH (2017) Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE Multimed* 24:64–71
- <span id="page-23-1"></span>36. Li C, Zhang Y, Xie EY (2019) When an attacker meets a cipher-image in 2018: A year in review. *J Inform Secur Appl* 48:102361
- <span id="page-23-9"></span>37. Liu L, Liu Q (2019) Cluster synchronization in a complex dynamical network of non-identical nodes with delayed and non-delayed coupling via pinning control. *Phys Scr* 94:045204
- <span id="page-23-24"></span>38. Liu H, Zhao B, Huang L (2019) A remote-sensing image encryption scheme using DNA bases probability and twodimensional logistic map[J]. *IEEE Access* 7:65450–65459
- <span id="page-23-7"></span>39. Lu JH, Chen GR (2002) A new chaotic attractor coined. *Int J Bifurcation Chaos* 12:659–661
- <span id="page-23-20"></span>40. Ma MZ, Liu Y, Li ZJ (2021) Study on Memristor Switched chaotic Circuit and its Attractor Coexistence[J]. *J Electron Inf Technol* 43(12):8
- <span id="page-23-25"></span>41. Min FH, Wang ZL, Wang ER (2016) New memristor chaotic circuit and its application to image encryption. *J Electron Inf Technol* 38:2681–2688
- <span id="page-23-2"></span>42. Pak C, Huang L (2017) A new color image encryption using combination of the 1D chaotic map. *Signal Process* 138:129–137
- <span id="page-23-22"></span>43. Qu SH, Yang ZH, Rong XW (2019) A New Memristor Chaotic System and Its Application in Image Encryption. *J Syst Simul* 31:984–991
- <span id="page-23-5"></span>44. Rajagopal K, Akgul A, Jafari S, Aricioglu B (2018) A chaotic memcapacitor oscillator with two unstable equilibriums and its fractional form with engineering applications. *Nonlinear Dyn* 91:957–974
- <span id="page-23-13"></span>45. Shi L, Yang X, Li Y, Feng Z (2016) Finite-time synchronization of nonidentical chaotic systems with multiple time-varying delays and bounded perturbations. *Nonlinear Dyn* 83:75–87
- <span id="page-23-21"></span>46. Solev D, Janjic P, Kocarev L (2011) Introduction to Chaos. In: Kocarev L, Lian S (eds) Chaos-Based Cryptography. Studies in Computational Intelligence, vol 354. Springer, Berlin, Heidelberg. [https://](https://doi.org/10.1007/978-3-642-20542-2_1) [doi.org/10.1007/978-3-642-20542-2\\_1](https://doi.org/10.1007/978-3-642-20542-2_1)
- <span id="page-23-8"></span>47. Sprott JC (1994) Some simple chaotic fows. *Phys Rev E* 50:R647–R650
- <span id="page-23-12"></span>48. Sun J, Wang Y, Wang Y, Shen Y (2016) Finite-time synchronization between two complex-variable chaotic systems with unknown parameters via nonsingular terminal sliding mode control. *Nonlinear Dyn* 85:1105–1117
- <span id="page-23-27"></span>49. Tian JL, Deng LG (2021) Image encryption method based on ffth order CNH Hyperchaotic system. *J Xihua Univ (Nat Sci Ed)* 40:63–70
- <span id="page-23-15"></span>50. Trejo Guerra R, Tlelo Cuautle E, Cruz Hernández C, Sanchĕz Lopĕz C (2009) Chaotic communication system using Chua's oscillators realized with CCII+ s. *Int J Bifurc Chaos* 19:4217–4226
- <span id="page-23-10"></span>51. Wang XF, Chen G (2002) Synchronization in scale-free dynamical networks: robustness and fragility. *IEEE Trans Circuits Syst I* 49:54–62
- <span id="page-23-14"></span>52. Wang L, Zeng Z, Hu J, Wang X (2017) Controller design for global fxed-time synchronization of delayed neural networks with discontinuous activations. *Neural Netw* 87:122–131
- <span id="page-23-6"></span>53. Wang N, Zhang G, Bao H (2019) Bursting oscillations and coexisting attractors in a simple memristorcapacitor-based chaotic circuit. Nonlinear Dyn 97:1477–1494
- 54. Wang N, Zhang G, Ren L (2020) Coexisting asymmetric behavior and free control in a simple 3-d chaotic system. *AEU-Int J Electron Commun* 122:153234
- <span id="page-24-0"></span>55. Wang N, Zhang G, Bao H (2020) Infnitely many coexisting conservative fows in a 4D conservative system inspired by LC circuit. *Nonlinear Dyn* 99:3197–3216
- <span id="page-24-8"></span>56. Wu X, Kan H, Ju et al (2015) A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps[J]. *Appl Soft Comput* 37:24–39
- <span id="page-24-5"></span>57. Yan SH, Shi WL, Wang QY et al (2022) Research and synchronization application of a new 3D switched chaotic system[J]. Complex Syst Complex Sci:1–13
- <span id="page-24-6"></span>58. Yan SH, Wang ET, Sun X et al A chaotic system with co-existence of attractors and its synchronization circuit realization [J]. J Shenzhen Univ Sci Technol Ed
- <span id="page-24-1"></span>59. Yang Y, Land HL, Xiang JZ (2021) Design of multi-wing 3D chaotic systems with only stable equilibria or no equilibrium point using rotation symmetry. *Int J Electron Commun* 135:153710
- <span id="page-24-3"></span>60. Yu J, Hu C, Jiang H, Fan X (2014) Projective synchronization for fractional neural networks. *Neural Netw* 49:87–95
- <span id="page-24-7"></span>61. Zhan K, Jiang WG (2017) Novel four-wing hyper-chaos system and its application in image encryption. *Comput Eng Applications* 53:36–44
- <span id="page-24-2"></span>62. Zhang J, Xu LH (2022) An active magnetron memristor hyperchaotic circuit and image encryption. Comput Eng Sci 44(8):1392–1401
- <span id="page-24-4"></span>63. Zhang G, Liu Z, Ma Z (2007) Generalized synchronization of diferent dimensional chaotic dynamical systems. *Chaos, Solitons Fractals* 32:773–779

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.