AIMS Mathematics, 9(3): 5582–5608.
DOI: 10.3934/math.2024270
Received: 09 October 2023
Revised: 20 January 2024
Accepted: 24 January 2024
Published: 30 January 2024

http://www.aimspress.com/journal/Math

Research article

A new image encryption based on hybrid heterogeneous time-delay chaotic systems

Yuzhen Zhou[1] **and Erxi Zhu**[1,2,*]

[1] College of Internet of Things Engineering, Jiangsu Vocational College of Information Technology, No.1 Qianou Road, Huishan District, Jiangsu Wuxi, 214153, China

[2] College of Computer Science and Technology, Nanjing University of Aeronautics & Astronautics, No.29 Jiangjun Avenue, Jiangning District, Nanjing, 211106, China

* **Correspondence:** Email: erxi666@163.com.

Abstract: Chaos theory has been widely utilized in password design, resulting in an encryption algorithm that exhibits strong security and high efficiency. However, rapid advancements in cryptanalysis technology have rendered single system generated sequences susceptible to tracking and simulation, compromising encryption algorithm security. To address this issue, we propose an image encryption algorithm based on hybrid heterogeneous time-delay chaotic systems. Our algorithm utilizes a collection of sequences generated by multiple heterogeneous time-delay chaotic systems, rather than sequences from a single chaotic system. Specifically, three sequences are randomly assigned to image pixel scrambling and diffusion operations. Furthermore, the time-delay chaotic system comprises multiple hyperchaotic systems with positive Lyapunov exponents, exhibiting a more complex dynamic behavior than non-delay chaotic systems. Our encryption algorithm is developed by a plurality of time-delay chaotic systems, thereby increasing the key space, enhancing security, and making the encrypted image more difficult to crack. Simulation experiment results verify that our algorithm exhibits superior encryption efficiency and security compared to other encryption algorithms.

Keywords: image encryption; chaotic encryption; heterogeneous time-delay chaotic system; hopf bifurcation; stability
Mathematics Subject Classification: 26E70

1. Introduction

After the relationship between chaos theory [1,2] and cryptography was found. the theory [3,4] has aroused the attention of cryptographers. They have suggested that the properties of quasi-randomness and initial value sensitivity of chaotic systems [5, 6] can satisfy the requirements of encryption

algorithms [7–9]. Subsequently, they have developed a considerable number of excellent encryption algorithms. In encryption algorithms, the pseudo-random sequence generated by the chaotic system is essentially adopted to perform scrambling and diffusion operations on image pixels. This type of algorithm shows the advantages of simple implementation and strong attack resistance, and they fall into three categories, including image encryption algorithms with low-dimensional chaotic systems, image encryption algorithms with high-dimensional chaotic systems, and image encryption algorithms combined with chaotic systems and other methods.

In the algorithm of image encryption with low-dimensional chaotic systems, Guo et al. [10] first proposed the concept of the "chaos password", which draws upon the sequence generated by the Logistic mapping to implement image encryption. The algorithm's security is entirely determined by the generated pseudo-random sequence. Subsequently, a symmetric product cipher was developed using the two-dimensional (2D) Baker map, whereas the operational efficiency of the encryption algorithm cannot be ensured [11]. On the basis of Kolmogoroff flows and shift registers, a block-oriented symmetric cryptosystem was employed to increase image encryption efficiency [12].

The sequence of high-dimensional chaotic systems is recognized to be more irregular and unpredictable as compared with that of low-dimensional chaotic systems. The key space of the algorithm is significantly larger than the key space of the algorithm constructed with low-dimensional chaotic systems [13–15]. Accordingly, they are more suitable for image encryption. For instance, the Cat mapping's sequence is employed to perform the scrambling operation; next, the Logistic mapping is adopted for the diffusion operation [16]. The image pixel is scrambled twice by the Henon map and the Lorenz map to increase the efficiency of image encryption [17]. However, the diffusion operation is not implemented on the image pixels, and the algorithm's security cannot be ensured. Based on the problems exposed in [17], the image pixel scrambling operation is performed using the Logistic map, and then the diffusion operation is implemented using the Henon map sequence, so as to improve the algorithm's security [18]. Furthermore, a secure symmetric encryption is developed using the sequence of 3D Cat maps to perform image pixel scrambling operations multiple times [19]. Park proposed a conservative chaotic system [20] with a simple structure, large LEs, continuous chaotic ranges, and high complexity, which is utilized to generate a novel image encryption algorithm exhibiting superior encryption performance. The above algorithms all exhibit a sufficiently large key space to be resistant to brute force attacks.

In the image encryption algorithm combining chaotic systems and other methods, the image pixel scrambling operation is performed using the DNA sequence, and the scrambling operation and the diffusion operation are carried out again using the 2D Logistic chaotic map [24]. The algorithm exhibits strong key sensitivity, while being easy to implement, and even capable of resisting statistical attacks. Furthermore, the plaintext image is first encoded into a DNA sequence, and then the sequence generated by chaos is employed to perform permutation and replacement operations on the encoded image pixels [25].

Since the theory of chaotic cryptography is not well established, the above schemes only demonstrate their security experimentally and cannot provide strict mathematical proofs. Thus, the research of chaotic cryptography is still a challenging frontier subject, which is worth investigating in depth. Existing chaotic encryption algorithms suggest that the security of low-dimensional or hyper-chaotic systems as chaotic passwords cannot be ensured; an attacker can always find a cracking method to predict the sequence came from a chaotic system, as an attempt to decipher the intercepted

ciphertext. For instance, the improved CKBA algorithm of image encryption [21] was cracked by Li et al. [22] through selected plaintext and known plaintext attacks. Using the same method, they successfully deciphered the hyperchaotic system-based image encryption algorithm [23]. The chaotic system with time-delay is characterized by its infinite dimension, stronger randomness, more complex dynamic behavior, and being more difficult to predict. Accordingly, the time-delay chaotic system becomes the choice of the next generation of chaotic ciphers. Moreover, the above encryption algorithms always use the sequence generated by a single chaotic system to realize scrambling operations and diffusion operations. This measure can be easily tracked using cryptanalysis techniques, thus causing the lost security of the encryption algorithm and the exposure of the encrypted information. In this paper, the focus is placed on an algorithm of image encryption based on a hybrid heterogeneous chaotic system with time-delay. The main feature of this algorithm refers to using the sequences generated by multiple heterogeneous time-delay chaotic systems to form a sequence set. Three sequences in the set are randomly assigned into image pixel scrambling and diffusion operations during image encryption. This encryption scheme can avoid brute force attacks because it cannot simulate the encryption sequence, and the key space of the encryption algorithm is increased, which improves the security of the algorithm. In addition, the encryption efficiency is improved by adopting non-iterative encryption.

The paper is organized as follows. In this first section, the research status of image encryption technology is briefed. In the second section, the stability and Hopf bifurcation of single-delay chaotic systems are studied. In the third section, image encryption is performed using the heterogeneous single-delay chaotic system. In the fourth section, the algorithm's encryption effect is verified. Lastly, the conclusions of this paper are drawn.

2. The chaotic system with time-delay

Since chaotic systems with time-delay is characterized by an infinite-dimensional state space and a highly complex dynamic behavior, they are used for serving as a chaotic password [26–29]. Besides the initial value conditions and parameters of the chaotic system, the chaotic cipher's key space of should also cover the time-delay and the position of the time-delay. Time-delay chaotic systems at different locations exhibit different dynamic behaviors. A chaotic system with time-delays at different positions is termed a heterogeneous time-delay chaotic system. For the state transition of a time-delay chaotic system, the bifurcation criticality of the system should be explored, in which Hopf bifurcation [30, 31] has been most commonly investigated.

Over the past few years, there have been rare studies of the Hopf bifurcation of chaotic systems with time-delay. In general, the linearization of the time-delay chaotic system at the singular point is the transcendental equation. Subsequently, the roots' distribution of the transcendental equation determines the Hopf bifurcation condition of the chaotic system with time-delay, which was analyzed by Hale [32]. The above result lays a theoretical basis for the Hopf bifurcation study of time-delay chaotic systems. Wei Junjie et al. [33] proposed the exponential polynomial zero-point distribution theorem based on Rouche's theorem, which has deepened the study of Hopf bifurcation theory. Faria and Magalhães [34–36] generalized and applied canonical theory to time-delay differential equations. They proposed a canonical calculation method which significantly contributed to the development of the bifurcation theory. Thus far, the bifurcation study of time-delay chaotic systems has been initiated

and gradually deepened. Gamal et al. [37] presented a generalized form of the time-delay Lorenz system. This Lorenz system had $2n+1$dimensions. Furthermore, they investigated the stability of trivial and non-trivial fixed points and the existence Hopf bifurcation conditions. Kun et al. [38] adopted the improved undetermined coefficient method to validate the homoclinic orbit of the Chen system with time delay feedback and proposed the helical involute projection method. Lian et al. [39] conducted the Hopf bifurcation study of Lorenz-like systems with time-delay. Additionally, Li et al. [40] conducted a Hopf bifurcation study of interfering Lorenz-like systems with time-delay. The research and analysis of the mentioned literature confirm that different time delay positions significantly affect the dynamic behavior of the system. In a 3D general Lorenz system, multiple heterogeneous single delay chaotic systems can be formed using time delays at different positions and can be generated by the sequence that the image encryption algorithm is dependent on.

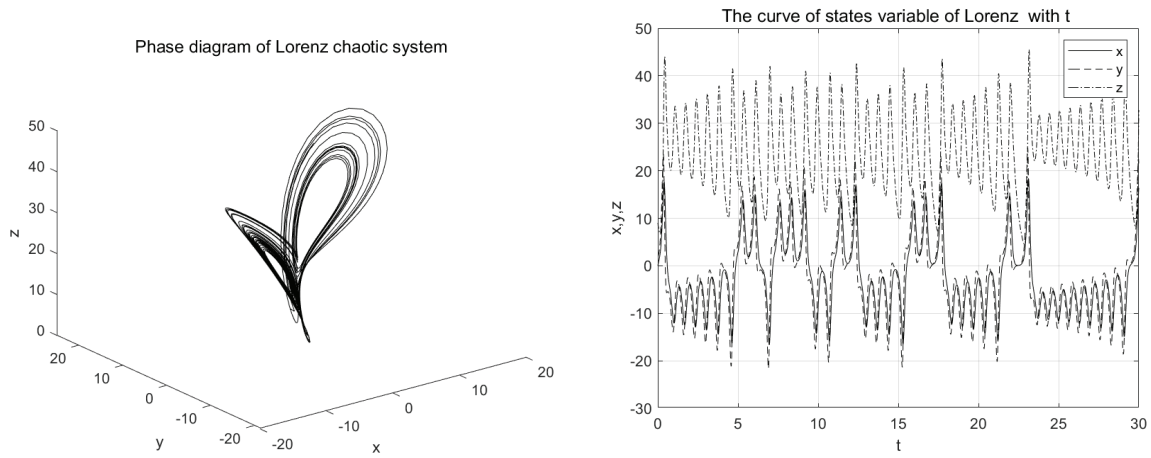
The unified system was proposed by Lü et al. in 2002. The system links the Lorenz system, Lü system and Chen system. Its system model is expressed as

$$\begin{cases} \dot{x} = (25\alpha + 10)(y - x) \\ \dot{y} = (28 - 35\alpha)x - xz + (29\alpha - 1)y \\ \dot{z} = xy - (8 + \alpha)z/3 \end{cases} \tag{2.1}$$

where x, y, z denote state variables and $\alpha \in [0, 1]$ represents the system parameter. When $\alpha \in [0, 0.8)$, the system pertains to the Lorenz system; when $\alpha \in (0.8, 1]$, the system belongs to the Chen system; and when $\alpha = 0.8$, the system belongs to the Lü system. The unified chaotic system model expresses the basic structure of the Lorenz model well through a single parameter. However, its system parameters are too singular, limiting the parameter range. Subsequently, researchers formed numerous deformations of Lorenz systems based on continuous updating (e.g., Lorenz-like systems [41]), and presented corresponding bifurcation laws and stability conditions [42]. Without loss of generality, this paper elucidates a general Lorenz system and the bifurcation law of its heterogeneous single-delay chaotic system. The system's equation is expressed as:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = bx + dy - xz \\ \dot{z} = -cz + xy \end{cases} \tag{2.2}$$

where a, b, c, d denote system parameters. Equation (2.2) contains seven terms, of which there are only two nonlinear terms, compared with other chaotic or hyperchaotic systems. Since the structure of the system is simpler, the circuit implementation can be achieved more easily. Thus, the system has a promising application in secure communication and other fields. Figure 1 illustrates the phase diagram and state vector trend of a general Lorenz system over time when $a = 10$, $b = 28$, $c = 8/3$, and $d = -1$.



(a) plots the change curve of the state variable x, y, z over time t (b) presents the phase diagram of the system in space $O-xyz$

Figure 1. Change trend of the general Lorenz system.

Figure 1 suggests that the general Lorenz system has two chaotic attractors with two wings and the state variable keeps periodic oscillation permanently with time. It is therefore implied that the system has entered a chaotic state.

Numerous researchers have obtained the time-delayed Lorenz chaotic system by imposing time-delay on the state variables. However, different positions of time delays can be introduced to form functional differential dynamical systems with different dynamical behaviors. In Eq (2.2), applying a single time delay to the state variables, nine forms of heterogeneous single time-delay chaotic systems can be established.

$$\begin{cases} \dot{x} = a(y(A) - x(B)) \\ \dot{y} = bx(C) + dy(D) - x(E)z(F) \\ \dot{z} = -cz(G) + x(H)y(I) \end{cases}$$

where $A - Z$ represents the imposition of a time delay of the form $t - \tau$ and $\tau(> 0)$ denotes time lag. The nine heterogeneous time-delay chaotic systems consist of three identical equilibrium points:

$$(0,0,0),\ (\sqrt{(b+d)c},\ \sqrt{(b+d)c}, b+d),\ (-\sqrt{(b+d)c}, -\sqrt{(b+d)c}, b+d).$$

When the parameters $a > 0$, $b + d < 0$, $c > 0$, the system contains a unique equilibrium point $O(0, 0, 0)$, and the time-delay general Lorenz system shows a better parameter range than other systems. Next, the stability of $O(0, 0, 0)$ of a single delay Lorenz system with a delay at position A (System A for short) is considered.

The linearization equation of system A at the point $O(0, 0, 0)$ is expressed as

$$\begin{cases} \dot{x} = a[y(t - \tau) - x] \\ \dot{y} = bx + dy \\ \dot{z} = -cz \end{cases} \tag{2.3}$$

where the value range of a, b, c, and d is $a > 0$, $b + d < 0$, $c > 0$, $a + c > d$, $|d| > |b|$. The characteristic equation of Eq (2.3) is expressed as

$$\begin{vmatrix} -a-\lambda & ae^{-\lambda\tau} & 0 \\ b & e-\lambda & 0 \\ 0 & 0 & -c-\lambda \end{vmatrix} = 0. \tag{2.4}$$

Equation (2.4) can be reduced to

$$\lambda^3 + (a + c - d)\lambda^2 + (ca - cd - ad)\lambda - acd - ab(\lambda + c)e^{-\lambda\tau} = 0. \tag{2.5}$$

Where $p_1 = a + c - d$; $p_2 = ca - cd - ad$; $p_3 = -acd$; $p_4 = -ab$; $p_5 = -abc$. Thus, the following lemma can be expressed as follows.

Lemma 1. *If $\tau = 0$, $a > 0$, $b + d < 0$, $c > 0$, $a + c > d$ and $|d| > |b|$, the zero equilibrium point of system A is locally asymptotically stable.*

Proof. When $\tau = 0$, the characteristic Eq (2.5) is transformed into

$$\lambda^3 + p_1\lambda^2 + (p_2 + p_4)\lambda + p_3 + p_5 = 0. \tag{2.6}$$

Since $a > 0$, $b + d < 0$, $c > 0$, $a + c > d$, and $|d| > |b|$, it is easy to obtain that $p_1 > 0$, $p_2 + p_4 > 0$, and $p_3 + p_5 > 0$. According to the Routh-Hurwitz theorem, all roots of Eq (2.6) are common in having negative real parts. Thus, the point $O(0, 0, 0)$ of system A is asymptotically stable when $\tau = 0$. □

When $\tau > 0$, suppose $\lambda = i\omega$ (ω is an undetermined constant greater than zero) is a pure imaginary root of Eq (2.5) so that the imaginary part ω satisfies

$$-i\omega^3 - p_1\omega^2 + ip_2\omega + p_3 + (ip_4\omega + p_5)(\cos\omega\tau - i\sin\omega\tau) = 0. \tag{2.7}$$

According to the equality of plural numbers, it can be obtained that

$$\begin{cases} p_5\cos\omega\tau + p_4\omega\sin\omega\tau = p_1\omega^2 - p_3 \\ p_4\omega\cos\omega\tau - p_5\sin\omega\tau = \omega^3 - p_2\omega. \end{cases} \tag{2.8}$$

Equation (2.8) can be equivalently transformed into

$$\omega^6 + (p_1^2 - 2p_2)\omega^4 + (p_2^2 - 2p_1p_3 - p_4^2)\omega^2 + p_3^2 - p_5^2 = 0. \tag{2.9}$$

A conclusion for Eq (2.9) can be reached as follows.

Lemma 2. *If $a > 0$, $b + d < 0$, $c > 0$, $a + c > d$ and $|d| > |b|$, Eq (9) has at least one positive real root.*

Proof. Set $u = \omega^2$. Then, Eq (2.9) can be reduced to

$$u^3 + (p_1^2 - 2p_2)u^2 + (p_2^2 - 2p_1p_3 - p_4^2)u + p_3^2 - p_5^2 = 0. \tag{2.10}$$

Suppose

$$f(u) = u^3 + (p_1^2 - 2p_2)u^2 + (p_3^2 - 2p_1p_3 - p_4^2)u + p_3^2 - p_5^2. \tag{2.11}$$

Equation (2.11) can be converted into

$$f(u) = \frac{1 + (p_1^2 - 2p_2)\frac{1}{u} + (p_3^2 - 2p_1p_3 - p_4^2)\frac{1}{u^2} + (p_3^2 - p_5^2)\frac{1}{u^3}}{\frac{1}{u^3}}. \tag{2.12}$$

It can be derived from Eqs (2.11) and (2.12) that

$$f(0) = p_3^2 - p_5^2 < 0, \lim_{u \to +\infty} f(u) = +\infty.$$

According to the zeros value theorem, there is at least one real number $u_0 \in (0, +\infty)$ that makes $f(u_0) = 0$. Thus, Eq (2.10) has one positive real root at minimum. Since $u = \omega^2$, Eq (2.9) has at least one positive real root. □

Suppose ω_0 is a real root of Eq (2.9). Then, Eq (2.5) has a pure imaginary root $i\omega_0$. It can be obtained from Eq (2.8) that

$$\cos \omega\tau = \frac{p_4\omega^4 - (p_1p_5 + p_2p_4)\omega^2 + p_3p_5}{p_4^2\omega^2 + p_5^2}. \tag{2.13}$$

By substituting $\omega = \omega_0$ into Eq (2.13), the time-delay τ can be calculated as:

$$\tau_k = \frac{1}{\omega_0} \arccos\left(\frac{p_4\omega_0^4 - (p_2p_4 - p_1p_5)\omega_0^2 - p_3p_5}{p_4^2\omega_0^2 + p_5^2}\right) + \frac{2k\pi}{\omega_0}, k = 0, 1, 2, \cdots \tag{2.14}$$

Thus, (ω_0, τ_k) is the solution of Eq (2.5), suggesting that $\lambda = \pm i\omega_0$ is a pair of conjugate pure imaginary roots of Eq (2.5) when $\tau = \tau_k$.

Suppose $\tau_0 = \min\{\tau_k\}$. Then, time delay $\tau = \tau_0$ is the minimum value when the pure imaginary root $\lambda = \pm i\omega_0$ of Eq (2.5) appears. Thus, we have the following lemma.

Lemma 3. *If $a > 0$, $b + d < 0$, $c > 0$, $a + c > d$, $|d| > |b|$, and $\tau = \tau_0$, then, Eq (2.5) has a pair of pure imaginary roots $\lambda = \pm i\omega_0$.*

Suppose $\lambda(\tau) = \alpha(\tau) + i\omega(\tau)$ satisfies $\alpha(\tau_k) = 0$ and $\omega(\tau_k) = \omega_0$. The following presents the transversal conditions.

Lemma 4. *If $a > 0$, $b + d < 0$, $c > 0$, $a + c > d$, $|d| > |b|$ and $f'(\omega_0^2) > 0$, then $\frac{d\mathrm{Re}\lambda(\tau)}{d\tau}\Big|_{\tau=\tau_k} > 0$.*

Proof. The derivation regarding τ of both sides of Eq (2.5) is performed to obtain

$$[3\lambda^2 + 2p_1\lambda + p_2 + p_4e^{-\lambda\tau} - \tau(p_4\lambda + p_5)e^{-\lambda\tau}]\frac{d\lambda}{d\tau} = \lambda(p_4\lambda + p_5)e^{-\lambda\tau}. \tag{2.15}$$

It can be calculated according to Eq (2.5) that

$$(p_4\lambda + p_5)e^{-\lambda\tau} = \lambda(\lambda^2 + p_1\lambda + p_2). \tag{2.16}$$

Substituting Eq (2.16) into Eq (2.15) yields

$$\left(\frac{d\lambda}{d\tau}\right)^{-1} = -\frac{3\lambda^2 + 2p_1\lambda + p_2}{\lambda^2(\lambda^2 + p_1\lambda + p_2)} + \frac{p_4}{\lambda(p_4\lambda + p_5)} - \frac{\tau}{\lambda} \tag{2.17}$$

$\tau_k = i\omega_0$ and therefore

$$\begin{aligned}\mathrm{Re}[(\tfrac{d\lambda}{d\tau})^{-1}\big|_{\tau=\tau_k}] &= -\mathrm{Re}[\tfrac{3\lambda^2+2p_1\lambda+p_2}{\lambda^2(\lambda^2+p_1\lambda+p_2)}\big|_{\tau=\tau_k}] + \mathrm{Re}[\tfrac{p_4}{\lambda(p_4\lambda+p_5)}\big|_{\tau=\tau_k}] \\ &= \mathrm{Re}[\tfrac{-3\omega_0^2+2ip_1\omega_0+p_2}{\omega_0^2(\omega_0^2-ip_1\omega_0-p_2)}] + \mathrm{Re}(\tfrac{p_4}{p_4\omega_0^2-ip_5\omega_0)}) \\ &= \tfrac{(p_2-3\omega_0^2)(\omega_0^2-p_2)-2p_1^2\omega_0^2}{\omega_0^2[(p_2-\omega_0^2)^2+p_1^2\omega_0^2]} - \tfrac{p_4^2}{p_4^2\omega_0^2+p_5^2}.\end{aligned} \tag{2.18}$$

When $\tau = \tau_k$, Eq (2.5) has pure imaginary roots $i\omega_0$, which are substituted into Eq (2.5) to obtain

$$-i\omega_0^3 - p_1\omega_0^2 + ip_2\omega_0 + p_2 - (ip_4\omega_0 + p_5)e^{-i\omega_0\tau} = 0 \tag{2.19}$$

$\left|e^{-i\omega_0\tau}\right| = 1$, because $e^{-i\omega_0\tau} = \cos\omega_0\tau - i\sin\omega_0\tau$. Thus, it can be calculated using Eq (2.19) that

$$\left|-p_1\omega_0^2 + p_3 + i(p_2\omega_0 - \omega_0^3)\right| = \left|-p_5 - ip_4\omega_0)\right|.$$

Namely,

$$\omega_0^2(p_2 - \omega_0^2)^2 + (p_1\omega_0^2 - p_3)^2 = (p_4\omega_0)^2 + p_5^2. \tag{2.20}$$

As obtained by combining Eqs (2.18) and (2.20),

$$\mathrm{Re}[(\frac{d\lambda}{d\tau})^{-1}\big|_{\tau=\tau_k}] = \frac{3\omega_0^4 + 2(p_1^2 - 2p_2)\omega_0^2 + (p_2^2 - 2p_1p_3 - p_4^2)}{p_4^2\omega_0^2 + p_5^2} = \frac{f'(\omega_0^2)}{p_4^2\omega_0^2 + p_5^2} > 0.$$

$Sign[\mathrm{Re}(\frac{d\lambda}{d\tau}\big|_{\tau=\tau_k})] = Sign\{\mathrm{Re}[(\frac{d\lambda}{d\tau})^{-1}\big|_{\tau=\tau_k}]\}$. Thus, the lemma is proved. □

According to Lemma 4 and Hopf bifurcation theory, we draw the following conclusions.

Theorem 1. *If $a > 0$, $b + d < 0$, $c > 0$, $a + c > d$, $|d| > |b|$, and $f'(\omega_0^2) > 0$, then,*

(1) when $\tau \in [0, \tau_0)$, system A is asymptotically stable at the point $O(0, 0, 0)$

(2) when $\tau > \tau_0$, system A is unstable at the point $O(0, 0, 0)$

(3) $\tau = \tau_k (k = 0, 1, 2, \cdots)$ is the Hopf bifurcation value of system A, suggesting that Hopf bifurcation occurs at the point $O(0, 0, 0)$ in system A.

Considering that the parameters of system A are $b + d < 0$, $c > 0$ and $a + c > d$, system A is simulated with $a = 10$, $c = 2.5$ and $d = 2$. In this case, system A can be converted into

$$\begin{cases} \dot{x} = 10y(t - \tau) - 10x \\ \dot{y} = -4x + 2y - xz \\ \dot{z} = -2.5z + xy. \end{cases} \tag{2.21}$$

It can be calculated using mathematical software that the positive real root of Eq (2.9) is $\omega_0 = 3.2376$, $f'(\omega_0^2) = 2.0909 \times 10^3 > 0$, and $\tau_0 = 0.2173$ in Eq (2.14). Thus, Corollary 1 can be simplified into the following corollaries.

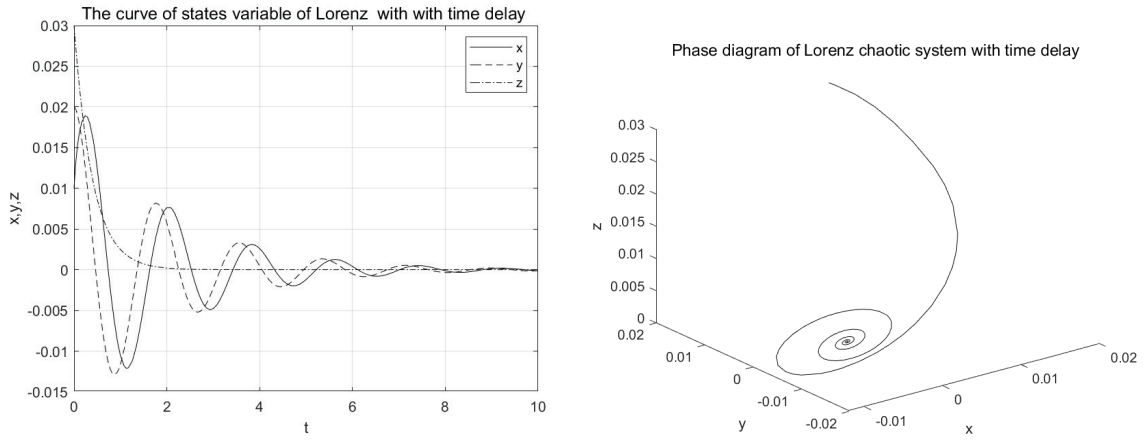
Corollary 1. *If $a > 0$, $b + d < 0$, $c > 0$, $a + c > d$ and $f'(\omega_0^2) > 0$, then,*

(1) When $\tau \in [0, 0.2173)$, system (2.21) is asymptotically stable at the point $O(0, 0, 0)$.

(2) When $\tau > 0.2173$, system (2.21) is unstable at the point $O(0, 0, 0)$.

(3) $\tau = 0.2173 + 0.6177k\pi(k = 0, 1, 2, 3, \cdots)$ *is the Hopf bifurcation value of system (2.21), suggesting that a Hopf bifurcation occurs in system (2.21) at the point* $O(0, 0, 0)$*, leading to limit cycles.*

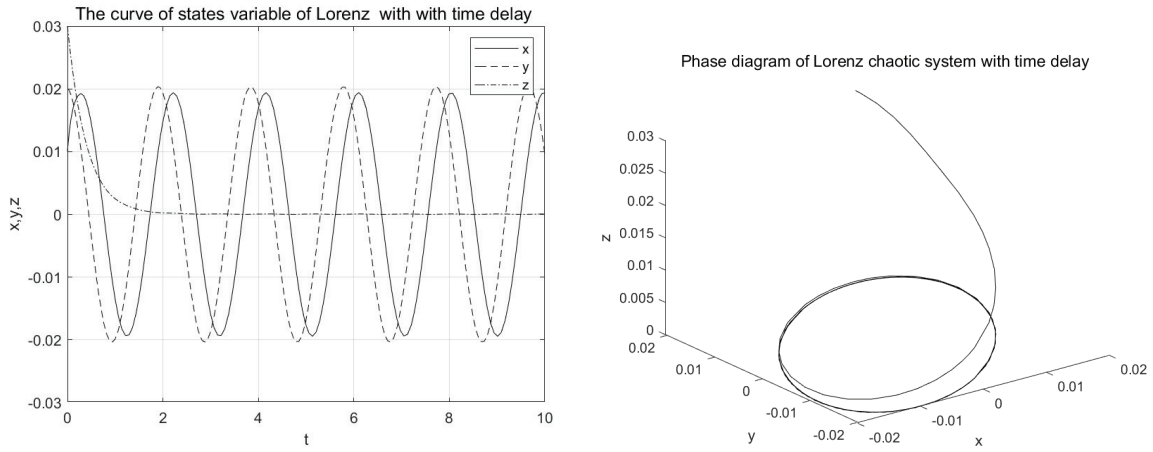
Mathematical software is applied to draw the state variables' trajectory diagram and phase diagram when the time-delay takes different values, as illustrated in Figures 2–4. The results obtained is verified.



(a) plots the change curve of the state variable, system x, y, z over time t (b) presents the phase diagram of the system in space $O-xyz$

Figure 2. The trend of changes in system (2.21) when $\tau = 0.17$, $x(t) = 0.01$, $y(t) = 0.02$, and $z(t) = 0.03(t \in [-0.17, 0])$.

As shown in Figure 2, the value of the state variable of system (2.21) approaches the equilibrium point $O(0, 0, 0)$ over time and as a result of which the equilibrium point $O(0, 0, 0)$ of system (2.21) is asymptotically stable.

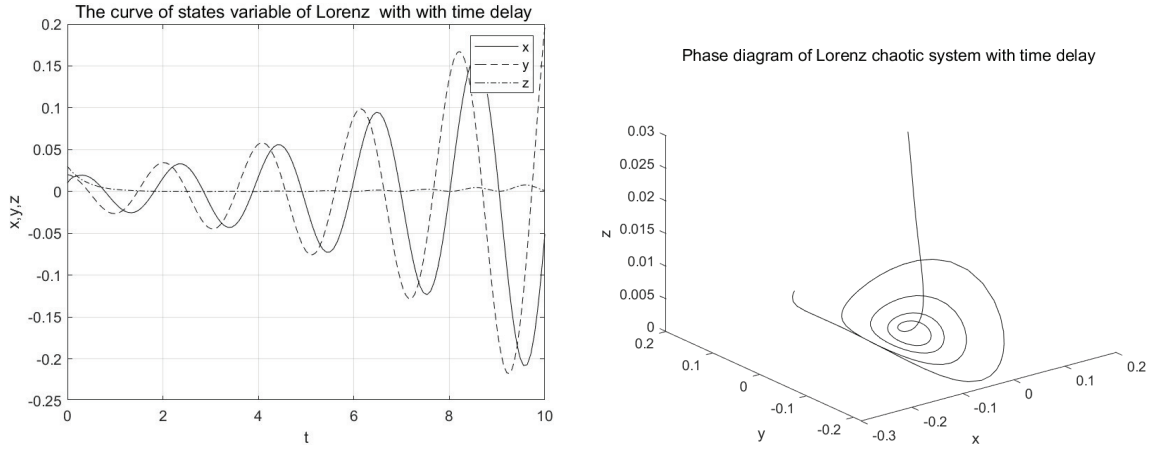


(a) plots the change curve of the state variables, system x, y, z over time t (b) presents the phase diagram of the system in space $O-xyz$

Figure 3. The trend of changes in system (2.21) when , $x(t) = 0.01$, and $z(t) = 0.03(t \in [-0.2173, 0])$.

It can be observed in Figure 3 that when $\tau = 0.2173$, the variable x, y, z keeps periodic oscillation,

and a limit cycles appear in the $O - xyz$ space, suggesting that a Hopf bifurcation occurs at the point $O(0, 0, 0)$.

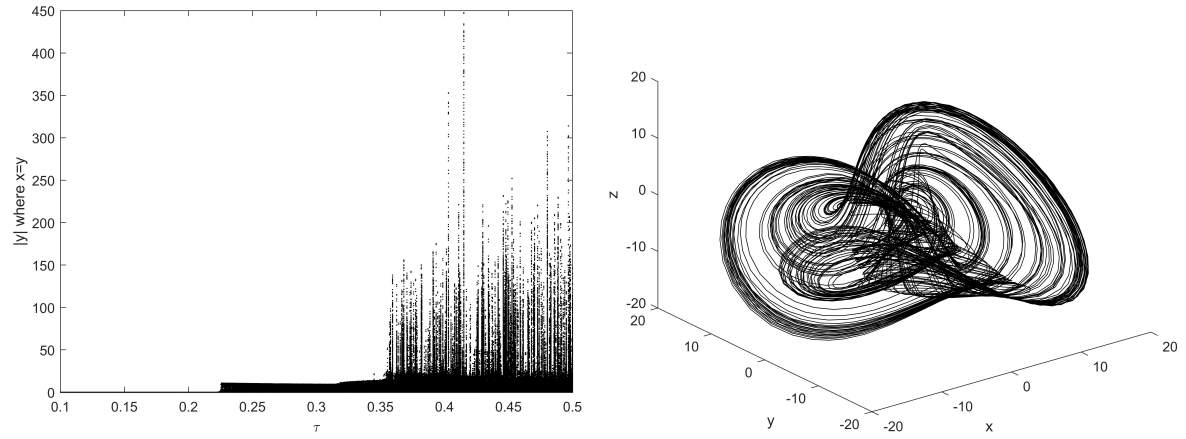


(a) plots the change curve of the state variables, system x, y, z over time t (b) presents the phase diagram of the system in space $O-xyz$

Figure 4. The trend of changes in system (2.21) when $\tau = 0.25$, $x(t) = 0.01$, $y(t) = 0.02$ and $z(t) = 0.03(t \in [-0.25, 0])$.

As shown from Figure 4, the value of the state variables x, y, z of system (2.21) shifts away from the equilibrium point progressively with time t, suggesting that the point $O(0, 0, 0)$ is unstable when $\tau = 0.25$.

The system's chaos is further verified in the following and the bifurcation diagram of system (2.21) over τ and the phase diagram of system (2.21) when $\tau = 0.3$ are respectively drawn, as shown in Figure 5. Figure 5(a) shows the bifurcation diagram of system (2.21) and system (2.21) enters chaos when τ is close to 0.3, further verifying the inferred results. Figure 5(b) shows the attractive substructure of the system, which can be observed to be complex and not similar to the Lorenz system or other chaotic systems.



(a) system's bifurcation diagram over τ. (b) system's phase diagram when $\tau = 0.3$.

Figure 5. System chaotic performance over τ.

Based on the above analysis method, the Hopf bifurcation critical values of the heterogeneous single-delay general Lorenz system are obtained using time delays at different positions under $a = 10$, $b = -4$, $c = 2.5$, and $d = 2$, as listed in Table 1.

Table 1. Hopf bifurcation critical values of the heterogeneous single-delay general Lorenz system.

Position	A	B	C	D	E	F	G	H	I
Hopf bifurcation critical value	0.2173	0.1850	0.3276	0.3819	0.8107	0.2765	6265	0.4396	0.2253

A sequence set is constructed from the chaotic sequences generated by nine heterogeneous single-delay chaotic systems, and three sequences are randomly assigned into image pixel scrambling and diffusion operations.

3. Image encryption scheme

Figure 6 shows the whole process of encrypting and decrypting images by combining the chaotic sequences generated by nine heterogeneous single time-delay chaotic systems. The sequence generated by the chaotic system exhibits pseudo-random properties, and it is employed for scrambling and diffusion operations during encryption, so as to form a chaotic cipher. The chaotic cipher is characterized by a large key space, strong self-adaptation of the key stream and high security. With the theory of chaos having been deeply researched, researchers have revealed that low-dimensional or high-dimensional chaotic systems are subject to problems (e.g., simple structure and periodic windows). It is therefore revealed that the sequence resistance of the low-dimensional chaotic system is weak and easy to crack, and the security of the password cannot be ensured. Moreover, the chaotic cipher adopts the sequence of a single chaotic system for scramble operations and diffusion operations. The sequence is extremely easy to identify, and cryptographic security is not ensured. In accordance with the above problems, a sequence set composed of chaotic sequences came from multiple heterogeneous single-delay chaotic systems as appeared in this paper, and three sequences from the set are randomly selected for image pixel scrambling and diffusion operations. Thus, the cryptanalysis technology cannot capture the properties of the chaotic system, which is conducive to ensuring the password's security.

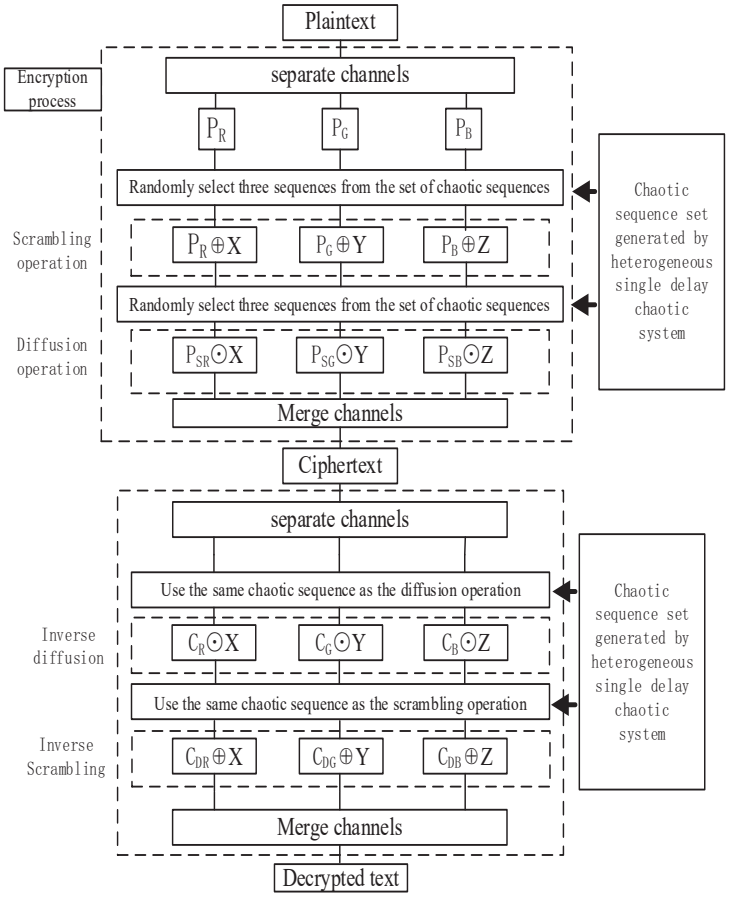


Figure 6. Encryption and decryption process and intermediate results.

The sequences from the heterogeneous time-delay chaotic system are employed to form a sequence set, and three sequences are randomly selected from the set for image scrambling and diffusion operations. It is therefore ensured that the randomly selected sequence does not necessarily originate from a chaotic system with a single time-delay, and cryptographic security is achieved.

3.1. Time-delay chaotic system generates pseudorandom sequences

Chaotic systems with time-delay and non-time-delay are essentially different in a considerable number of ways, and their dynamic behaviors are completely different. Time-delay chaotic systems refer to a class of infinite-dimensional dynamical systems. No matter how small the time delay is, the system's state space is infinite-dimensional and exhibits more complex dynamic behavior. Before encryption, nine heterogeneous single-delay general Lorenz systems are adopted to simultaneously generate 27 pseudo-random sequences for the formation of a sequence set. Subsequently, three sequences corresponding to the images after the color image separation channel are randomly selected from the sequence set for scrambling operations and diffusion operations. Accordingly, the chaotic cipher's key space is larger than that of the previous chaotic cipher. If the image size is $M \times N \times 3$, the amount of data generated using the time-delay chaotic system is significantly larger than $M \times N$. N and M denote the horizontal and vertical pixel values of the image, respectively.

3.1.1. Encryption method

The scrambling operation is the primary work of the encryption algorithm. To be specific, randomly selected sequences from the sequence set are arranged in an ascending order, and then the pixel positions of the plaintext image are transformed according to the sequence, so as to achieve the location of the obfuscated plaintext image pixels. The diffusion operation randomly selects sequences from the sequence set again to build a matrix and multiplies the matrix by the scrambled pixel matrix to capture the pixel matrix of the encrypted image.

For a color plaintext image P with a size of $M \times N \times 3$, where 3 denotes the number of channels of the color image, in accordance with the channel, P falls into three layers of P_R, P_G, and P_B, and scrambling and diffusion operations are performed for each layer. With P_R as an example, the 2D image matrix P_R is expanded into a one-dimensional vector by row or column, expressed as A; the following operations are performed with a sequence X randomly selected from the sequence set:

(1) Truncate the number of $M \times N$ at the given position parameter d and X to form $\{x_i, i = 1, 2, \cdots, MN\}$; each element of $\{x_i\}$ is rounded according to Eq (3.1).

$$x_i = (x_i * 10^4) \bmod MN + 1. \tag{3.1}$$

(2) Arrange $\{x_i\}$ in ascending order, remove duplicates, and perform a difference operation with the set $\{1, 2, 3, \cdots, MN\}$. The results are sorted in ascending order and added to the end of $\{x_i\}$.

(3) Swap the $A(x_i)$ and $A(x_{MN-i+1})$ positions. After the scrambling operation ends, the vector after scrambling is recorded as P_{SR}.

Sequences are selected randomly again from the sequence set to build a matrix, and a diffusion operation is carried out on the matrix of the scrambled image. The diffusion operation can be performed using Eq (3.2), and its inverse operation is Eq (3.3). The diffusion operation and the scrambling operation of the plaintext image are over.

$$C_i = C_{i-1} * x_i * P_{SRi} \tag{3.2}$$

$$P_{SRi} = C_i / C_{i-1} / x_i \tag{3.3}$$

The decryption algorithm is the inverse encryption algorithm's process, described as follows:

Algorithm: Image encryption algorithm based on heterogeneous time-delay chaotic system.

Input: Plaintext image;
Encryption key: chaotic system parameters, time delay position, time delay value, truncation sequence position parameter;
Output: Ciphertext image;

Step 1: Read plaintext images, construct matrices P_R, P_G and P_B, and form column matrices A_R, A_G and A_B, respectively.
Step 2: Establish a sequence set in accordance with the key information; randomly select three sequences (X, Y, Z) from the set; intercept the sequence following the position parameter.
Step 3: Perform a scrambling operation on P_R, P_G and P_B. According to Eq (3.1), round, sort and append the intercepted sequence $\{x_i\}$ to form a novel sequence $\{x_i\}$. Then, exchange the pixel positions in A_R, A_G and A_B to form a scrambling matrix P_{SR}, P_{SG} and P_{SB}.
Step 4: Implement a diffusion operation on P_{SR}, P_{SG} and P_{SB}. Again, three sequences (X, Y, Z) are randomly selected from the set, and the sequences are truncated based on the position parameter. The interception sequence $\{x_i\}$ is adopted for operation according to Eq (3.2) to form diffusion matrices P_{DR}, P_{DG} and P_{DB}.
Step 5: Combine P_{DR}, P_{DG} and P_{DB}.

3.1.2. Decryption method

Decryption algorithm is the reverse process of encryption algorithm, as presented below:

Algorithm: Image Decryption algorithm based on heterogeneous time-delay chaotic system..

Input: Ciphertext image;
Encryption key: chaotic system parameters, time delay position, time delay value, truncation sequence position parameter;
Output: Decrypted image;

Step 1: Read the ciphertext image and construct the matrix C_R, C_G and C_B.
Step 2: Form a sequence set according to the key information; select three sequences (X, Y, Z) from the set in the sequence selection manner; intercept the pseudo-random sequence $\{x_i\}$ following the position parameter.
Step 3: Implement the inverse diffusion operation onC_R, C_G and C_B; use the intercepted sequence $\{x_i\}$ to operate based on Eq (3.3) to form matrices C_{DR}, C_{DG} and C_{DB}.
Step 4: Perform the scrambling inverse operation on C_{DR}, C_{DG} and C_{DB}. Again, three sequences (X, Y, Z) are selected from the set by sequence selection. According to Eq (3.3), round, sort and append the intercepted sequence to form a novel sequence $\{x_i\}$. Subsequently, exchange the pixel positions in C_{DR}, C_{DG} and C_{DB} to establish a matrix C_{SR}, C_{SG} and C_{SB}.
Step 5: Combine C_{SR}, C_{SG} and C_{SB}.

3.2. *Experimental results and algorithm performance analysis*

The algorithm's effectiveness is verified by taking the Lena color image of size 1 as the test object. Color images' encryption and decryption are performed using the aforementioned heterogeneous single delay Lorenz system to form a sequence set. The number of sequence elements generated by the chaotic system with time-delay is significantly larger than the size of the color image, and is stored in a fixed manner. In the sequence, a certain number of elements are intercepted based on the position parameters to participate in the diffusion and scrambling operations. Table 1 and Figure 4 depict the parameters and initial conditions of the heterogeneous single-delay Lorenz system, with the location parameter of $d_i \geq 300$. The encryption algorithm's performance is evaluated through histogram analysis, adjacent pixel correlation coefficient analysis, NPCR and UACI analysis.

3.2.1. Histogram

Figure 7 illustrates the R, G, and B pixel histograms for the plaintext image. Figure 8 exhibits the R, G, and B pixel histograms for the encrypted image. Figure 9 depicts the R, G, and B pixel histograms for the decrypted image.

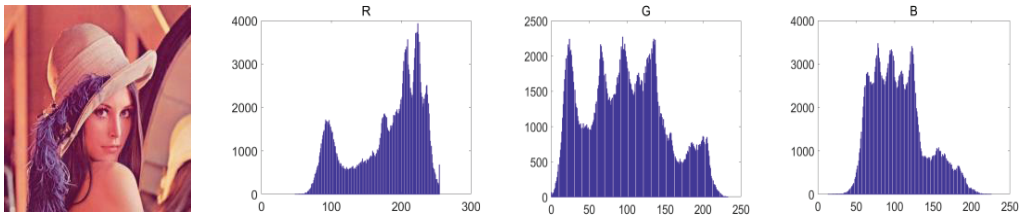


Figure 7. R, G, and B pixel histogram of the plaintext image.

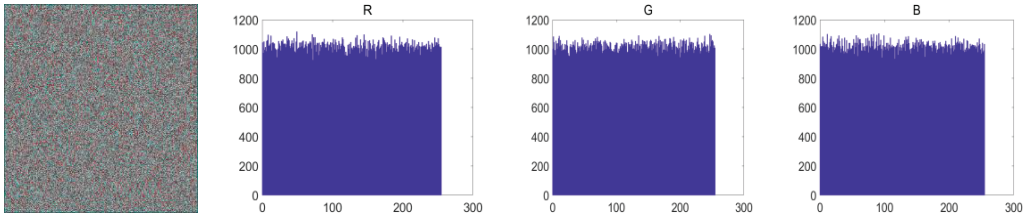


Figure 8. R, G, and B pixel histogram of the encrypted image.

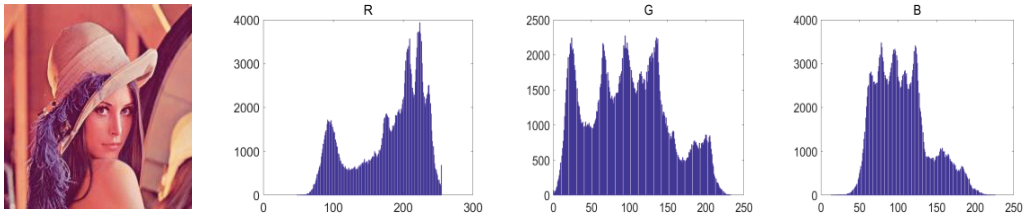


Figure 9. R, G, and B pixel histogram of the decrypted image.

Figure 7 depicts that the pixel values' distribution of the R, G and B channels of the plaintext image has apparent statistical laws, and the plaintext image's pixel value change curve is significant.

After scrambling and expansion operations are completed, the pixel values of the ciphertext image are evenly distributed in the respective gray level interval (Figure 8). In other words, the frequency of the respective encrypted image's pixel appears close. Moreover, the three channels are basically the same, and thus, statistical methods cannot be adopted to attack. As demonstrated in Figure 9, the pixel values' distribution of the R, G and B channels of the plaintext image is basically the same as that of the decrypted image. This suggests that the decryption effect is perfect, and the image can be restored to the plaintext image without being affected by the decryption algorithm. The above results confirm that the information of the plaintext image is effectively diffused, and the encryption algorithm has a good ability to resist statistical attacks.

3.2.2. Adjacent pixel correlation coefficient

The Pearson correlation coefficient is capable of effectively measuring the dependence of two adjacent sequences in an image in a certain direction. Next, the correlation coefficient is calculated directly using Eq (3.4) for the images before and after encryption.

$$r = \frac{n(\sum_{i=1}^{n} x_i y_i) - (\sum_{i=1}^{n} x_i)(\sum_{i=1}^{n} y_i)}{\sqrt{[n(\sum_{i=1}^{n} x_i^2) - (\sum_{i=1}^{n} x_i)^2][n(\sum_{i=1}^{n} y_i^2) - (\sum_{i=1}^{n} y_i)^2]}} \tag{3.4}$$

where $n(\sum_{i=1}^{n} x_i y_i) - (\sum_{i=1}^{n} x_i)(\sum_{i=1}^{n} y_i)$ denotes the sample variance, $n(\sum_{i=1}^{n} x_i^2) - (\sum_{i=1}^{n} x_i)^2$ and $n(\sum_{i=1}^{n} y_i^2) - (\sum_{i=1}^{n} y_i)^2$ denote the sample standard deviations of the sequences X_j and Y_j ($j = 1, 2, \cdots, m-1$), respectively. The correlation coefficient is one of the important indicators reflecting the encryption algorithm's performance. In general, the correlation coefficient between adjacent pixels can be calculated from the vertical direction, the horizontal direction, and the diagonal direction according to Eq (3.4). When determined in the horizontal direction, m is the row number of the encrypted image; when obtained in the vertical direction, m is the column number of the encrypted image; when calculated from the diagonal direction, m is the diagonal line number of the encrypted image. Table 2 lists the calculation result.

Table 2. Pearson correlation coefficients between adjacent pixels in different directions.

Image	Horizontal direction			Vertical direction			Diagonal direction		
	R	G	B	R	G	B	R	G	B
Original image	0.9002	0.9016	0.9675	0.9412	0.9522	0.9213	0.9423	0.9702	0.9772
Encrypted image	0.0122	0.0023	0.0206	0.0012	0.0056	0.0165	0.0025	0.0021	0.0024

Table 2 depicts that the encrypted image's correlation coefficients on the vertical, horizontal and diagonal lines all approach zero for the encryption implemented under the heterogeneous single-delay Lorenz system mapping. However, the above are just some of the overall results. The correlation of the plaintext image and the encrypted image in different directions are depicted one by one using a scatter plot to analyze the correlation between any two adjacent pixels in depth. Figure 10 illustrates the correlation coefficient results for the Lena image in the horizontal, vertical, and diagonal directions.

Figure 11 illustrates the correlation coefficient results of the encrypted image in horizontal, vertical, and diagonal directions.

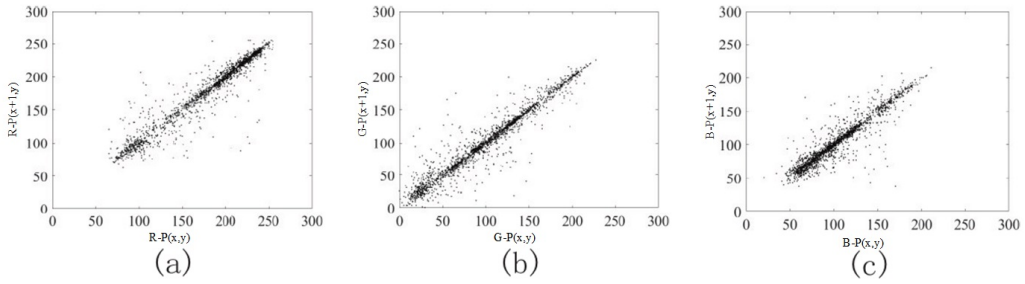


Figure 10. Correlation coefficients of the encrypted image in horizontal, vertical, and diagonal directions. (a) Horizontal direction, $r = 0.0122$, (b) Vertical direction, $r = 0.0012$, (c) Diagonal direction, $r = 0.0025$.

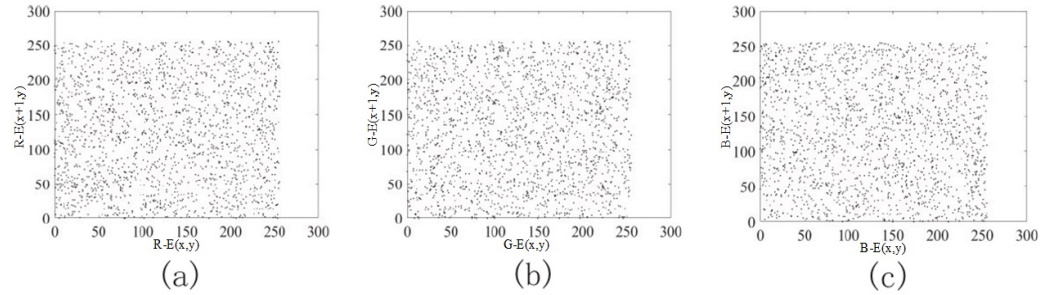


Figure 11. Encrypted image's correlation coefficients in horizontal, vertical, and diagonal directions. (a) Horizontal direction, $r = 0.0122$, (b) Vertical direction, $r = 0.0012$, (c) Diagonal direction, $r = 0.0025$.

As depicted in Figure 10, the plaintext image shows a high correlation between any two adjacent pixels in different directions. However, the correlation between adjacent pixels corresponding to the encrypted image is close to 0 (Figure 11). To be specific, the correlation coefficients changed from 0.9002, 0.9412 and 0.9423 to 0.0122, 0.0012 and 0.0025, respectively. It is therefore revealed that the encryption algorithm eliminates the correlation between the plaintext image's adjacent pixels, thus making it difficult for attackers to acquire any information of the plaintext image through correlation analysis.

3.2.3. Keyspace

The keyspace elements of the encryption and decryption algorithm consist of the time-delay Lorenz system's parameters a, b, c, initial conditions $x(t)$, $y(t)$, $z(t)$, time-delays τ_i, $i = 1$ to 9, time-delay position parameters, as well as intercepting pseudo-random sequences' position parameters. In MATLAB, 96-bits of storage system parameters, initial conditions and double delay are required, and the rest can be stored with 64 bits. The position parameter of time-delays is the position relation of time- delay quantities τ_i in the Lorenz system, and different position relations express a chaotic system with time-delay. Moreover, the pseudo-random sequence interception positions are three random

values, respectively representing the value positions on different state vectors. Accordingly, the number of all the different combinations of this cryptosystem is significantly higher than 2^{256}. The above large keyspace and the use at a time make the encryption algorithm sufficiently resistant to brute force attacks.

3.2.4. Key sensitivity

Key sensitivity is recognized as another significant indicator to measure the image encryption algorithm's performance. Encryption algorithms with prominent performance should generally be sensitive to keys, so cryptanalysts cannot crack them by repeated trials. The sensitivity here reveals that the decryption algorithm cannot recover the plaintext image or acquire the relevant information of the plaintext image even after a small modification of any element in the keyspace. In other words, only when a completely correct key is employed can the plaintext image be recovered by a decryption algorithm. Figure 12 presents the image (12 (b)) obtained by decryption with a correct key, the image (12 (c)) obtained by decryption with a wrong delay parameter τ, and the image (12 (d) obtained by intercepting position parameters in the direction of wrong pseudo-random sequence$x$ under the time-delay quantities of $\tau_A = 0.1521$.

Figure 12. Key sensitivity test. (a) Plaintext image, (b) Decryption image $\tau_A = 0.1521$, (c) Decryption image $\tau_A = 0.1522$, (d) Decryption image $d_x = 400$.

According to Figure 12(b),(c) when the parameters of the heterogeneous single time-delay chaotic system change slightly and other keys are adopted correctly, the decryption algorithm can neither recover and obtain the plaintext image nor acquire any information of the plaintext image. According to Figure 12(c),(d) the decryption algorithm cannot acquire any plaintext image's information when the position parameters intercepted by the pseudo-random sequence are changed or when other keys remain unchanged. This is because the small changes of system parameters and the changes of sequence interception positions generally cause a completely different chaotic matrix B, so the matrix A determined by $A = CB$ is overall inconsistent with the correct scrambling matrix. Thus, the decryption algorithm cannot recover the plaintext image.

3.2.5. NPCR and UACI

The average intensity of change (UACI) and the average rate of change of pixels (NPCR) represent two indicators to measure the diffusion effect of encryption algorithms. NPCR compares the number of changes of elements in the pixel matrix corresponding to the plaintext image and the encrypted image to ensure that sufficient elements of the pixel matrix are changed. UACI reveals the average change in

the pixel value of the corresponding position of the plaintext image and the encrypted image. They are defined as

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\% \tag{3.5}$$

$$UACI = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{|A(i,j) - A_{SD}(i,j)|}{255}. \tag{3.6}$$

Here,

$$D(i,j) = \begin{cases} 0, A(i,j) = A_{SD}(i,j) \\ 1, A(i,j) \neq A_{SD}(i,j) \end{cases}$$

where A denotes the plaintext image pixel matrix; M and N represent its rows and column numbers, respectively; and A_{SD} represents the encrypted image's pixel matrix. For two random images, the expected values for UACI and NPCR are 96.6094% and 33.4635%, respectively [43]. The NPCR and UACI of the encrypted image are close to their respective expected values, which indicates that the information of the plaintext image is significantly diffused into the encrypted image. Accordingly, the attacker's attempt to obtain information about the plaintext image through differential attack will be futile.

In accordance with Eqs (3.5) and (3.6), the UACI and NPCR values of the encrypted image can be calculated respectively. Table 3 lists the calculation results.

Table 3. NPCR and UACI test results of encrypted images.

Image	**NPCR(%)**			**UACI(%)**		
	R	G	B	R	G	B
Encrypted image	99.6011	99.6066	99.6200	33.1101	33.2622	33.3230
Average		99.6092			33.2384	

The results in Table 3 reveal that the average NPCR of encrypted images is 99.6092%, and the average UACI is nearly 33.2384%, both close to the expected value. To obtain better NPCR and UACI values, the number of columns should be up-regulated in the permutation matrix A. At this time, the size of the required chaos matrix B will increase. In this way, the information of the plaintext image will be better diffused into the encrypted image. Accordingly, the algorithm can effectively resist differential attacks.

3.2.6. Correlation comparison between adjacent pixels of encrypted images

The correlation coefficient's reduction between adjacent pixels of an encrypted image is an essential criterion to measure the encryption algorithm's security. This paper attempts to reflect the proposed algorithm's security by comparing it with other encryption algorithms. The image encryption schemes involved in the comparison consist of image encryption algorithms based on

multiple chaotic systems [43], bit-level scrambling and diffusion [21,44], generalized Arnold map [12], DNA sequence operation [24], and cyclic shift and XOR operation [45]. Table 4 lists the correlation coefficients between adjacent encrypted images' pixels under various schemes. To be specific, the results of correlation coefficient in the respective direction can be obtained by averaging the correlation coefficients of the R, G, and B layer pixel matrices.

Table 4. Comparison of correlation coefficients of adjacent pixels.

Encryption algorithm	Our	Huang [43]	Lin [21]	Ye [12]	Zhang [24]	Zahra [45]
Horizontal direction	0.0012	-0.0752	0.0315	0.0464	0.0713	0.0048
Vertical direction	0.0122	-0.0753	0.2651	0.0562	-0.3255	0.0231
Diagonal direction	0.0361	0.0466	0.0455	0.0397	-0.0423	0.0280
Average	0.0169	0.0661	0.2119	0.0478	0.1467	0.0190

As depicted in Table 4, in the comparison of the correlation coefficients of adjacent pixels, the proposed algorithm has the smallest correlation coefficients in the horizontal and vertical directions. In the diagonal direction, the proposed encryption method can lead to a smaller correlation between adjacent pixels of the encrypted image, besides Zahra's result. In the three directions, the results obtained by all algorithms are averaged by taking the absolute value, and the proposed algorithm is also proven to be optimal.

3.2.7. Chosen/known plain image attack

Various image encryption algorithms with excellent statistical results have been selected/cracked by known plaintext image attacks. In this paper, we consider the following measures to prevent this powerful attack. According to Eq (3.1), the permutation-diffusion process is implemented in a single stage, and thus the algorithm can resist divide-and-conquer attacks. According to Table 1, the encrypted chaotic sequence is obtained from the delay and the position of the delay in the chaotic system. The key to this algorithm is not using a single chaotic system to generate data, but employing multiple chaotic systems to generate data. Therefore, the encrypted chaotic sequences originating from multiple chaotic systems cannot be simulated and recognized by AI tools, thus preventing the secret key from being cracked.

In the selected plaintext image attack, cryptanalysts have temporary access to encryption equipment and can choose a specific image for encryption, attempting to find the used secret key: First, the cryptanalyst selects a black image with all pixel values fixed at zero (Figure 13(a)). Then, the cryptanalyst encrypts the black image (Figure 13(b)), resulting in the chaotic sequence possibly used in the encryption process (secret key). Afterward, the cryptanalyst can implement the known plaintext image attack using the Lena image (Figure 13(c)), but without success (Figure 13(d)). From Table 1, the Z−value of Figure 13(a) is $S = 0$, and the Lena image is encrypted using $S \neq 0$. Therefore, we obtain different Z−value and chaotic sequences for each plaintext image.

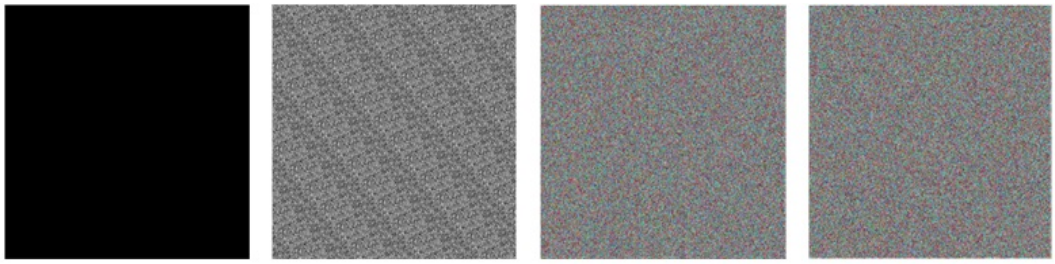


Figure 13. Chosen/known plain image attack. (a) chosen black plain image, (b) encrypted black image, (c) encrypted Lena image, and (d) decrypted Lena image with possible secret key from encrypted black image

In image encryption, the Z-value is commonly used to represent a chaotic sequence of pixel values. A chaotic sequence is a deterministic sequence that appears to be random and can be used in encryption algorithms to generate pseudo-random keystreams.In the context described, the Z-value may be a specific value from a sequence generated by a chaotic system, used to represent the initial state of pixel values or some form of key information. Cryptanalysts can utilize this Z-value to attempt to break the encryption algorithm by selecting specific plaintext images for encryption and observing the generated chaotic sequence in order to infer the key information used for encryption.In summary, the Z-value in image encryption can be used as part of a chaotic sequence to generate pseudo-random keystreams, thereby facilitating the process of encrypting and decrypting images.

3.2.8. Information entropy

Information entropy is a mathematical property that determines the randomness, unpredictability, or complexity of a message. If the encryption process does not produce enough disorder at the output, the cryptosystem can be the subject of the entropy attack. According to the information entropy calculation method given in the literature [46,47], we calculated the images before and after encryption respectively. In Table 5, the entropy results of both The Lena 256×256 RGB plain image and its corresponding encrypted image are presented. Therefore, the entropy value close to eight in the encrypted image means a highly unpredictable message; hence, the encryption algorithm can resist an entropy attack.

Table 5. Information entropy of the plain and encrypted image.

	Plain Image			Encrypted Image		
	R	G	B	R	G	B
H	7.6215	7.9425	7.7426	7.8695	7.9526	7.9265

3.2.9. Robustness evaluation

An excellent encryption system, if its encrypted image can effectively resist cropping and noise attacks, possesses good robustness. Taking the cropping attack for example, when the encrypted result is subjected to pixel cropping attacks, the quality of the reconstructed image is significantly reduced. Figure 14 demonstrates various degrees of pixel cropping and the corresponding decryption results,

along with an analysis of the encryption scheme's resistance to cropping attacks. It can be seen from the figure that the algorithm has a good ability to resist cropping attacks.

Figure 14. Clipping attack result.

3.2.10. Time efficiency analysis

In this section, we analyze the speed of the encryption system. To verify the significant improvement in encryption efficiency of the proposed scheme, we separately calculate the encryption time of the Lena image and the encryption time is obtained many times and averaged. From Table 6, it can be seen that the efficiency of encrypting images using this scheme is significantly better than that of encrypting plaintext images. Comparative experiments also show that our scheme has obvious advantages. The three algorithms were implemented using MATLAB 2022b and were implemented on an AMD Ryzen 96 900HX with Radeon Graphics, and the execution efficiency of the algorithms on color images was calculated.

Table 6. Speed analysis.

	ours	[48]	[47]
Average Speed (s)	1.4126	2.0322	2.0716

4. Conclusions

In view of the excellent qualities of time-delay chaotic systems, such as infinite dimension, a unique encryption scheme designed, and the proposed image encryption algorithm has the advantages of large

key space, high encryption efficiency and good security. The image encryption algorithm based on heterogeneous time-delay chaotic systems consists of adding a time-delay to different state variables of chaotic system to form multiple very complex time-delay chaotic systems. Subsequently, the resulting sequences generate a set of sequences employed for cryptographic operations (e.g., image scrambling and diffusion). In accordance with the location where the time lag is added, an encryption strategy is formulated in this location. In this paper, the designed image encryption scheme is presented from four perspectives, including an encryption algorithm, decryption algorithm, algorithm performance analysis and comparative analysis. The proposed encryption algorithm is characterized by its large key space, low computational complexity, and strong ability to resist statistical and differential attacks, which is simple. Moreover, this algorithm is easy to implement. Heterogeneous time-delay chaotic systems exhibit complex dynamic behavior and are capable of ensuring the security of the algorithm by generating chaotic sequences with strong randomness. However, this sequence generation calculation takes a long time. The sequence generated by the time-delay chaotic system can be stored in advance, and it can then be selected randomly and intercepted to achieve real-time encryption.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

Some of the authors of this publication are also working on these related projects: (1) higher vocational education teaching fusion production integration platform construction projects of Jiangsu province under grant no.2019(26), (2) natural science fund of Jiangsu province under grant no.BK20131097, (3) "Qin Lan project" teaching team in colleges and universities of Jiangsu province under grant no.2017(15), (4) high level of Jiangsu province key construction project funding under grant no.2017(17), (5)High Level Specialty Group Construction Project of Jiangsu province Higher Vocational Education under grant no.2021(1), (6) Vocational education teacher and teaching innovation team of Jiangsu province under grant no.2021(23), (7) Jiangsu province education science 14th Five-Year plan under grant no.D/2021/03/88, (8) Jiangsu province higher education teaching reform research project under grant no.2023JSJG593.

Conflict of interest

The authors declare no conflict of interest.

References

1. M. Bouchaala, C. Ghazel, L. A. Saidane, Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card, *J. Supercomput.*, **78** (2022), 497–522. https://doi.org/10.1007/s11227-021-03857-7
2. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, C. Wang, et al., Asynchronous updating Boolean network encryption algorithm, *IEEE T. Circ. Syst. Vid.*, **33** (2023), 4388–4400. https://doi.org/10.1109/TCSVT.2023.3237136

3. L. Yuan, S. Zheng, Z. Alam, Dynamics analysis and cryptographic application of fractional logistic map, *Nonlinear Dynam.*, **202** (2019), 615–636. https://doi.org/10.1007/s11071-019-04810-3
4. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, C. Wang, et al., A 3D model encryption scheme based on a cascaded chaotic system, *Signal Process.*, **202** (2023), 108745. https://doi.org/10.1016/j.sigpro.2022.108745
5. D. Park, S. Hong, N. S. Chang, S. M. Cho, Efficient implementation of modular multiplication over 192-bit NIST prime for 8-bit AVR-based sensor node, *J. Supercomput.*, **77** (2021), 4852–4870. https://doi.org/10.1007/s11227-020-03441-5
6. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, C. Wang, et al., EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory, *Inform. Sciences*, **621** (2023), 766–781. https://doi.org/10.1016/j.ins.2022.11.121
7. X. Huang, Image encryption algorithm using chaotic Chebyshev generator, *Nonlinear Dynam.*, **67** (2012), 2411–2417. https://doi.org/10.1007/s11071-011-0155-7
8. X. Wang, L. Liu, Y. Zhang, A novel chaotic block image encryption algorithm based on dynamic random growth technique, *Opt. Laser. Eng.*, **66** (2015), 10–18. https://doi.org/10.1016/j.optlaseng.2014.08.005
9. A. Akhshani, A. Akhavan, S. C. Lim, Z. Hassan, An image encryption scheme based on quantum logistic map, *Commun. Nonlinear Sci.*, **17** (2012), 4653–4661. https://doi.org/10.1016/J.CNSNS.2012.05.033
10. Y. Guo, J. Yang, B. Liu, Application of chaotic encryption algorithm based on variable parameters in RFID security, *EURASIP J. Wirel. Comm.*, **155** (2021), 1–22. https://doi.org/10.1186/s13638-021-02023-0
11. F. Pichler, J. Scharinger, *Finite dimensional generalized baker dynamical systems for cryptographic applications*, International Conference on Computer Aided Systems Theory, 1995, 465–476.
12. G. Ye, K. W. Wong, An efficient chaotic image encryption algorithm based on a generalized Arnold map, *Nonlinear Dynam.*, **69** (2012), 2079–2087. https://doi.org/10.1007/s11071-012-0409-z
13. F. Sun, S. Liu, Z. Li, Z. Lü, A novel image encryption scheme based on spatial chaos map, *Chaos Soliton. Fract.*, **38** (2008), 631–640. https://doi.org/10.1016/j.chaos.2008.01.028
14. F. Sun, Z. Lü, S. Liu, A new cryptosystem based on spatial chaotic system, *Opt. Commun.*, **283** (2010), 2066–2073. https://doi.org/10.1016/j.optcom.2010.01.028
15. H. J. Liu, X. Y. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, *Opt. Commun.*, **284** (2011), 3895–3903. https://doi.org/10.1016/J.OPTCOM.2011.04.001
16. Z. Zhu, W. Zhang, K. W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, *Inform. Sciences*, **181** (2011), 1171–1186. https://doi.org/10.1016/j.ins.2010.11.009

17. P. Manjunath, K. L. Sudha, Chaos image encryption using pixel shuffling, *Comput. Sci. Inform. Tech.*, **1** (2012), 169–179. https://doi.org/10.5121/csit.2011.1217
18. Y. Jiang, B. Li, *A novel image encryption algorithm based on logistic and henon map*, In: 2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2016, 66–69.
19. G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos Soliton. Fract.*, **21** (2004), 749–761. https://doi.org/10.1016/j.chaos.2003.12.022
20. S. Zhou, Y. Qiu, G. Qi, A new conservative chaotic system and its application in image encryption, *Chaos Soliton. Fract.*, **175** (2023), 113909. https://doi.org/10.1016/j.chaos.2023.113909
21. Y. Luo, M. Du, A novel digital image encryption scheme based on spatial-chaos, *J. Converg. Inform. Tech.*, **7** (2012), 199–207. https://doi.org/10.4156/jcit.vol7.issue3.23
22. C. Li, Y. Liu, L. Y. Zhang, M. Z. Q. Chen, Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation, *Int. J. Bifurcat. Chaos*, **23** (2013), 1350075. https://doi.org/10.1142/S0218127413500752
23. C. Gangadhar, K. D. Rao, Hyperchaos based image encryption, *Int. J. Bifurcat. Chaos*, **19** (2009), 3833–3839. https://doi.org/10.1007/s10489-023-04727-w
24. Q. Zhang, X. L. Xue, X. P. Wei, A novel image encryption algorithm based on DNA subsequence operation, *The Scientific World J.*, **17** (2015), 6954–6968. https://doi.org/10.3390/e17106954
25. S. Lian, J. Sun, Z. Wang, A block cipher based on a suitable use of the chaotic standard map, *Chaos, Soliton. Fract.*, **26** (2005), 117–129. https://doi.org/10.1016/j.chaos.2004.11.096
26. Q. L. Chen, X. H. Hao, X. P. Yan, P. Li, A high performance waveform and a new ranging method for the proximity detector, *Def. Technol.*, **16** (2020), 1–12. https://doi.org/10.1016/j.dt.2019.10.009
27. F. Gao, D. H. Hu, H. Q. Tong, C. M. Wang, Chaotic analysis of fractional Willis delayed aneurysm system, *Acta Phys. Sin.-Ch. Ed.*, **67** (2018). https://doi.org/10.7498/aps.67.20180262
28. D. Ding, F. Liu, H. Chen, N. Wang, D. Liang, Sliding mode control of fractional-order delayed memristive chaotic system with uncertainty and disturbance, *Commun. Theor. Phys.*, **68** (2017), 741. https://doi.org/10.1088/0253-6102/68/6/741
29. X. An, X. Li, Q. Shi, S. Qiao, L. Zhang, Dynamics explore of an improved HR neuron model under electromagnetic radiation and its applications, *Nonlinear Dynam.*, **111** (2023), 9509–9535. https://doi.org/10.1007/s11071-023-08320-1
30. J. Li, J. Huang, Subharmonic resonance of a clamped-clamped buckled beam with 1:1 internal resonance under base harmonic excitations, *Appl. Math. Mech.*, **41** (2010), 1–16. https://doi.org/10.1007/s10483-020-2694-6
31. H. M. Zhu, W. F. Chen, R. P. Zhu, L. Zhang, J. Gao, M. J. Liao, Dynamic analysis of a flexible rotor supported by ball bearings with damping rings based on FEM and lumped mass theory, *J. Cent. South Univ.*, **27** (2020), 3684–3701. https://doi.org/10.1007/s11771-020-4510-z
32. J. K. Hale, *Theory of functional differential equation*, Theory of Functional Differential Equation, New York: Springer, 1977, 12–13. https://doi.org/10.1007/978-94-015-8084-7

33. S. Ruan, J. Wei, On the zeros of a third degree exponential polynomial with applications to a delayed model for the control of testosterone secretion, *IMA J. Math. Appl. Med.*, **18** (2001), 41–52. https://doi.org/10.1093/imammb/18.1.41

34. T. Faria, L. T. Magalhaes, Normal forms for retarded functional differential equations and applications to Bogdanov-Takens singularity, *J. Differ. Equations*, **122** (1995), 201–224. https://doi.org/10.1006/jdeq.1995.1145

35. T. Faria, L. T. Magalhaes, Normal forms for retarded functional differential equations with parameters and applications to Hopf bifurcation, *J. Differ. Equations*, **122** (1995), 181–200. https://doi.org/10.1006/jdeq.1995.1144

36. T. Faria, Normal forms for semilinear functional differential equations in Banach spaces and applications, Part II, *Discrete Cont. Dyn.-A*, **7** (2012), 155–176. https://doi.org/10.3934/dcds.2001.7.155

37. G. M. Mahmoud, A. A. Arafa, E. E. Mahmoud, Bifurcations and chaos of time delay Lorenz system with dimension 2n+1, *Eur. Phys. J. Plus*, **132** (2017), 461. https://doi.org/10.1140/epjp/i2017-11739-6

38. K. Tian, H. P. Ren, C. Grebogi, Existence of chaos in the chen system with linear time-delay feedback, *Int. J. Bifurcat. Chaos*, **29** (2019), 2708–2710. https://doi.org/10.1142/S0218127419501141

39. W. Li, X. Niu, X. Li, Y. Yu, Hopf bifurcation analysis of the disturbed Lorenz-like System with the delayed, *Pure Appl. Math.*, **262** (2015), 335–343. https://doi.org/10.1016/j.amc.2015.04.072

40. E. Zhu, M. Xu, D. Pi, Hopf bifurcation and stability of the double-delay Lorenz system, *Int. J. Bifurcat. Chaos*, **33** (2023), 1–14. https://doi.org/10.1142/S0218127423500153

41. G. R. Guan, C. M. Wu, J. Qian, An improved high performance Lorenz system and its application, *Acta Phys. Sin.-Ch. Ed.*, **64** (2015), 20501–020501. https://doi.org/10.7498/aps.64.020501

42. Y. Li, Z. Wei, A. A. Aly, A 4D hyperchaotic Lorenz-type system: Zero-Hopf bifurcation, ultimate bound estimation, and its variable-order fractional network, *Eur. Phys. J.*, **231** (2022), 1847–1858. https://doi.org/10.1140/epjs/s11734-022-00448-2

43. X. L. Huang, Image encryption algorithm using chaotic Chebyshev generator, *Nonlinear Dynam.*, **67** (2012), 2411–2417. https://doi.org/10.1007/s11071-011-0155-7

44. L. Teng, X. Wang, A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive, *Opt. Commun.*, **285** (2012), 4048–4054. https://doi.org/10.1016/j.optcom.2012.06.004

45. Z. Parvin, H. Seyedarabi, M. Shamsi, A new secure and sensitive image encryption scheme based on new substitution with chaotic function, *Multimed. Tools Appl.*, **75** (2014), 10631–10648. https://doi.org/10.1007/s11042-014-2115-y

46. M. A. Murillo-Escobar, M. O. Meranza-Castillón, R. M. López-Gutiérrez, C. Cruz-Hernández, Suggested integral analysis for chaos-based image cryptosystems, *Entropy*, **21** (2019), 815. https://doi.org/10.3390/e21080815

47. R. Hosseinzadeh, M. Zarebnia, R. Parvaz, Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral, *Opt. Laser Technol.*, **120** (2019), 105678. https://doi.org/10.1016/j.optlastec.2019.105698

48. X. Wang, S. Chen, Y. Zhang, A chaotic image encryption algorithm based on random dynamic mixing, *Opt. Laser Technol.*, **138** (2021), 106837. https://doi.org/10.1016/j.optlastec.2020.106837

AIMS Press