Data Encryption System Based on Four-dimensional Chaotic System with PSO Parameter Optimization

Qi Liang, Qian Xiong*, Chunsheng Jiang, Wenxin Yu

Abstract—**This paper addresses the challenges of high computational costs and prolonged processing times in chaotic system parameter calculations by integrating the Particle Swarm Optimization (PSO) algorithm into chaotic systems, searching for optimal parameters. A novel data encryption system is proposed, integrating a four-dimensional chaotic system with PSO-based parameter optimization.**

In the first step, A new four-dimensional chaotic system is formulated with reference to the simplified Lorentz chaotic system, and the chaotic properties of the chaotic system are analyzed, such as dissipation analysis, equilibrium point analysis and Lyapunov exponential analysis. In the second step, the equation delineating the mathematical relationship between the parameters of the chaotic system and the maximum Lyapunov exponent is constructed, the optimal parameter values of the chaotic system are found based on the PSO algorithm, and the chaotic characteristics of the simplified Lorenz chaotic system, the optimized chaotic system and the original system are compared and analyzed. In the third step, the optimized chaotic system's output sequence is merged with perturbation and diffusion algorithms for performing image encryption and decryption, and the encryption security analysis is carried out. Finally, the encryption and decryption function are implemented on ZYNQ.

Through software testing and hardware experimental evaluation, the system shows stable security performance, and can adapt to the security communication needs of different encryption objects, which have certain practical application values.

Index Terms—**Chaos, Data encryption, PSO algorithm, ZYNQ platform**

I. Introduction

With the deep connection between science and technology, computer technology and Internet applications, the information field pays more and more attention to data security, and once some information is leaked, it will inevitably lead to some irreversible consequences, such as economic losses and security threats. Therefore, based on the diversity and sensitivity of information and data, it is particularly important to build a safe and reliable confidential communication system. Secure communication hinges on encryption algorithms. Researchers in the area have proposed numerous algorithms and applied them to encryption tasks, such as 3DES (Triple Data Encryption Standard) [1], ECC (Elliptic Curve Cryptography) [2] and so on.

Chaos theory is one of the greatest discoveries in physics in the 20th century, and together with quantum mechanics and relativity theory, it is known as the three major milestones of 20th century science. Because of the pseudo-randomness, hiddenness, high susceptibility to initial values and unpredictability in the long run of chaotic systems, many researchers have focused on chaotic cryptography. In chaotic systems, a large number of non-periodic, noise-like signals can be generated, and this property can be used to achieve encryption of data. For example, a chaotic system is used to encrypt power data [3], or to fuse chaos with other theories to innovate encryption methods, such as the combination of chaos theory and DNA coding principle [4], the fusion of chaotic system and block compression sensing [5], and the integration of chaotic system and neural network [6]. Therefore, it is possible to encrypt chaotic sequences generated by chaotic systems as encrypted sequences, which have a huge key space and are strongly influenced by the internal parameters of the chaotic system and its initial state are designed so that slight parameter tweaks or initial condition changes can cause significant mutations in the generated encrypted sequences [7]. Dingwell J B posits that Lyapunov characteristic exponents occupy a pivotal role in delineating the behavioral patterns of dynamical system [8]. To make sure chaotic systems are stable and reliable, this paper is devoted to exploring and determining the optimal parameters of the system. To this end, a functional relationship between chaos parameters and Lyapunov exponent is constructed to maximize the Lyapunov exponent to boost system complexity and reliability, and shield the encryption performance.

Optimization problems are ubiquitous in life and scientific research, addressing many challenges, and the swarm intelligence algorithms have become one of the efficient solutions due to their unique advantages. For instance, Kennedy and Eberhart introduced PSO, a bio-inspired algorithm that locates optimal solutions via population-based collaborative and divisive exploration[9]. Wu D et al. proposed a unique intelligent diagnostic approach aimed at identifying and solving faults in motor bearings more efficiently [10]. Wang C et al. adopted artificial intelligence

Manuscript received September 26, 2024, revised July 18, 2025.

This work was supported by a grant (No. NCOC-24-03) from Key Laboratory of Nonlinear Circuit and Optical Communications (Guangxi Normal University).

Qi Liang is a visiting student of Key Laboratory of Nonlinear Circuit and Optical Communications, Guangxi, China (e-mail: 2692057273@qq.com).

Qian Xiong is a postgraduate student of Hunan University of Science and Technology, Xiangtan, China (corresponding author to provide e-mail: 2077193636@qq.com).

Chunsheng Jiang is an associate professor of School of Guangxi Normal University, Guangxi, China (e-mail: 20210038@mailbox.gxnu.edu.cn).

Wenxin Yu is a lecturer at School of Information and Electrical Engineering, Hunan University of Science and Technology, Xiangtan, China (e-mail: slowbird@sohu.com).

algorithm methods to optimize the weights of indicators [11]. You Z P et al. proposed a nature-inspired and chaos theory that merges ant colony optimization (ACO) and particle swarm optimization (PSO) to improve image quality [12]. Bigdellou S et al. suggested a hybrid PSO-heuristic algorithm that integrates combinatorial Benders' cuts to dynamically address road blockages and fuel constraints in wildfire evacuation[13]. Allaoui et al. introduced t-SNE-PSO, a PSO-enhanced manifold learning algorithm ,improving clustering silhouette scores by 27% and overcoming gradient descent's susceptibility to local optima[14]. The above literature is sorted out and analyzed to provide a clear insight into the value of the application of intelligent algorithms in the problem solving domain. Based on this, PSO algorithm is introduced in this paper for the specific and critical context of optimal parameter finding.

To guarantee the efficacy of encryption algorithms in practical implementations, Liu X et al. built a chaotic cryptographic encryption system grounded in discrete memristor and meminductor tech on the DSP platform [15]. Mohamed G et al. successfully built a sturdy system for real-time image encryption and decryption on an FPGA platform [16]. The practical applicability of FPGAs has facilitated the offline implementation of encryption algorithms in various application scenarios. In this context, this paper explores the hardware implementation of the encryption system designed for the ZYNQ platform, emphasizing its technical rigor and practical applicability.

In summary, this paper presents an image encryption system using a 4D chaotic system and PSO parameter optimization. Here, the knowledge of chaos theory, nonlinear system, control theory and intelligent algorithm is comprehensively utilized to construct a complex chaotic system and use them in the data encryption system. The designed encryption algorithm's reliability and complexity are boosted by maximizing the Lyapunov exponent of the built chaotic system.

II. Parameter Optimization of Four-Dimensional Chaotic System

A. Construction of a Four-dimensional Chaotic System and its Dynamics Analysis

The simplified Lorenz chaotic system is represented by the following Eq. (1) [17]:

$$\begin{cases} \dot{x} = m(y-x) \\ \dot{y} = (24-4g)x + gy - xz \\ \dot{z} = -nz + xy \end{cases} \tag{1}$$

In Eq. (1). The system dimensions are denoted by x, y, z , while the system parameters are denoted by m, n, g . The usual setup parameters are $m = 2, n = \frac{8}{3}, g = 2$ .The simplified Lorenz chaotic system is a simplification of the classical Lorenz system, which retains the chaotic properties but is simpler to compute, and exhibits complex dynamical behavior with a small number of variables and equations.

Using the simplified Lorenz chaotic system from Eq. (1), a four-dimensional chaotic system is built with the Eq. (2):

$$\begin{cases} \dot{x} = a(y-x) - bzw \\ \dot{y} = (18-2c)x - cyz - 8.546xw \\ \dot{z} = 5xy + 3z - 6w^2 \\ \dot{w} = 7z - 2yw \end{cases} \tag{2}$$

In Eq. (2). x, y, z, w is the dimension of the system and a, b, c is the system parameter. The dissipative nature of this system is articulated in Eq. (3):

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = -a - cz + 3 - 2y \tag{3}$$

Thus when $-a - cz + 3 - 2y < 0$ the system shows dissipative traits and converges an exponential rate $e^{(-a-cz+3-2y)}$, so that as time t tends to infinity, every tiny volume element in the dynamic trajectory of the system follows an exponential decay law, gradually shrinking to zero, implying that all of the system's trajectories will ultimately converge and be confined to a zero-volume set of limit points. This process reveals that the asymptotic dynamical behavior of the system will be fixed to an attractor, thus confirming the possible existence of a chaotic attractor within the system.

Let $\dot{x} = \dot{y} = \dot{z} = \dot{w} = 0$, which gives the equilibrium point of the system as $(0,0,0,0)$, and through linearizing the system at the equilibrium state point, we obtain the Jacobi matrix of the system: $J = \begin{bmatrix} -a & a & 0 & 0 \\ 18-2c & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 7 & 0 \end{bmatrix}$.

To derive the characteristic equation associated with J at the equilibrium point, let $|\lambda E - J| = 0$, then the characteristic equation at the equilibrium point is expressed as Eq. (4).

$$\lambda(\lambda - 3)\left(\lambda^2 + a\lambda + a(2c-18)\right) = 0 \tag{4}$$

Solving Eq. (4) yields $\lambda_1 = 0, \lambda_2 = 3$, $\lambda_{3,4} = \frac{-a \pm \sqrt{a^2 - 4a(2c-18)}}{2}$, and the Routh–Hurwitz stability criterion posits that for a system to remain stable, it is necessary for the real part of all its eigenvalues to be negative. However, according to the calculated eigenvalues, it can be seen that there are eigenvalues with positive and solid parts in the system, which indicates the system presents unstable characteristics when at the equilibrium point $(0,0,0,0)$. It is therefore possible that the system may exhibit chaotic or more complex hyperchaotic behavior.

The parameter variations of the system are not only concerned with the maintenance of its equilibrium point's stability, but also affect the chaotic phenomena within the system, prompting its changes. In order to deeply observe and analyze the chaotic dynamics' trajectory alterations in the system the paper examines the dynamics behaviors of the system in terms of Lyapunov exponents of different variables.

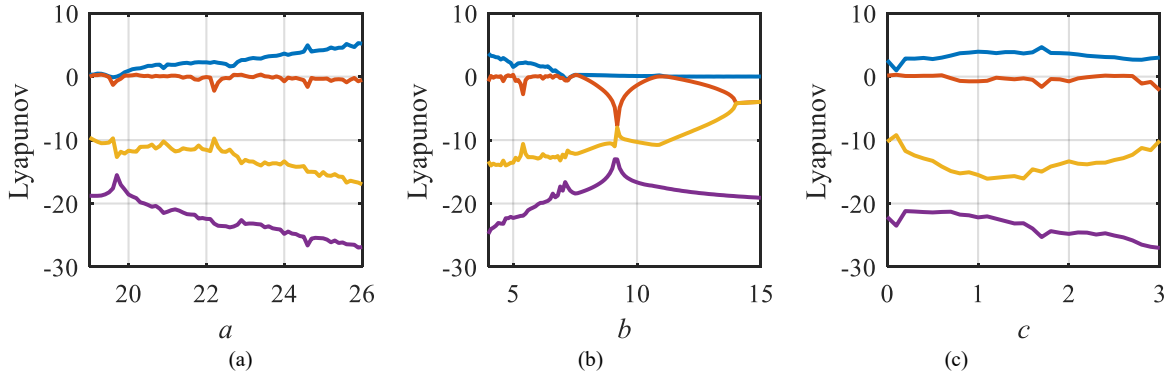

Fig. 1. Dynamic analysis of parameter variations: (a) $b=4.00, c=2, a\in(19,26)$,(b) $a=24, c=2, b\in(4,15)$,(c) $a=24, b=4, c\in(0,3)$

The Lyapunov exponent is a quantitative measure that provides an average estimation of the rate of convergence or divergence of neighboring trajectories in a system's phase area. For a system with attractors of chaotic nature, its characteristics are: (1) a positive Lyapunov exponent can at least be identified, (2) there must be one Lyapunov exponent that is zero, (3) the sum of all Lyapunov exponents must be negative. The maximum Lyapunov exponent plays a pivotal role in the exploration of chaotic phenomena, which is not only a key symbol for judging whether a system is characterized by chaotic behavior or not in a given state, but also able to elucidate the extent of chaos and reveal the high sensitivity of the system to minor discrepancies in the initial conditions. In light of the fact that the system constructed in this paper has a dimension of four, the system has four corresponding Lyapunov exponents. By monitoring and evaluating the maximum values of these four indices, it is possible to determine whether the system is in a chaotic state with a high degree of certainty. Specifically, when the magnitude of the maximal Lyapunov exponent exceeds zero, it means that the system is diverging exponentially between trajectories.

Varying the parameters $a,b,c(a\in[19,25],\ b\in[4,15],\ c\in[0,3])$, respectively, the values of the Lyapunov exponents for the system are depicted in Fig. 1(a)(b)(c) under the assumption that all other parameters remain constant. In Fig. 1(a)(b)(c), a state of chaos is exhibited by the system when the maximum Lyapunov exponent takes on a positive value and the other Lyapunov exponents satisfy the above characteristics.

B. Optimization Of System Parameters

This paper utilizes the PSO algorithm to conduct optimization on chaotic parameter tuning to construct a chaotic system with obvious chaotic features, and the proposed implementation flowchart is shown in Fig. 2.

The Particle Swarm Algorithm (PSO), an intelligent optimization methodology grounded in the group dynamics observed in nature, is harnessed in this paper to conduct exploratory research and determine the optimal configuration of the chaotic system parameters a,b,c .By adjusting these parameters, the optimization process is carried out on the system's maximum Lyapunov exponent with the aim of achieving its maximum possible value, which in turn optimizes the chaotic properties of the system and improves its performance in applications.

The specific of the PSO algorithm to find the optimal a,b,c to obtain the optimal system are as follows:

Step 1 Specific parameters are configured as follows: the population dimension is assigned a value of 3, the particle count is set at 20, and the upper limit for the number of iterations is established as 301, the position restriction $a\in[19,26],\ b\in[0,8], c\in[0,5]$, the particle velocity restriction is set to $u_{\min}=-1,\ u_{\max}=1$, the inertia weight $\omega=1$, the individual learning factor $d_1=1.5$, the population learning factor $d_2=1$, additionally, the initial values for the chaotic system $(5,1,5,1)$ are determined and specified.

Step 2 Initialize the number of iterations $k=0$, and randomly initialize the particle velocity and particle position within the set position and velocity limits, and subsequently for each particle position corresponding to the parameters a,b,c , substitute them into the chaotic system model to calculate the maximum Lyapunov exponent of the system, which is taken as the value of the objective function as shown in Eq. (5). By comparing the fitness of each particle, the initial best individual position and the best group position are determined, additionally, the value of the maximum Lyapunov exponent corresponding to this instance is documented.

$$\begin{cases} ly_i=\dfrac{\ln\left|triu_{ii}(J\cdot E)\right|}{N}, i=\{1,2,3,4\} \\ Ly=sort(ly_1,ly_2,ly_3,ly_4) \end{cases} \tag{5}$$

Then the value of the maximum Lyapunov exponent is Ly_4 , while the above equation needs to satisfy $Ly_4>0\,\&\,\sum_{i=1}^{4}Ly_i<0\,\&\,Ly_2\cdot Ly_3=0$. In Eq. (5) $triu_{ij}(\bullet)$ denotes i rows and j columns of $\bullet$, $sort(\bullet)$ denotes the sorting of all elements in $\bullet$ from smallest to largest, E is the unit matrix, J is the Jacobi matrix of the system as shown in Eq. (6).

$$J=\begin{bmatrix} -a & a & -bw & -bz \\ 18-2c-8.546w & -cz & -cy & -8.546x \\ 5y & 5x & 3 & -12w \\ 0 & -2w & 7 & -2y \end{bmatrix} \tag{6}$$

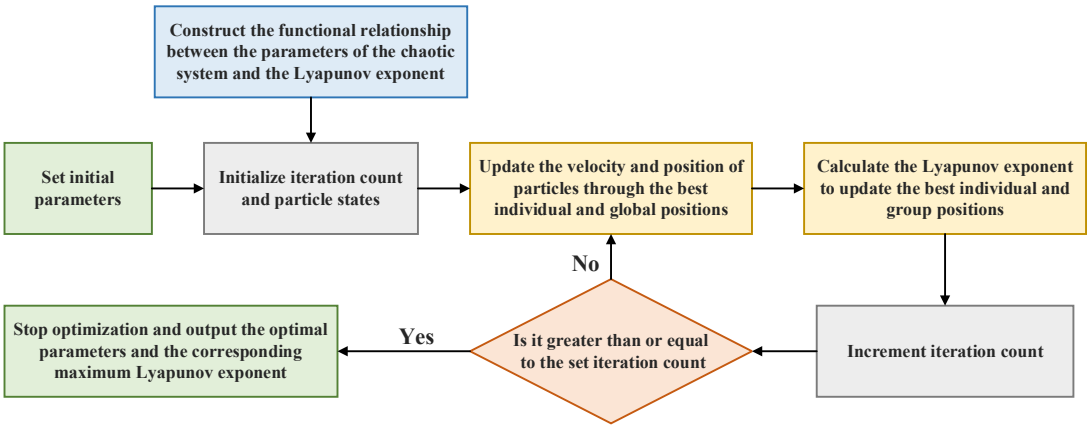

Fig. 2. Implementation flowchart

Step 3 Implementing the refreshment of particle velocities and positions by the individual optimal position W_{id} and the population optimal position W_{od} ,as shown in Eq. (7).

$$\begin{aligned} U_i^{k+1} &= \omega U_i^k + d_1 e_1 (W_{id}^k - Q_i^k) + d_2 e_2 (W_{od}^k - Q_i^k) \\ Q_i^{k+1} &= Q_i^k + U_i^{k+1} \end{aligned} \tag{7}$$

In Eq. (7), $i = 1,2,\cdots N$, N is the length of the sequence, d_1 is the individual learning factor, and d_2 is the population learning factor, k represents the count of iterations at the present stage, U_i is the velocity of the particle, Q_i is the position of the particle, ω is the inertia weight, e_1 and e_2 are random numbers belonging to the interval [0,1].

Step 4 Recalculate the fitness (maximum Lyapunov exponent) of each particle after the update and compare it with the previous best individual and population fitness. If better fitness is found, update the best individual position and the best population position. At the same time, the number of iterations k is added by one.

Step 5 Loop **steps 3** and **steps 4**, and when the number of iterations k reaches a set value, the search for the optimal parameter superiority is stopped and output the final optimal population position (the optimal parameter a,b,c) and the corresponding maximum Lyapunov exponent.

After the above steps, 20 sets of experimental tests were completed, and the results of one of the experiments were taken to obtain the optimal parameters of the four-dimensional system at this point in time as $a = 24.76225, b = 3.803894, c = 1.394659$, and the maximum Lyapunov exponent as 7.171601 . The parameter results of this experimental test satisfy the parameter range mentioned in the previous section, Substituting the parameters a,b,c obtained from optimization into Eq. (2) so that the system can output the chaotic sequence with the maximum Lyapunov exponent. The optimization graph obtained from the experimental test is shown in Fig. 3, and the test results of Lyapunov exponent obtained from other experiments fluctuate between 6.7 and 7.8, which is close to the results of other experiments in the past, showing good consistency and stability.

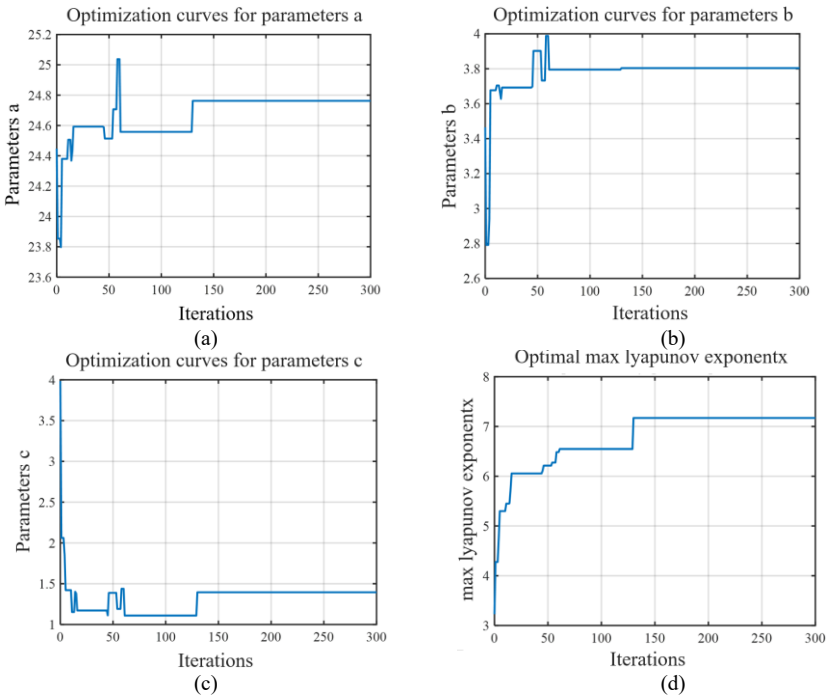

Fig. 3. Optimization curve diagram: (a) Parameter an optimization, (b) Parameter b optimization, (c) Parameter c optimization, (d) Maximum Lyapunov exponential optimization

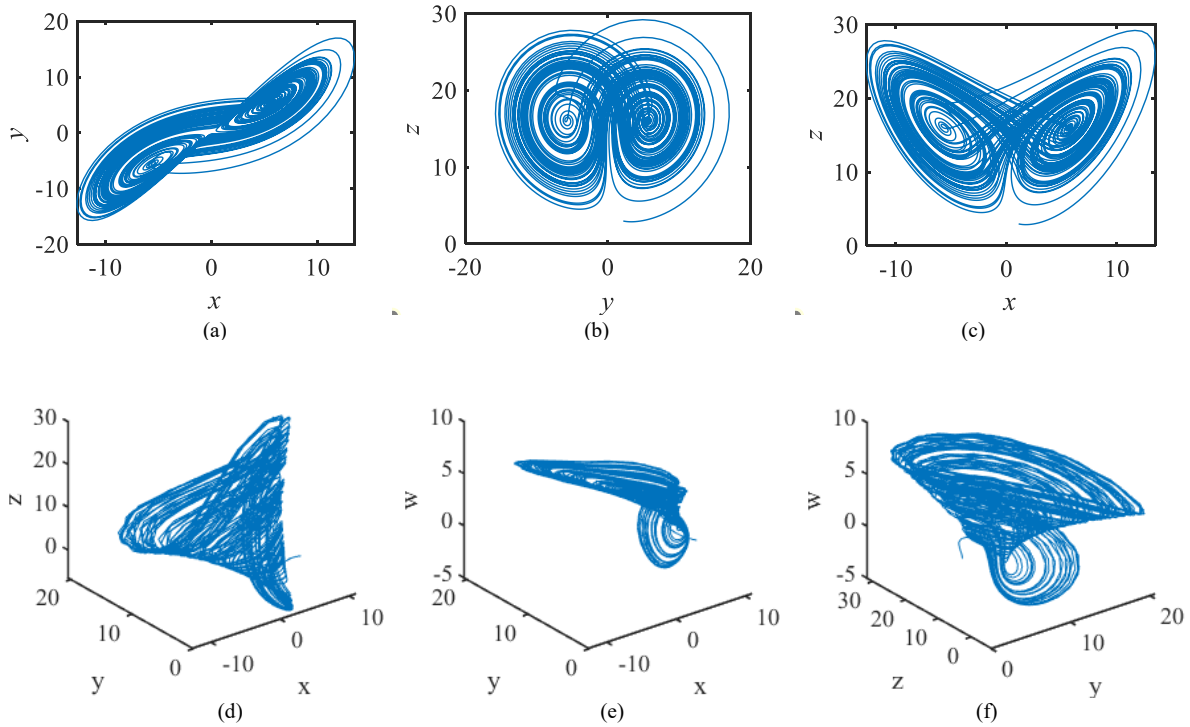

Fig. 4. Phase portrait of attractor for simplified Lorenz chaotic system: (a)x-y, (b)y-z, (c)-z. Phase portrait of attractor for simplified Lorenz chaotic system:(d) x-y-z, (e)x-y-w, (f)y-z-w.

C. Comparative analysis of the dynamics of the optimized chaotic system and the original chaotic system

Establishing the parameter values of the simplified Lorenz system to be $m=2, n=\frac{8}{3}, g=2$, the initial value is $[x0, y0, z0]=[1,2,3]$, Phase diagram of the system can be obtained as shown in Fig. 4(a)(b)(c).

Taking the optimal parameter obtained above $a=24.76225, b=3.803894, c=1.394659$ and the initial value of the chaotic system is $[x0, y0, z0, w0]=[5,1,5,1]$, the phase diagram of the chaotic system as shown in Fig. 4(d)(e)(f) is generated. In Fig. 4, it can be seen that the states in which both the simplified Lorenz system and the optimized system in this paper are located have relatively obvious chaotic characteristics. And the phase trajectory of the chaotic attractor shows a large number of distortions and folding in the phase space, forming a seemingly disordered curve, and this complexity makes the behavior of the chaotic system difficult to be predicted and control. Therefore, the output sequence of the system has sufficient complexity and is characterized by sensitivity to its initial value and system parameters, non-periodicity, etc., which makes it suitable for application in confidential communication.

The 0-1 test constitutes a testing algorithm that can measure whether a time series is chaotic, and for non-chaotic systems, the trajectory motion of the 0-1 test demonstrates bounded movement, indicating that the domain of values is restricted to a finite range, For a system that has entered a chaotic state, the trajectory motion of the 0-1 test exhibits unbounded properties similar to Brownian motion, and then the value can be assumed to fluctuate infinitely over time without being confined to any fixed range.

The graph of the 0-1 test results for the optimized four-dimensional chaotic system is shown in Fig. 5. The trajectory motion obtained for the optimized four-dimensional chaotic system exhibits properties analogous to those observed in Brownian motion, thus, it suggests that the system is experiencing a chaotic state.

The complexity of a chaotic system can measure how closely a chaotic sequence approximates a random sequence. As the complexity value increases, the degree of randomness in the sequence also rises, and correspondingly, the better the chaotic characteristics. Among the measures of chaotic system complexity, both SE complexity and C_o complexity are of particular importance. These indicators mirror the inherent characteristics of the system in the frequency domain through different computational methods.

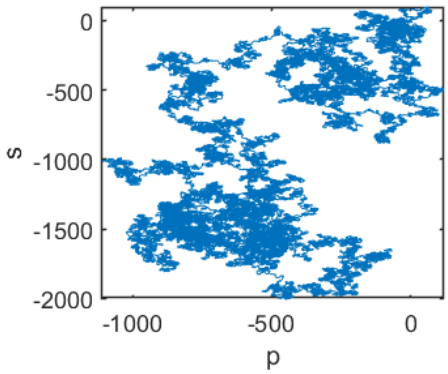

Fig. 5 The 0-1 test graph of the optimized chaotic system.

SE complexity: By calculating the relative power spectrum predicated on the energy allocation situation in the Fourier transform domain, and subsequently incorporating Shannon entropy probability, the corresponding spectral entropy value can be derived. Eq. (8) for SE complexity is shown as follows.

$$SE(N)=\frac{-\sum_{K=0}^{\frac{N}{2}-1}P_k \ln P_k}{\ln(\frac{N}{2})} \tag{8}$$

N stands for the length measurement of the chaotic sequence, P_k indicates the relative power spectrum probability associated with the sequence.

C_o complexity: Disassemble the chaotic sequence into regular and irregular parts, and then compute the percentage that the irregular part occupies within the chaotic sequence. Eq. (9) for C_o complexity is shown as follows.

$$C_O(N)=\frac{\sum_{n=0}^{N-1}\left|x(i)-\tilde{x}(i)\right|^2}{\sum_{n=0}^{N-1}\left|x(i)\right|^2} \tag{9}$$

N stands for the length measurement of the chaotic sequence, $x(i)$ represents the chaotic sequence $\{x(i), i=0,1,2,\cdots,N-1\}$, $\tilde{x}(i)$ represents the result of applying an inverse Fourier transform 0after performing a Fourier transform on $x(i)$ and removing the irregular components.

TABLE I
Complexity of Different Chaotic Systems

System	SE Complexity	C_o Complexity
Simplified Lorenz system	0.4041	0.1337
Original system	0.6318	0.4126
Optimized system	0.6560	0.4495

As shown in Table 1, the optimized chaotic system demonstrates the highest SE complexity and C_o complexity, followed by the constructed original chaotic system, in contrast, the simplified Lorenz chaotic system occupies the lowest position in the ranking. This indicates that the chaotic sequence produced by the optimized system exhibits greater complexity, with enhanced chaotic characteristics, thereby providing greater security in image information transmission.

III. Encryption System and Experimental Analysis

Digital images contain more information compared to data information and are a representative data structure. In order to verify the optimized four-dimensional chaotic system which is based on the PSO optimization algorithm presented in the context of the present study, it is employed for the purpose of image encryption and the related analysis and evaluation are carried out. The complexity and practicality of it for data encryption are further confirmed through experimental analyses.

Taking the encryption of color image data with grey level $L=256$ and size $M\times N\times 3$ as an example, the formulated data encryption system process predicated on the four - dimensional chaotic framework and PSO parameter searching is shown in Fig. 6. To begin with, the PSO algorithm is applied to identify the most suitable parameters a,b,c of the chaotic system and then the parameters a,b,c of the optimal system are substituted into the four-dimensional chaotic system, so that the system outputs the chaotic sequence with the maximum complexity. Finally, using the sequence of the output of the chaotic system optimized by the PSO algorithm, chaotic disruption and diffusion matrices were created, and these two matrices were subsequently applied to the encryption process of plaintext images to achieve disruption and diffusion processing of the images.

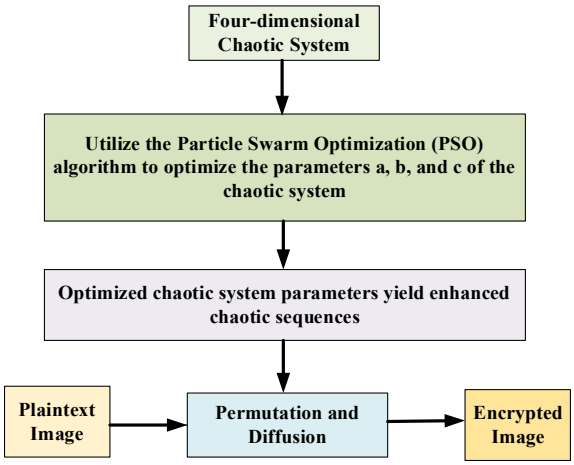

Fig. 6. Image encryption process based on parameter-optimized four-dimensional chaos

In the disruption process, the generated chaotic disruption matrix is employed to modify the positional configuration of pixels in the plaintext image. The pixel positions within the disrupted image undergo modification, yet the gray - level value of every pixel remains unaltered, so the distribution of the grey value and the related statistical characteristic information of the image are not affected. In the subsequent diffusion stage, the diffusion matrix constructed using chaos theory transforms the grayscale intensities of the image with dislocated pixels, it adeptly conceals the statistical traits inherent in the original image. Meanwhile, the decryption stage acts as the inverse operation of encryption, bringing the image back to its initial condition.

The initial value $[x0, y0, z0, w0]$ of the four-dimensional chaotic system is used as the encryption and decryption key, and the default key used in this paper is $[x0, y0, z0, w0]=[5,1,5,1]$. Fig. 7 presents the outcomes derived from the encryption and decryption experimental procedures of some common color images, as shown in the figure, in which the size of Lena image is $256\times256\times3$, the size of House image is $256\times256\times3$, and the size of Baboon image is $512\times512\times3$. From the figure, it can be clearly observed that the plaintext data within the ciphertext image is entirely concealed. Moreover, the decrypted image precisely matches the original plaintext image, and the image encryption method proposed in this paper is effective in encrypting and decrypting the image using the parameter optimized four-dimensional chaotic system. This manuscript presents a four - dimensional chaotic system - based image encryption approach, which is grounded on parameter optimization, which can effectively perform image encryption and decryption.

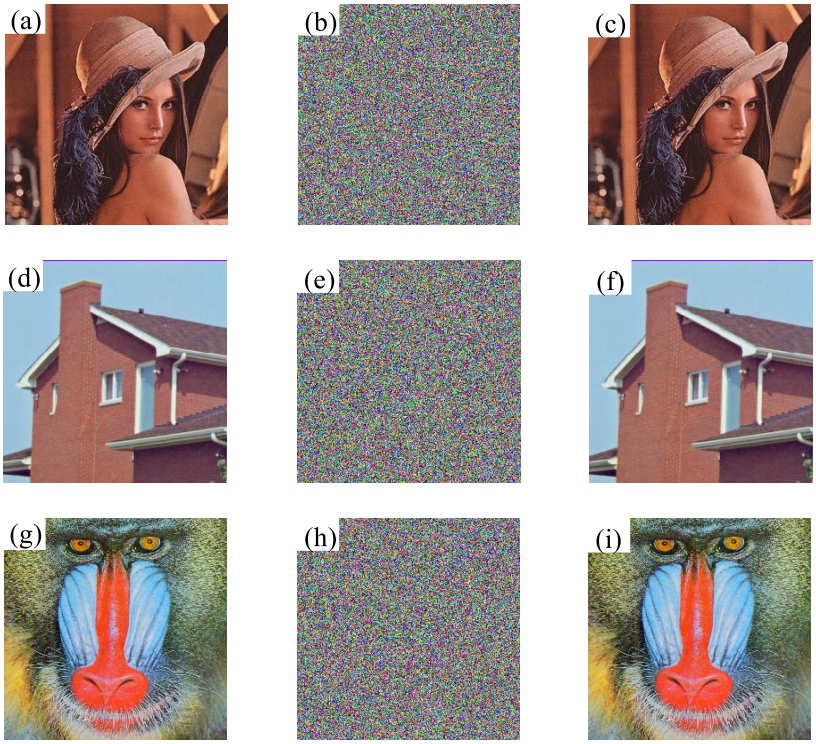

Fig. 7. Experimental diagram of image encryption and decryption: (a) Lena plaintext image, (b) Lena ciphertext image, (c) Lena decrypted image, (d) House plaintext image, (e) House ciphertext image, (f) House decrypted image, (g) Baboon plaintext image, (h) Baboon ciphertext image, (i) Baboon decrypted imag

IV. Encryption Security Analysis

A. Histogram Analysis

Histogram analysis techniques are applied to perform an evaluation on the allocation pattern of various grey levels across an image, and ideally, the histogram should exhibit a uniform distribution, meaning that all grey values are employed in the encrypted image in approximately equal amounts, consequently, it becomes highly challenging to infer any details regarding the original image based on the frequency distribution of its gray values.

Fig. 8 shows a plaintext histogram and a ciphertext histogram of the Lena image. As depicted in the figure, the histogram corresponding to the plaintext image indicates an irregular distribution pattern among individual gray values, which reflects the original image content, while the gray value distribution in the ciphertext histogram tends to be uniform, and the encrypted image can be better protected against statistical attacks.

B. Relevance Analysis

Correlation between neighboring pixels is also a detection metric in statistical analysis, including horizontal neighboring pixel point correlation, vertical neighboring pixel point correlation, orthogonal neighboring pixel point correlation, and anti-diagonal neighboring pixel point correlation. Ideally, in a plaintext image, neighboring pixels are strongly correlated with each other, there is not supposed to be any correlation between neighboring pixels in a ciphertext image.

While two interdependent and uncorrelated random sequences have a theoretical correlation coefficient of 0, indicating that there is no linear correlation between them, on the contrary, when two random sequences are completely linearly correlated, their correlation coefficients will reach a theoretical maximum value of 1, which signifies that there is a complete positive linear relationship between them.

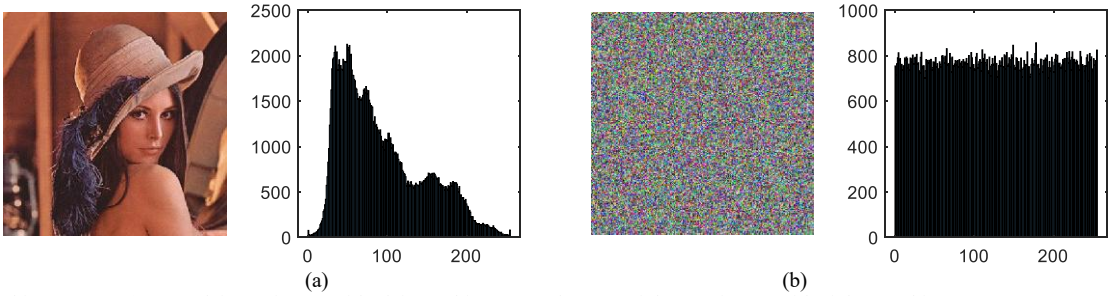

Fig. 8. Image histograms: (a) Lena plaintext image with plaintext histogram, (b) Lena ciphertext image with ciphertext histogram

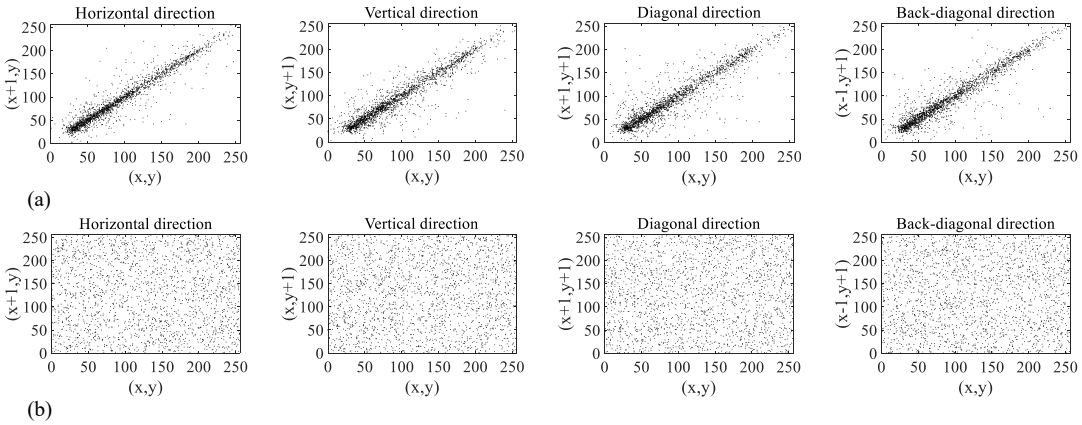

Fig. 9. Lena image: (a) correlation of plaintext image in each direction, (b) correlation of ciphertext image in each direction

Fig. 9 presents the relationship of correspondence between the Lena plaintext image and its encrypted ciphertext image after the optimization proposed in this paper as an encrypted sequence in all directions of the Lena image. Table 2 lists its correlation coefficients in each direction, with the additional presentation of the correlation coefficients of the resulting ciphertext images, when the simplified Lorenz system and the unoptimized system proposed in this paper are used as encryption sequences, respectively.

TABLE II
Correlation Coefficients

Image	Horizontal Direction	Vertical direction	Forward diagonal direction	Anti-diagonal direction
Plaintext Image	0.9568	0.9343	0.9166	0.9248
Encrypted Image1	0.0096	0.0094	0.0092	0.0093
Encrypted Image2	0.0095	0.0094	0.0092	0.0093
Encrypted Image3	0.0095	0.0093	0.0092	0.0093

The correlation coefficients presented in Table 2 represent the mean values derived from 1000 experimental trials, and these values indicate that the relevance of the plaintext image between neighboring pixels is strong in each direction, while the relevance of the three ciphertext image is quite different, and the relevance of the neighboring pixels approaches to zero in every direction, presenting an approximate uncorrelated state. And Encrypted Image 1 corresponds to the image encrypted employing the chaotic sequence that is produced through the simplified Lorenz chaotic system. Encrypted Image 2 corresponds to the image encrypted employing the chaotic sequence that is produced through the constructed original chaotic system. Encrypted Image 3 corresponds to the image encrypted employing the chaotic sequence that is produced through the optimized chaotic system.

As shown in Table 2, in the forward diagonal direction, the correlation coefficients of encrypted image 1, encrypted image 2, and encrypted image 3 are all 0.0092. In the anti-diagonal direction, they are all 0.0093. In the horizontal direction, the correlation coefficients for encrypted image 2 and encrypted image 3 both register at 0.0096, which is 0.0001 lower than that of encrypted image 1 and closer to 0. In the vertical direction, the correlation coefficients of encrypted image 1 and encrypted image 2 are both 0.0094, and that of encrypted image 3 is 0.0001 lower than encrypted image 1 and encrypted image 2, closer to 0. This indicates that, in comparison to the simplified Lorenz chaotic system and the sufficiently simple original chaotic system, the chaotic sequence of the optimized chaotic system results in lower correlation after image encryption, demonstrating better performance.

C. Information Entropy Analysis

The concept of information entropy reflects the inherent disorder within digital images. Greater entropy levels indicate more complicated image structures and poorer visual distinctness. The computational formula for determining entropy is:

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \tag{10}$$

In Eq. (10), L is the number of grey levels of the image and $p(i)$ is the occurrence probability of gray-level value i. Theoretical analysis shows that the upper bound of information entropy H for a grayscale random image is 8 (based on the case where L is 256). As the image's information entropy approaches the theoretical maximum of 8, it can be regarded as a random image.

TABLE III
Information Entropy

Image		Information Entropy
Lena image (256×256)	Plaintext Image	7.5176
	Encrypted Image	7.9991
House image (256×256)	Plaintext Image	7.0686
	Encrypted Image	7.9990
Baboon image (512×512)	Plaintext Image	7.7624
	Encrypted Image	7.9997

From Table 3, the experimental results demonstrate that when employing the optimized chaotic sequence generated by our proposed system for encryption, the resulting ciphertext image exhibits significantly higher information entropy compared to the original plaintext. Notably, both entropy values approach the theoretical maximum of 8, confirming the superior performance of the encryption scheme.

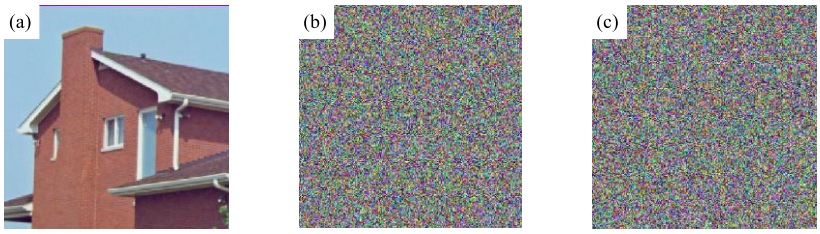

Fig. 10. Forward encryption and decryption of House image: (a) original image, (b) encrypted image, (c) wrongly decrypted image

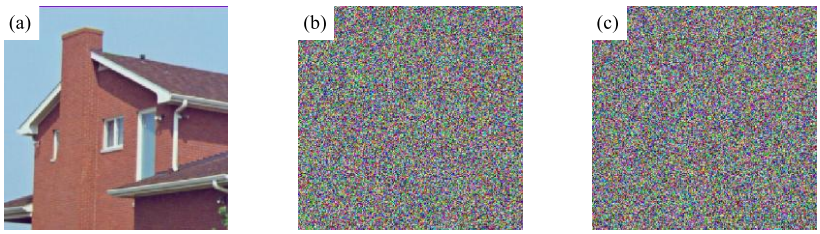

Fig. 11. House image reverse encryption and decryption: (a) original image, (b) encrypted image, (c) incorrectly decrypted image

D.Key Sensitivity Analysis

The objective of the key sensitivity analysis is to examine the response characteristics in which a slight change in the key, even if the encryption is of the same original plaintext image, results in a notable disparity is observed between the two generated ciphertext images, such a difference to the extent that the original key can no longer be used to efficiently decrypt any of the images that were encrypted with the changed key, thus ensuring that the encryption process is highly security and robustness of the encryption process.

As shown in Fig. 10, the original key $K=[x0,y0,z0,w0]=[5,1,5,1]$ is set, and the original key is slightly adjusted to $K'=[x0,y0,z0,w0]=[5+10^{-10},1,5,1]$. The House image is encrypted by the original key K, and then the encrypted image is decrypted by K'.

On the contrary, the House image is encrypted by the key $K'=[x0,y0,z0,w0]=[5+10^{-10},1,5,1]$, and then the encrypted image is decrypted by the original key $K=[x0,y0,z0,w0]=[5,1,5,1]$, and the result of the encryption and decryption is illustrated in Fig. 11.

Observing Fig. 10 and Fig. 11, it can be concluded that the small difference between keys (even if it is only of the order of 10^{-10}) is enough to cause the encryption system to be unable to perform effective decryption, which reflects the good response sensitivity of the encryption system designed in this paper under key changes.

E. Cryptographic Quality Analysis

In order to analyze the cryptographic quality of the encryption algorithm proposed in this paper, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM) are used as evaluation metrics. MSE is a key quantitative measure of the degree of variation between image pairs, with increasing MSE values indicating greater differences, the more significant the alteration of the original information by the encryption process is, thus reflecting the better encryption effect. PSNR is defined according to MSE PSNR is a metric for evaluating the similarity between images, ranging from 0 to 1. For identical images without any changes, the SSIM value is 1, whereas for images with very different contents, the SSIM value tends to be zero.

Table 4 summarizes the encryption quality assessment results obtained for various images. Observing the values of the metrics in Table 4, it can be obtained that all the color images present high MSE values after encryption under different color components, while the PSNR of these images are below 10 dB, in addition, the SSIM values are approaching zero. These data verify the effective obfuscation and protection of image information by the encryption algorithm.

TABLE IV
Correlation Coefficients Analysis of Quality Indicators

Image	MSE			PSNR (dB)			SSIM		
	R	G	B	R	G	B	R	G	B
Lena (256×256×3)	8658	9456	10430	8.75	8.37	7.94	0.0095	0.0085	0.0095
House (256×256×3)	6829	8643	9598	9.78	8.76	8.30	0.0106	0.0094	0.0092
Baboon (512×512×3)	8649	7748	9508	8.76	9.23	8.34	0.0106	0.0087	0.0085
Lena (256×256×3)	8658	9456	10430	8.75	8.37	7.94	0.0095	0.0085	0.0095

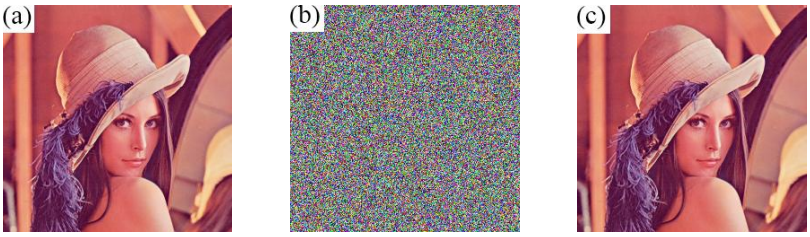

Fig. 12. Hardware circuit display result diagram: (a) the unencrypted image, (b) the image formed after encryption, (c) the image that has been decrypted and restored

V. Hardware Circuit Experiment

The experimental setup utilizes the XILINX ZYNQ7000 platform, featuring dual-core ARM Cortex-A9 processors and FPGA programmable logic components. The relevant chaotic circuits have been constructed using the platform, and chaotic encrypted sequences have been imported into the circuits. The confidential communication system formed by combining them with the chaotic diffusion algorithm has been mapped to the ZYNQ, and the experimental outcomes are illustrated in Fig. 12 and Fig. 13.

The results of the images generated by the confidential communication system in the ZYNQ experimental platform and displayed on the display are shown in Fig. 13, and the images exported from the SD card are shown in Fig. 12, where Fig. 12(a) is the unencrypted image Fig. 12(b) is the image formed after encryption, and Fig. 12(c) is the image that has been decrypted and restored. Comparison of Fig. 12(a) and Fig. 12(b) demonstrates that the unencrypted image and the image formed after encryption exhibit significant non-correlation, ensuring that it is difficult to establish a direct link between the two is challenging, whether visually or analytically. Comparison of Fig. 12(a) and Fig. 12(c) reveals that the unencrypted image is the same as the image that has been decrypted, and that the image has been completely restored through the decryption circuit. The experiments results demonstrate the efficacy of the secure communication system can correctly carry out secure communication, the image data can be concealed within the carrier, and the data content will not be lost during the secure communication process. The efficacy of the proposed secure communication system founded on the four-dimensional chaotic system and the PSO parameter optimization data encryption method is demonstrated by its practical application.

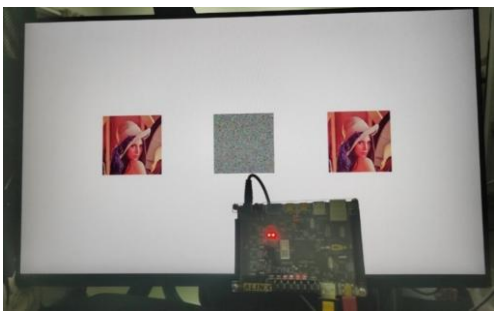

Fig. 13. Confidential communication system in the ZYNQ experimental platform implementation and display results

VI. Conclusion

A four-dimensional chaotic system is suggested in this paper, and a data encryption method based on the four-dimensional chaotic system and PSO parameter optimization is constructed. Firstly, according to the mathematical relationship equation between the designed chaotic system parameters and the maximum Lyapunov exponent, the PSO algorithm is applied to optimize the parameters of the four-dimensional chaotic system to obtain the optimal chaotic system, so that the chaotic sequence output is more appropriate for signal encryption, and the optimized chaotic system is analyzed by attractor phase map, 0-1 test map and complexity analysis to verify its good performance. Secondly, the digital image is scrambled and diffused using the chaotic sequence output from the optimized four-dimensional chaotic system, so as to achieve the purpose of encrypting the image information. The encryption effect security analysis is conducted from the histogram analysis, correlation analysis, information entropy analysis, key sensitivity analysis and encryption quality analysis of the plaintext image and the ciphertext image, and the test results verify the validity and dependability in the novel encryption scheme developed in this study, and the designed encryption method has a sound encryption and decryption performance, which provides reliable encryption scheme for the practical application of data encryption. Finally, an image encryption system based on four-dimensional chaotic system and PSO parameter optimization was implemented on the ZYNQ platform, and the software test and hardware experiment verify that the system has good confidentiality performance and practical application effect.

References

[1] Tezcan C, “Key lengths revisited: GPU-based brute force cryptanalysis of DES, 3DES, and PRESENT,” Journal of Systems Architecture, vol. 124, pp. 102402, 2022.

[2] Ullah S, Zheng J, Din N, et al., “Elliptic Curve Cryptography, Applications, challenges, recent advances, and future trends: A comprehensive survey,” Computer Science Review, vol. 47, pp. 100530, 2023.

[3] Zhang F, Huang Z, Kou L, et al., “Data encryption based on a 9D complex chaotic system with quaternion for smart grid,” Chinese Physics B, vol. 32, no. 1, pp. 010502, 2023.

[4] Wang X, Liu C, “A novel and effective image encryption algorithm based on chaos and DNA encoding,” Multimedia Tools and Applications, vol. 76, no. 5, pp. 6229-6245, 2017.

[5] Dou Y ,Yue S ,Zhang X , et al., “A special image encryption strategy based on a novel digital chaotic system and binary block compressed sensing for fixed-point DSP,” Nonlinear Dynamics, vol. 113, no. 9, pp. 10535-10558, 2025.

[6] Tao Y, Cui W H, Zhang Z, and Shi T W, “An Image Encryption Algorithm Based on Hopfield Neural Network and Lorenz HyperChaotic System,” IAENG International Journal of Computer Science, vol. 49, no. 4, pp. 1201-1211, 2022.
[7] Wang S, Peng Q, Du B, “Chaotic color image encryption based on 4D chaotic maps and DNA sequence,” Optics & Laser Technology, vol. 148, pp. 107753, 2022.
[8] Dingwell J B, “Lyapunov exponents”, Wiley encyclopedia of biomedical engineering, vol. 2104, pp. 127-133, 2014.
[9] J. Kennedy and R. Eberhart, “Particle swarm optimization", Proc. ICNN95–Int. Conf. Neural Networks, vol. 4, pp. 1942-1948, 1995.
[10] Deng W, Yao R, Zhao H, et al. , “A novel intelligent diagnosis method using optimal LS-SVM with improved PSO algorithm,” Soft computing, vol. 23, no. 7, pp. 2445-2462, 2019.
[11] Wang C N, Yang F C, Nguyen V T T, et al. , “CFD analysis and optimum design for a centrifugal pump using an effectively artificial intelligent algorithm,” Micromachines, vol. 13, no. 8, pp. 1208, 2022.
[12] You Z P, Yi D J, Fang Z, Zhang W H, “Image Enhancement ANPSO Processing Technology Based on Improved Particle Swarm Optimization Algorithm,” IAENG International Journal of Computer Science, vol. 51, no. 11, pp. 1781-1792, 2024.
[13] Bigdellou S ,Chen Q ,Beheshti S , “A novel Hybrid PSO-Heuristic Algorithm with Combinatorial Benders' Cuts for maximal evacuation planning in wildfire disasters,” Applied Mathematical Modelling, vol. 145, pp. 116131-116131, 2025.
[14] Allaoui M ,Belhaouari B S ,Hedjam R , et al., “t-SNE-PSO: Optimizing t-SNE using particle swarm optimization,” Expert Systems With Applications, vol. 269, pp. 126398-126398, 2025.
[15] Liu X, Mou J, Zhang Y, et al. , “A new hyperchaotic map based on discrete memristor and meminductor: dynamics analysis, encryption application, and DSP implementation,” IEEE Transactions on Industrial Electronics, vol. 71, no. 5, pp. 5094-5104, 2023.
[16] Gafsi M, Hajjaji M A, Malek J, et al. , “FPGA hardware acceleration of an improved chaos-based cryptosystem for real-time image encryption and decryption,” Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 6, pp. 7001-7022, 2021.
[17] Sun K H, Sprott J.C., “Dynamics of simplified Lorenz system,” International Journal of Bifurcation and Chaos, vol. 19, no. 4, pp. 1357-1366, 2009.

Qi Liang received the B.E. degree in optoelectronic information science and engineering from the Hunan University of Science and Technology, Xiangtan, China, in 2022, where she is currently pursuing the M.S. degree. Her research interests include signal processing and circuit design.

Qian Xiong received the B.E. degree in optoelectronic information science and engineering from the Hunan University of Science and Technology, Xiangtan, China, in 2024, where she is currently pursuing the M.S. degree. Her research interests include signal processing and circuit design.

Chunsheng Jiang, associate researcher, graduated from the Department of Microelectronics and Nanoelectronics at Tsinghua University in July 2018 with a PhD in Engineering. Research direction: Experimental preparation, mechanism modeling, and simulation of novel semiconductor low-power devices (FinFET, Tunneling FET, Junctionless Transistor, Negative capacitance Transistor, etc.)

Wenxin Yu received the B.Sc. degree in applied mathematics from Hebei Normal University, Shijiazhuang, China, in 2005, the M.S. degree in wavelet analysis from the Changsha University of Science and Technology, Changsha, China, in 2008, and the Ph.D. degree in electrical engineering from Hunan University, Changsha, in 2015. He was with the Hunan University of Science and Technology, Xiangtan, China, where he is currently a Lecturer with the School of Information and Electrical Engineering. His interests include the research of intelligent control, fault diagnosis, signal processing, wavelet analysis, and its application.