

An enhanced fingerprint template protection scheme based on four-dimensional superchaotic system and dynamic DNA coding

Baiqiang Hu(胡百强), Jiahui Liu(刘嘉辉), Zhe Liu(刘喆)

Citation: Chin. Phys. B, 2025, 34 (**7**): 070505. DOI: 10.1088/1674-1056/adca9fJournal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Resonant tunneling diode cellular neural network with memristor coupling and its application in police forensic digital image protection

Fei Yu(余飞), Dan Su(苏丹), Shaoqi He(何邵祁), Yiya Wu(吴亦雅), Shankou Zhang(张善扣), and Huige Yin(尹挥戈)
Chin. Phys. B, 2025, 34 (**5**): 050502. DOI: 10.1088/1674-1056/adb8bb

A novel approach to visual image encryption: 2D hyperchaos, variable Josephus, and 3D diffusion

Yan Hong(洪炎), Xinyan Duan(段心妍), Jingming Su(苏静明), Zhaopan Wang(王昭盼), and Shihui Fang(方士辉)
Chin. Phys. B, 2025, 34 (**4**): 040504. DOI: 10.1088/1674-1056/adacc7

Hybrid image encryption scheme based on hyperchaotic map with spherical attractors

Zhitang Han(韩智堂), Yinghong Cao(曹颖鸿), Santo Banerjee, and Jun Mou(牟俊)
Chin. Phys. B, 2025, 34 (**3**): 030503. DOI: 10.1088/1674-1056/ada7db

A color image encryption scheme based on a 2D coupled chaotic system and diagonal scrambling algorithm

Jingming Su(苏静明), Shihui Fang(方士辉), Yan Hong(洪炎), and Yan Wen(温言)
Chin. Phys. B, 2024, 33 (**7**): 070502. DOI: 10.1088/1674-1056/ad3efa

Remote sensing image encryption algorithm based on novel hyperchaos and an elliptic curve cryptosystem

Jing-Xi Tian(田婧希), Song-Chang Jin(金松昌), Xiao-Qiang Zhang(张晓强), Shao-Wu Yang(杨绍武), and Dian-Xi Shi(史殿习)
Chin. Phys. B, 2024, 33 (**5**): 050502. DOI: 10.1088/1674-1056/ad20d9

An enhanced fingerprint template protection scheme based on four-dimensional superchaotic system and dynamic DNA coding

Baiqiang Hu(胡百强)[†], Jiahui Liu(刘嘉辉), and Zhe Liu(刘喆)

School of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150006, *China*

(Received 6 February 2025; revised manuscript received 3 April 2025; accepted manuscript online 9 April 2025)

With the rapid development of Internet of things technology, the efficiency of data transmission between devices has been significantly improved. However, the open network environment also poses serious security risks. This paper proposes an innovative fingerprint template protection scheme, which generates key streams through an improved four-dimensional superchaotic system (4CSCS), uses the space-filling property of Hilbert curves to achieve pixel scrambling, and introduces dynamic DNA encoding to improve encryption. Experimental results show that this scheme has a large key space 2^{528}, encrypts image information entropy of more than 7.9970, and shows excellent performance in defending against statistical attacks and differential attacks. Compared with existing methods, this scheme has significant advantages in terms of encryption performance and security, and provides a reliable protection mechanism for fingerprint authentication systems in the Internet of things environment.

Keywords: four-dimensional superchaotic system, fingerprint template protection, Zernike moments, image encryption

PACS: 05.45.–a, 05.45.Gg

DOI: 10.1088/1674-1056/adca9f **CSTR:** 32038.14.CPB.adca9f

1. Introduction

With the widespread adoption of Internet of things (IoT) technology, data transmission between personal devices and network nodes has become more efficient. However, the open network environment raises significant security concerns. In the medical field, attackers may compromise trusted communications by tampering with, forging, or injecting false patient information.[1] Many effective solutions have been proposed.[2–4] In intelligent transportation, the rapid advancement of autonomous driving has heightened the need for stringent security measures, particularly in identity authentication and data management, which are crucial for the development of driverless systems and telematics.[5] Traditional authentication methods, such as PIN codes and smart cards, are insufficient to meet the high-security demands of IoT-based access control systems.[6]

Fingerprints, as highly individualized and difficult-to-replicate biometric traits, are widely employed in biometric identification. Even identical twins do not possess identical fingerprints, reinforcing their irreplaceability in identity verification. Moreover, fingerprint feature information is exceptionally rich and complex, encompassing ridge flow patterns, ridge frequencies, spatial distributions of singularities such as cores and deltas, relationships between ridge directions and locations, minutiae distributions, variations in ridge counts between neighboring minutiae, and pore distributions.[7] With the rapid advancement of the industrial Internet of things (IIoT), traditional fingerprint recognition systems face significant challenges in template protection. To address these issues, Aseel Bedari *et al.* proposed a secure online fingerprint authentication system leveraging 5G networks. This system utilizes a user-specific key to transform raw fingerprint feature data through a cancelable fingerprint template design, generating an irreversible distorted version. This approach enhances data security and privacy while preserving the essential characteristics of the original fingerprint features.[8] Furthermore, to mitigate the risk of unauthorized access to fingerprint template data during the authentication process, Amit Kumar Trivedi *et al.* proposed an irreversible and cancelable fingerprint template design based on Delaunay triangulation and a user-specific key.[9] This approach effectively enhances the security, revocability, and versatility of fingerprint information while achieving outstanding recognition accuracy, as demonstrated in evaluations using the standard FVC2002 database. The rich and diverse biometric characteristics of fingerprints provide robust data support for the advancement of fingerprint recognition technology, further driving its widespread adoption across various domains.

The widespread adoption of fingerprint biometrics has significantly enhanced the security of identity authentication. However, their integration into IoT environments introduces critical privacy and security challenges. While complex biometric traits enable efficient individual identification in open IoT ecosystems, any compromise or loss of fingerprint data could result in irreversible identity exposure or cyber vulnerabilities.[10,11] Consequently, safeguarding fingerprint templates from theft or corruption and ensuring the se-

[†]Corresponding author. E-mail: baiqianghu@gmail.com

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

cure transmission of fingerprint data within IoT communication channels have become pressing challenges that require effective solutions.

Digital image encryption technologies have historically relied on a set of conventional algorithms, including RSA, AES, and DES, which have gained wide application across various domains.[12] However, these conventional approaches often prove inadequate when confronted with the challenges posed by increasingly intricate and voluminous image data. As data volumes escalate and encryption requirements become more intricate, the limitations of these traditional algorithms become more pronounced, prompting researchers to explore more efficient and secure alternatives. In recent years, image encryption technology based on chaotic systems has garnered significant attention due to its unique advantages and it has emerged as an effective solution to overcome the limitations of traditional algorithms.[13,14] Chaos systems possess characteristics such as high sensitivity to initial conditions, local randomness, and global invariance. These systems are capable of generating complex random keys, thereby providing a wider key space and significantly enhancing encryption security. Consequently, chaos image encryption technology demonstrates superior performance in processing large-scale image data when compared to traditional encryption algorithms. For instance, Wang *et al.* proposed an optical single-channel color image encryption scheme based on chaotic fingerprint phase masks and diffractive imaging.[15] This scheme utilizes a fingerprint to generate a random phase mask, which, in conjunction with the chaotic Lozi map and the SHA-256 algorithm, enhances the security of encryption. The efficacy of this scheme is further enhanced by the utilization of phase truncation technology and chaotic fingerprint phase masks with varying diffraction distances, which effectively converts color images into diffraction patterns resembling noise, thereby increasing the attack resistance and security of the encryption process. Ye *et al.* proposed an encryption algorithm for the visual significance of multiple images, which achieves cross-plane confusion through the construction of a three-dimensional coupled chaotic model.[16] Hu *et al.*[17] developed a chaotic-based partial Adama matrix to measure image blocks, and used block compressed sensing to complete the corresponding algorithm.

In addition, Rajeskannan Subraman *et al.* studied the application of a secondary hyperstable chaotic oscillator (QMO) in the encryption of biometric fingerprint images, revealing the complex dynamic characteristics of the QMO system,[18] including its high sensitivity to initial conditions and nonlocal attractor properties. In practical applications, QMO systems are used to encrypt fingerprint images, achieving high security and complexity through their dynamic characteristics. The efficacy of this encryption system has been demonstrated in a series of rigorous tests, indicating its significant potential for application in the domain of secure communications. In the context of the IoT, Esam *et al.* have proposed a physical layer encryption authentication scheme,[19] which is based on MP-FrFT-OFDM and dynamic chaotic biometrics. This scheme utilizes a multi-stage coupled chaotic modulation fractional sine map to generate dynamic keys, thereby significantly enhancing the security and attack resistance of IoT image transmission. Experimental results demonstrate the efficacy and reliability of this scheme, offering an innovative solution to the security challenges posed by IoT communications.

In addressing the encryption of multi-biometric images, Cong Ding *et al.* proposed a method that integrates fast Fourier transform (FFT) and hyperchaotic systems.[20] This approach involves transforming the image to the frequency domain, where encryption is achieved through matrix reconstruction and a non-repeating scrambling rule, in conjunction with the hyperchaotic Lorenz system key stream generated by the Logistic system. Subsequent to this, the image is reconstructed by inverse FFT, and the image is obfuscated and diffused by combining an additive mode with Galois field diffusion. This approach effectively addresses the challenges of inadequate security and low reconstruction accuracy that plague multi-biometric image encryption transmission. The incorporation of chaotic systems in image encryption has been demonstrated to effectively address the limitations encountered by conventional encryption algorithms in processing large-scale image data. Furthermore, it has been shown to offer novel research directions for enhancing the security and efficiency of encryption technology. Zhou *et al.* proposed an encryption algorithm based on a new bit-level expansion,[21] and the correlation of the encrypted image is almost 0. Guo *et al.* proposed an encryption algorithm that uses ghost imaging,[22] and the two-channel encryption method provides multiple layers of protection for the plaintext image.

Image encryption technology based on chaotic systems has emerged as a promising solution to address the limitations of traditional encryption algorithms in processing complex image data. However, with the increasing adoption of fingerprint recognition technology, the encryption of fingerprint images has become a more challenging task. Fingerprints, as an irreplaceable and crucial component of identity authentication, possess a wealth of intricate characteristics. This necessitates not only efficiency in the encryption process but also enhanced security and resistance to attacks. Previous research has explored chaos systems, DNA coding, or fractal curves as standalone methods. However, our innovative approach integrates these techniques to create synergistic security benefits, specifically targeting fingerprint biometric protection in IoT environments. A four-dimensional superchaotic system (4CSCS) provides an expanded key space, while Hilbert curves enable efficient pixel scrambling to achieve a global disorder effect. Guided by Zernike moments, dynamic DNA coding introduces content-adaptive diffusion that is highly sensitive to the characteristics of the fingerprint image.

The innovations in this paper are as follows:

(i) A fingerprint template protection scheme based on a 4CSCS has been proposed. This encryption method is based on an improved 4CSCS. The encryption scheme's optimization of the stability and complexity of the chaotic system provides a larger key space and higher security. At the same time, analysis of the system's dissipative and Lyapunov exponents further verifies its advantages in complex dynamic behavior.

(ii) The image encryption mechanism under consideration combines the Hilbert curve and dynamic DNA encoding. The spatial filling property of the Hilbert fractal curve is used to achieve efficient scrambling of fingerprint image pixels. This is then combined with dynamic DNA encoding to improve data obfuscation and anti-attack capabilities. The innovative design effectively enhances the complexity of the image scrambling and diffusion process.

(iii) A dynamic diffusion method incorporating the characteristics of Zernike moments has been developed. This method involves the extraction of the rotational and shape characteristics of the fingerprint image. Zernike moments are then introduced to dynamically adjust the DNA encoding matrix. The diffusion operation is optimized as a result, significantly improving the encryption system's resistance to differential attacks.

2. Related work

2.1. Four-dimensional coupled sine-Chen hyperchaotic system

The Chen chaotic system is a three-dimensional classical system with three nonlinear equations. It is highly sensitive to initial conditions and displays complex dynamic behavior. This system generates complex chaotic trajectories through nonlinear interactions. It is widely used in encryption to generate highly random key streams, enhancing security. Its mathematical expression is as follows:

$$\begin{cases} \dot{x} = a(y-x), \\ \dot{y} = bx - y - xz, \\ \dot{z} = -cz + xy, \end{cases} \tag{1}$$

where x, y, and z are the state variables of the system, and a, b, and c are the control parameters.

The present paper puts forth a novel four-dimensional hyperchaotic system based on Chen's chaos system, which has the mathematical form

$$\begin{cases} \dot{x} = -ax + by^2, \\ \dot{y} = ry - gz + xz^3 \sin(w), \\ \dot{z} = -dz + ecxy - a\sin(w), \\ \dot{w} = cx\sin(gz) + \sin(ey). \end{cases} \tag{2}$$

The variables x, y, z, and w represent the state variables of the system, while a, b, c, d, e, g, and r are the parameters that govern its chaotic behavior. After parameter tuning, when the system parameters are set to

$$a = 2,\ \ b = 7,\ \ \ c = 5,$$
$$d = 8,\ \ g = 11,\ \ r = 5,\ \ e = 2,$$

the system transitions into a superchaotic state, exhibiting enhanced chaotic behavior. Given the initial conditions

$$x_0 = 0.1,\ \ y_0 = 0.2,\ \ z_0 = 0.2,\ \ w_0 = 0.2,$$

the phase diagram of the superchaotic system is illustrated in Fig. 1.

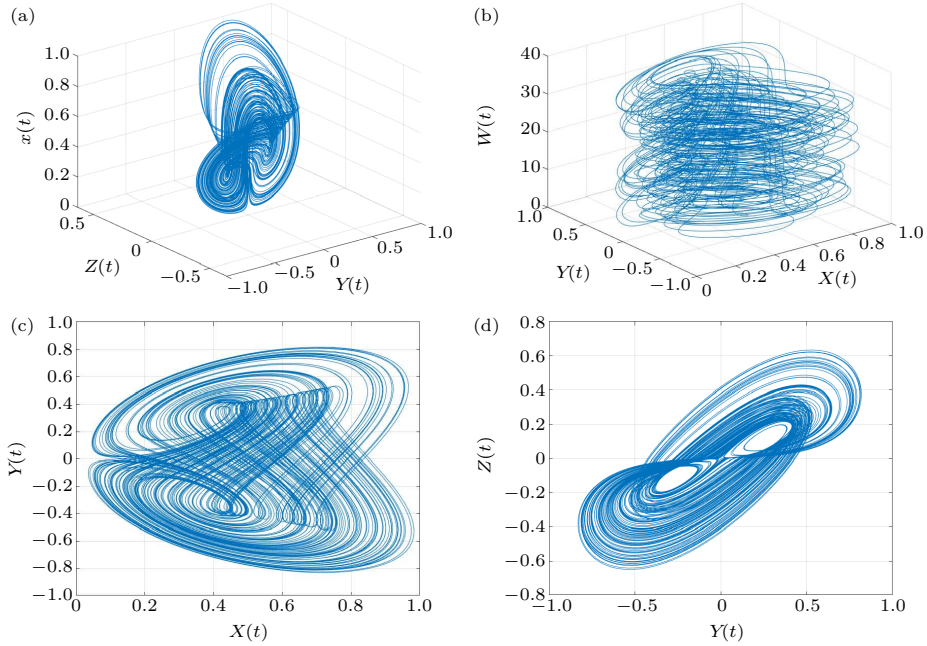


Fig. 1. The 4CSCS phase diagram analysis

2.1.1. Chaos system bifurcation diagram analysis

A bifurcation diagram can visually reveal the dynamic behavior of a system under different control parameters. In a dynamical system, when the control parameters change, the dynamic behavior of the system will change significantly. In order to effectively capture the evolution of this dynamic behavior, the Poinciana section method is usually used to project the complex trajectory of the system in a high-dimensional phase space onto a low-dimensional plane, thereby forming a mapping that varies with the parameter. This mapping is a two-dimensional image in the coordinate system, which is a bifurcation diagram.

As demonstrated in Fig. 2, the 4CSCS superchaotic system manifests stable chaotic behavior across a broader spectrum of parameters, exhibiting more uniformly dispersed points. This observation signifies that the 4CSCS superchaotic system possesses enhanced stability and complexity when the parameters undergo variation, thereby establishing a theoretical foundation for investigating its potential for practical applications.

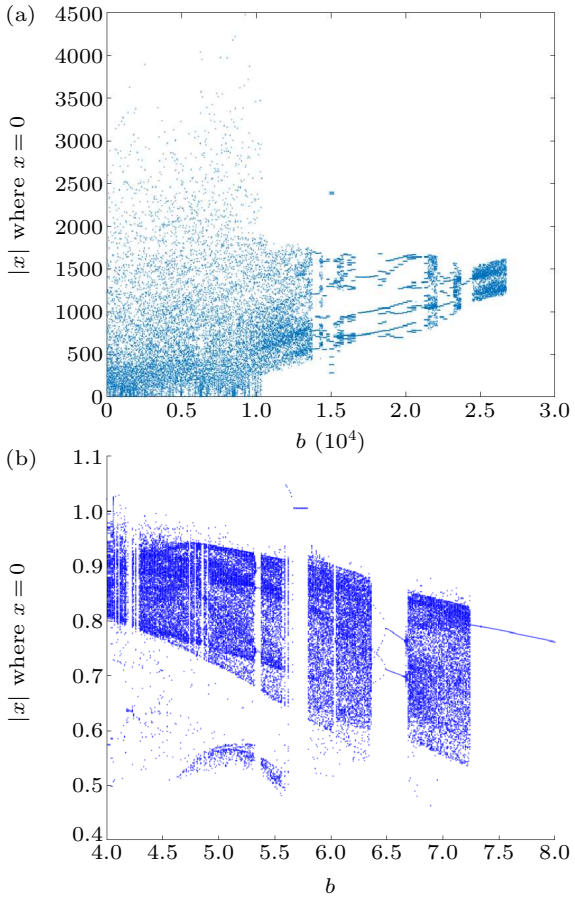


Fig. 2. (a) The bifurcation of the state variable x of the 4CSCS superchaotic system as a function of the parameter b over a wide range. The horizontal axis indicates the range of variation of the parameter b (0 to 30000), and the vertical axis shows the steady-state distribution of the variable x. (b) A detailed enlargement of the state variable of the system as the parameter b varies over a normalized range, which more clearly shows how the system evolves through periodic, chaotic, and superchaotic states as the parameter varies.

2.2. Dissipative property analysis

The total energy of a chaotic system gradually decreases over time, and the phase space also contracts during the evolution of the system. This property is known as the dissipativity of chaotic systems. Dissipativity reflects the intrinsic law of energy dissipation and convergence of the phase space in chaotic systems, and can be quantitatively described by analyzing the system's divergence and volume evolution.

The system's divergence is calculated as the trace of the Jacobian matrix

$$\operatorname{div} V = \operatorname{Tr}(J) = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} < 0. \tag{3}$$

For a dissipative system, the evolution of the phase space volume follows

$$\frac{\mathrm{d}V}{\mathrm{d}t} = V(0) \cdot \mathrm{e}^{\operatorname{div} V \cdot t}, \tag{4}$$

where t is time, $V(t)$ is the phase space volume at time t, and $V(0)$ is the initial phase space volume.

For the proposed 4CSCS system with parameters $a = 2$, $b = 7$, $c = 5$, $d = 8$, $g = 11$, $r = 5$, and $e = 2$, the divergence can be calculated as

$$\begin{aligned} \operatorname{div} V &= \frac{\partial(-ax + by^2)}{\partial x} + \frac{\partial(ry - gz + xz^3 \sin(w))}{\partial y} \\ &\quad + \frac{\partial(-dz + ecxy - a\sin(w))}{\partial z} \\ &\quad + \frac{\partial(cx\sin(gz) + \sin(ey))}{\partial w} \\ &= -a + r - d + 0 = -2 + 5 - 8 = -5 < 0. \end{aligned} \tag{5}$$

Since $\operatorname{div} V = -5 < 0$, the system exhibits dissipative behavior. This means that as time progresses indefinitely, the volume of the phase space gradually contracts according to

$$V(t) = V(0)\,\mathrm{e}^{-5t}, \tag{6}$$

where $V(0)$ represents the initial phase space volume.

The system will eventually converge to a finite region in phase space, known as an attractor. The exponential contraction rate of -5 determines the speed at which this attractor forms. This dissipative property ensures the system's long-term stability and demonstrates its suitability for practical applications where stable dynamic behavior is required.

2.2.1. Lyapunov exponent analysis

The Lyapunov exponent test shows that the system has entered a hyperchaotic state. Hyperchaos refers to the state of a chaotic system with two or more positive Lyapunov exponents. Compared to general chaos, hyperchaotic systems exhibit more complex dynamic characteristics, with higher randomness and unpredictability. General chaotic systems only have a positive Lyapunov index, while hyperchaotic systems have at least two positive Lyapunov indices. Chaos and hyperchaos can be effectively distinguished by the number and sign of the Lyapunov indices.

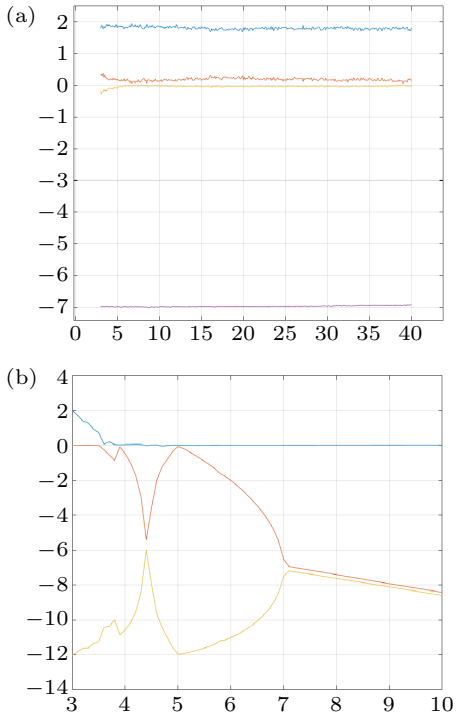


Fig. 3. (a) The Lyapunov exponent calculation result for the 4CSCS system in the parameter range 0 to 40, where the horizontal axis represents the value of the system parameter and the vertical axis represents the magnitude of the Lyapunov exponent. It can be seen that there are at least two stable positive Lyapunov exponents (the blue and orange curves are positive), indicating that the system always maintains a superchaotic state. (b) Lyapunov exponent test plot for the Chen chaotic system, showing its small chaotic range and low chaotic performance.

As shown in Fig. 3, the proposed 4CSCS system can maintain a stable superchaotic state for parameter values in the range $a \in [0,40]$. Compared with the classic Chen superchaotic system, this system exhibits stronger superchaotic characteristics and stability in the same parameter range.

As shown in Figs. 2 and 3, 4CSCS has stable chaotic behavior. Stable chaotic behavior means that when there is a small change in the parameter perturbation or initial value of a chaotic system, the system continues to maintain a large positive Lyapunov exponent, continuously exhibiting strong randomness and complex dynamic characteristics. At the same time, chaotic behavior is highly robust to parameter changes and can stably maintain superchaotic states over a wide range of parameters.

2.3. DNA encoding

Deoxyribonucleic acid (DNA) is the central genetic material of all living things and is responsible for passing on the characteristics of the parents to the offspring. The DNA molecule is characterized by its unique double helix structure, in which two strands are tightly wound around each other to form a stable storage system for genetic information. The backbone of each strand is composed of alternating deoxyribose and phosphate groups, and the specific coding of genetic information is determined by the bases linked to the deoxyribose molecule. The four bases, adenine (A), thymine (T), cytosine (C), and guanine (G), are paired by specific hydrogen bonds, with two hydrogen bonds forming between A and T, and three hydrogen bonds forming between C and G. This pairing maintains the stability of the double-stranded structure and ensures the efficient and accurate transmission of genetic information.

The order in which bases are arranged in a DNA molecule is analogous to the way in which binary numbers are encoded in computers. Each of the four bases (A, C, G, T) can be encoded as a binary value (e.g., 00, 01, 10, 11), allowing DNA to store and process vast amounts of information in a combined form. It is noteworthy that, theoretically, there exist 24 possible encoding methods; however, only eight of these methods comply with the Watson–Crick complementary pairing rule. The complete list of these encoding methods can be found in Table 1.

Table 1. Encoded rules table.

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

The application of DNA in the domain of computing has given rise to novel research directions. In 1944, Adleman of the University of Southern California in the United States successfully solved the Hamilton path problem, a problem that is NP-complete, using DNA computing for the first time through experimentation. This achievement became a milestone in the research of DNA computing. Subsequent research has expanded the boundaries of DNA computing, leading to the design of sophisticated computational rules, including XOR, addition, and subtraction. These rules have not only expanded the theoretical framework of DNA computing but also have provided significant support for its practical application in solving complex problems.

2.4. Hilbert fractal curve

In 1890, the Italian mathematician Peano proposed a Peano curve (space-filling curve) that can continuously traverse and completely cover two-dimensional space. Subsequently, in 1891, the German mathematician Hilbert simplified the Peano curve and proposed the now widely used Hilbert curve.

The Hilbert curve is a continuous fractal curve with good space-filling properties. Its mathematical expression is

$$H_n = \begin{cases} \dfrac{1}{2}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, & n = 1, \\ \dfrac{1}{2}\begin{bmatrix} H_{n-1}^{(\mathrm{TL})} & H_{n-1}^{(\mathrm{TR})} \\ H_{n-1}^{(\mathrm{BL})} & H_{n-1}^{(\mathrm{BR})} \end{bmatrix}, & n > 1. \end{cases} \tag{7}$$

The curve can establish an efficient mapping relationship between two-dimensional space and one-dimensional space by continuously subdividing space recursively and connecting subregions with specific rules for rotation and flipping. As the number of recursive steps increases, the complexity of the Hilbert curve gradually increases, and it eventually completely traverses and covers the entire two-dimensional space.

This property stems from the self-similarity of the Hilbert curve, meaning that by subdividing the space infinitely and approaching the target point, a curve that fills the entire plane is eventually generated. The space-filling process is governed by a specific rotation and flip rule, ensuring the continuity and space-filling nature of the curve. When this recursive process continues indefinitely, the resulting curve approaches the ideal Hilbert curve, traversing and covering the entire space with infinite length.

3. Proposed scheme

In the actual encryption process, image encryption can be summarized as user identity registration, key generation using 4CSCS, scrambling operation, and diffusion operation. The proposed scheme will be detailed below.

3.1. User identity registration

In the context of a transparent IoT environment, fingerprint biometric systems generally employ features such as minutiae points, ridge lines, and global structures for the purpose of identity verification. However, it should be noted that potential blurring and noise during the processing of fingerprint images can often result in the partial (or even single-level) features being compromised without leading to a complete recognition failure. To address this challenge, a key seed generator with robust security can be constructed by modifying specific pixels in the fingerprint image and utilizing a one-way function that is highly sensitive to initial values. This approach ensures data security by significantly expanding the key space, as different keys are generated in each transmission process, even when using the same plaintext image.

The basic algorithm modifies selected pixels in the fingerprint image and combines the user's initial ID with a system-provided timestamp to generate encryption key seeds. The specific process is as follows:

(i) For a fingerprint image P of size $M \times N$, its pixel set is defined as $\{p_1, p_2, \ldots, p_{m\times n}\}$. For any input fingerprint image, the user provides an initial ID, which undergoes an offset operation before composition:

$$\mathrm{ID}' = \mathrm{ID} + \mathrm{ID} \oplus T, \tag{8}$$

where T is the system-provided timestamp, and $\oplus$ represents the bitwise XOR operation, ensuring that different offset IDs are generated under different timestamps.

(ii) For each pixel p_i in the fingerprint image, expand ID' into binary format, forming a binary group $\{b_1, b_2, \ldots, b_8\}$.

(iii) The modification position is determined by the following equation:

$$\mathrm{Index} = (\mathrm{ID}' \oplus \mathrm{ID}) \bmod 8. \tag{9}$$

This index determines which bit of pixel p_i will be inverted.

Through pixel modification, a new image P' will be generated. These modifications depend not only on the initial ID but also on the timestamp and actual pixel values, ensuring a completely different key space for each transmission or usage. The key to this process lies in initial value sensitivity: even minor changes (such as small variations in timestamp or ID) will result in significant changes in the key.

3.2. Key generation

For an effective encryption algorithm, a large key space and sophisticated key utilization are fundamental to its security. In this paper, the key generation is highly correlated with the input image. The detailed steps are as follows:

(i) Process the modified image P' using SHA-256 hash algorithm to convert it into a 256-bit pseudorandom number. Group the generated pseudorandom number into 8-bit segments, forming an array $\{h_1, h_2, \ldots, h_{64}\}$.

(ii) Generate more uniform random values through the following equations:

$$\begin{cases} H_1 = h_1 \oplus h_2 \oplus h_3 \ldots h_{15} \oplus h_{16}, \\ H_2 = h_{17} \oplus h_{18} \oplus h_{19} \ldots h_{15} \oplus h_{32}, \\ H_3 = h_{33} \oplus h_{34} \oplus h_{35} \ldots h_{15} \oplus h_{48}, \\ H_4 = h_{49} \oplus h_{50} \oplus h_{51} \ldots h_{15} \oplus h_{64}. \end{cases} \tag{10}$$

Use the uniform random values $\{H_1, H_2, H_3, H_4\}$ as perturbation terms to disturb the initial values (x_0, y_0, z_0, w_0) of the chaotic system:

$$\begin{cases} x_0' = x_0 \cdot (1 + \varepsilon \cdot H_1), \\ y_0' = y_0 \cdot (1 + \varepsilon \cdot H_1), \\ z_0' = z_0 \cdot (1 + \varepsilon \cdot H_1), \\ w_0' = w_0 \cdot (1 + \varepsilon \cdot H_1), \end{cases} \tag{11}$$

where ε is a very small perturbation coefficient to ensure the disturbance is small but effective.

(iii) Generate random starting points for the Hilbert curve using values from the chaotic sequence:

$$\mathrm{Start_H}(i, j) = (\lfloor x_n \bmod 1 \rfloor \cdot M, \lfloor y_n \bmod 1 \rfloor \cdot N), \tag{12}$$

where $M \times N$ is the image size.

Generate a random matrix for diffusion operation using a chaotic sequence:

$$R_{ij} = \lfloor ((z_n \oplus w_n) \bmod 1) \cdot 255 \rfloor. \tag{13}$$

3.3. Image scrambling

Image scrambling aims to alter the positional relationships between pixels. This paper achieves index reordering through random Hilbert curve interference with DNA coding matrix. The scrambling process is detailed below:

(i) For an original image of size $M \times N$, its pixel array is $[p_1, p_2, \ldots p_{m\times n}]$. For any pixel p_i with maximum value 255, expand it into 8-bit binary code group $[b_0, b_1, \ldots, b_7]$.

(ii) For binary code group $[b_0, b_1, \ldots, b_7]$, split it into four 2-bit blocks $[B_0, B_1, B_2, B_3]$. For example, if a pixel value is $[234]_{10} = [11101010]_2$, it will be split into $[11, 10, 10, 10]$, with mapping rules

$$B_i = \begin{cases} \mathrm{A}, & \text{if } B_i = 00, \\ \mathrm{G}, & \text{if } B_i = 01, \\ \mathrm{C}, & \text{if } B_i = 10, \\ \mathrm{T}, & \text{if } B_i = 11. \end{cases} \tag{14}$$

(ii) For the original Hilbert curve path,

$$H_1 = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}. \tag{15}$$

Recurse according to

$$H_n = \begin{bmatrix} H_{n-1}^{(\mathrm{TL})} & H_{n-1}^{(\mathrm{TR})} \\ H_{n-1}^{(\mathrm{BL})} & H_{n-1}^{(\mathrm{BR})} \end{bmatrix}, \tag{16}$$

where $H_{n-1}^{(\mathrm{TL})}$ represents top-left recursive path, $H_{n-1}^{(\mathrm{TR})}$ represents top-right recursive path, $H_{n-1}^{(\mathrm{BL})}$ represents bottom-left recursive path, and $H_{n-1}^{(\mathrm{BR})}$ represents bottom-right recursive path.

(iv) Through the complete Hilbert curve path, for the DNA encoding of each pixel in the image (obtained from step (ii)), reorder according to the two-dimensional coordinate sequence provided by the Hilbert curve. Specifically, map each point in the curve to a bit-level one-dimensional index.

Algorithm 1: Hilbert curve-based image scrambling.

Require: Image P of size $M \times N$, Hilbert curve order n.
Ensure: Scrambled image S.
1: Initialize $H \leftarrow \mathrm{HilbertCurve}(n)$ {Generate 2D Hilbert curve coordinates}
2: Convert P into pixel vector V of size $M \times N$
3: **for** each pixel p_i in V **do**
4: Encode p_i into 8-bit binary representation $[b_0, b_1, \ldots, b_7]$
5: Split binary into four groups of 2 bits $[B_0, B_1, B_2, B_3]$
6: Map each B_i to DNA base according to rule: $\begin{cases} B_i = A, & \text{if } B_i = 00, \\ B_i = G, & \text{if } B_i = 01, \\ B_i = C, & \text{if } B_i = 10, \\ B_i = T, & \text{if } B_i = 11. \end{cases}$
7: **end for**
8: Reorder DNA-encoded pixels using Hilbert curve coordinates H
9: **for** each pixel's DNA sequence in reordered matrix **do**
10: Decode DNA bases back into binary blocks $[B_0, B_1, B_2, B_3]$
11: Merge binary blocks to form the 8-bit value of scrambled pixel
12: **end for**
13: Convert scrambled pixel vector back to 2D image S of size $M \times N$
14: **return** S

(v) Implement DNA decoding to obtain the scrambled image. If a pixel corresponds to $\{\mathrm{T}, \mathrm{C}, \mathrm{C}, \mathrm{C}\}$ in the encoding phase, convert it to binary blocks $[11, 10, 10, 10]$ according to the previous mapping relationship, and further synthesize into an 8-bit binary number to obtain the final pixel value.

The specific pseudocode is presented in Algorithm 1.

3.4. Image diffusion

Image diffusion aims to break the correlation between pixels by altering pixel values and their relationships. The process of image diffusion using dynamic DNA encoding is described below.

(i) For the input original image, calculate its Zernike moments using the following formula:

$$Z_{nm} = \sum_{x=1}^{M} \sum_{y=1}^{N} V(x,y) \cdot R_{nm}(r,\theta) \cdot \mathrm{e}^{-\mathrm{i}m\theta}, \tag{17}$$

where $R_{nm}(r,\theta)$ is the Zernike polynomial, $V(x,y)$ is the pixel value, (x,y) is the pixel coordinate, and r and θ are the radial and angular coordinates in polar coordinates.

Fingerprint data are susceptible to extraction devices and methods during collection. Therefore, to reduce complex calculations while extracting rotation and shape information as invariant moments, we select low-order terms from Zernike moments such as Z_{00}, Z_{10}, Z_{11}, etc., to calculate the offset using

$$\Delta = \alpha|Z_{10}| + \beta|Z_{11}| + \gamma|Z_{20}| + \delta|Z_{22}|, \tag{18}$$

where Z_{ij} represents the low-frequency components describing rotation and shape in Zernike moments, and α, β, γ, δ are weight coefficients indicating the influence of different Zernike moments on offset calculation.

(ii) Dynamically modify binary blocks based on the offset. For example, when the offset is 2, the mapping rule updates to

$$B_i = \begin{cases} \mathrm{G}, & \text{if } B_i = 00, \\ \mathrm{T}, & \text{if } B_i = 01, \\ \mathrm{A}, & \text{if } B_i = 10, \\ \mathrm{C}, & \text{if } B_i = 11. \end{cases} \tag{19}$$

(iii) Generate and update the key pool using 4CSCS key stream. For the dynamic DNA encoding matrix, determine its interference term based on its index position in the key pool. Perform XOR operation between each DNA code block B_i and the corresponding position $R(i,j)$ in the random number matrix to update DNA values:

$$B_i' = B_i \oplus R_{ij}. \tag{20}$$

Decode the XORed DNA bases back to binary blocks and synthesize into 8-bit binary numbers to obtain updated pixel values.

Algorithm 2: Dynamic DNA-based image diffusion.

Require: Image P of size $M \times N$, 4CSCS key stream K
Ensure: Diffused image D
Calculate Zernike moments Z_{nm} for P
Compute shift offset $\Delta = \alpha|Z_{10}| + \beta|Z_{11}| + \gamma|Z_{20}| + \delta|Z_{22}|$
for each pixel p_i in P **do**
    Convert p_i to 8-bit binary representation $[b_0, b_1, \ldots, b_7]$
    Split binary into four groups of 2 bits $[B_0, B_1, B_2, B_3]$
    Map each B_i to DNA base using Δ
end for 8: Generate DNA key matrix R using 4CSCS key stream K
for each DNA-encoded pixel block B_i **do**
    Update DNA block $B_i' = B_i \oplus R(i, j)$
    Decode DNA block B_i' back to binary and merge
end for
Convert updated binary values back to image D of size $M \times N$
return D

4. Experimental simulation

In order to verify the safety and efficacy of the algorithm proposed in this paper for protecting fingerprint templates, experimental simulation tests were conducted. The degree of filling and the complexity of fractal curves in space were used in combination with the improved 4CSCS chaotic system and the characteristics of the dynamic DNA encoding matrix to encrypt fingerprint templates. The results were analyzed from different perspectives and compared with other similar schemes. The test results demonstrate the superiority of our scheme.

4.1. Key security analysis

The key space is a pivotal metric for assessing the security of an encryption system because it encompasses all potential keys that could be utilized. The magnitude of the key space directly correlates to the complexity of brute force attacks on the encryption algorithm. An expansive key space necessitates a more protracted time span for searching for keys, thereby impeding the efficiency of brute force attacks and fortifying the security of the encryption algorithm. According to the seminal work on cryptographic security, the key space for systems with stringent requirements should not be less than 2^{100}. The encryption system designed in this paper achieves a key space of 2^{528}, which significantly exceeds the ideal value. This renders the system completely resistant to exhaustive attacks and ensures sufficient security.

4.2. Encryption security analysis

To demonstrate the encryption effect more intuitively, we selected four representative fingerprint images for experimental simulation, as shown in Figs. 4(a)–4(d). These fingerprint images are denoted as 01, 02, 03, and 04 in the subsequent analysis. Figures 4(e)–4(h) show the corresponding ciphertext images, which exhibit random noise characteristics with no discernible fingerprint information from the original images. The decrypted images are shown in Figs. 4(i)–4(l), which are identical to the original images, verifying the effectiveness of the encryption–decryption system. The results demonstrate that our proposed encryption scheme can effectively transform clear fingerprint images into noise-like patterns while maintaining perfect reconstruction capability during decryption. As observed from the experiment results, the ciphertext images appear as pure noise, completely concealing the visual features of the original fingerprint images. Meanwhile, the decrypted images perfectly match the original images, indicating zero information loss during the encryption–decryption process. This validates both the security and reversibility of our proposed encryption scheme.

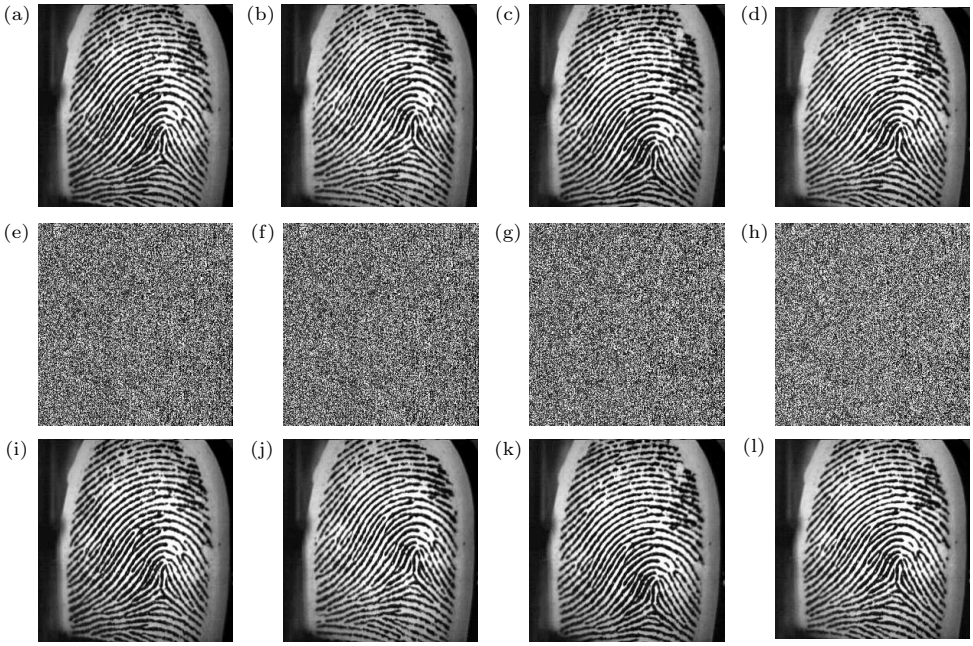


Fig. 4. Experimental simulation results.

4.2.1. Histogram analysis

A histogram is a statistical representation of the pixel distribution of an image, and a relatively flat histogram indicates that each pixel in the image appears with a similar frequency, suggesting that the image has a strong ability to hide statistical information; otherwise, it has a weak ability. Figure 5 shows the histogram of the ciphertext image after the test image is encrypted. As is evident in the figure, the histograms presented in this article are all relatively flat, exhibiting no significant accumulation of pixels at specific values. This observation indicates that the algorithm effectively prevents attacks from various statistical algorithms.

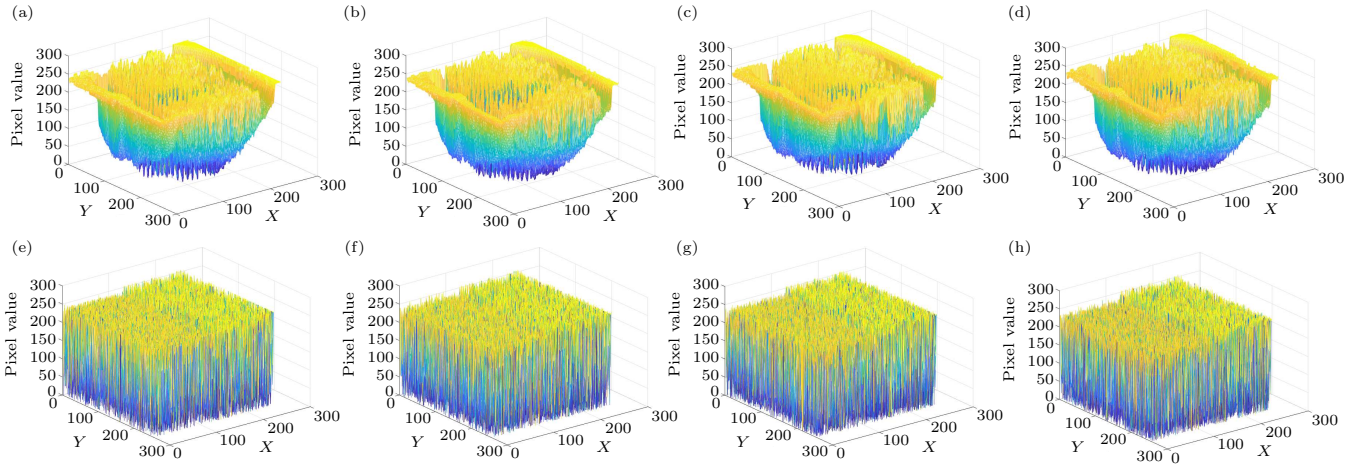


Fig. 5. (a)–(d) Plaintext image histogram. (e)–(h) Ciphertext image histogram.

4.2.2. Adjacency pixel correlation analysis

Correlation analysis is the process of calculating the correlation coefficient to quantify the linear relationship between variables. In this paper, we apply it to assess the security of a ciphertext image between two adjacent pixels. The test can be conducted in three directions: horizontal, vertical, and diagonal. The distribution of adjacent pixels in the plaintext image is depicted in Figs. 6(a)–6(d). It is evident from these figures that the coefficient distribution of the plaintext image is predominantly concentrated on the diagonal, indicating a substantial correlation between adjacent pixels. In contrast, the pixel correlation of the ciphertext image is thoroughly disrupted, with pixels randomly distributed throughout the image, as depicted in Figs. 6(e)–6(h). The algorithm demonstrates robust resistance to correlation attacks.

In this paper, 5000 pairs of pixels are randomly selected from both plaintext and ciphertext images for correlation analysis. The correlation coefficient formula is given by

$$C = \frac{\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i)(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i)}{\sqrt{\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i)^2 \sum_{i=1}^{N}(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i)^2}}, \quad (21)$$

where x and y represent the gray levels of two adjacent pixels in the image, and N is the total number of pixels in the image. By comparing the adjacent pixel correlation coefficients between our encryption algorithm and those reported in other literature, as shown in Table 2, it is evident that our algorithm achieves lower correlation coefficients. Therefore, the proposed encryption algorithm demonstrates higher security against statistical attacks.

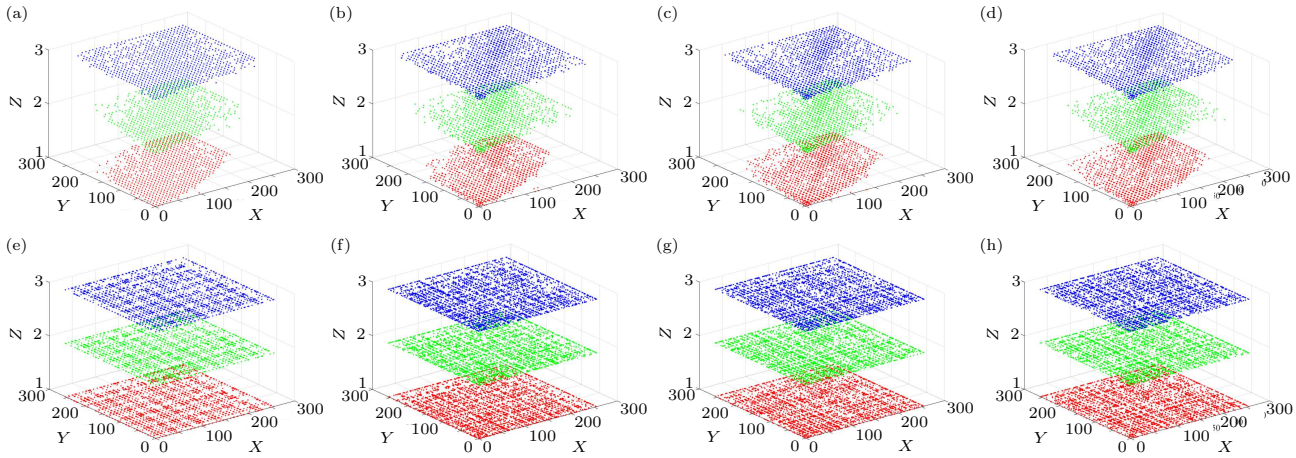


Fig. 6. (a)–(d) Plaintext image test. (e)–(h) Ciphertext image test.

Table 2. Correlation coefficients of test images in three directions.

Image	Original image			Encrypted image		
	horizontal	vertical	diagonal	horizontal	vertical	diagonal
01	0.8581	0.8806	0.6993	0.0360	0.0337	−0.0074
02	0.8642	0.8777	0.6910	0.0362	0.0133	0.0201
03	0.8490	0.8987	0.6833	0.0575	0.0055	0.0098
04	0.8548	0.8898	0.6914	0.0351	0.0192	−0.0043

4.2.3. Information entropy analysis

In the field of image encryption, information entropy is a crucial indicator for measuring the uncertainty and randomness of ciphertext images. The higher the information entropy, the more chaotic the ciphertext image. For plaintext images with a grayscale range of 0–255, the ideal information entropy value of their ciphertext images is 8, meaning that each grayscale value has an equal probability of occurrence. The closer the information entropy of a ciphertext image is to 8, the less visual information it contains, indicating better encryption performance.

The calculation formula for information entropy is given by

$$H(m) = -\sum_{i=0}^{2^{N-1}} p(m_i)\log_2 p(m_i), \tag{22}$$

where N represents the image grayscale level, and $p(m_i)$ represents the probability of pixel value occurrence. We calculated the information entropy of the test images, all achieving values above 7.9970. Table 3 compares our results with those reported in other literature, demonstrating the superior encryption performance of our proposed algorithm.

Table 3. Information entropy of encrypted images.

Test image	Information entropy (bits)
01	7.9972
02	7.9970
03	7.9969
04	7.9970
Ref. [23]	7.9934
Ref. [24]	7.9971
Ref. [25]	7.9973

4.2.4. Differential attack

A differential attack is one of the common attack methods in cryptography. To evaluate an encryption scheme's resistance to differential attacks, it is necessary to compare the ciphertext images of two plaintext images with minimal differences, analyzing whether the encryption algorithm is sensitive to plaintext changes. Specifically, attackers would first make slight modifications to the plaintext image, and then observe the differences between the corresponding ciphertext images to obtain the relationship between plaintext and ciphertext changes to crack the encryption algorithm.

To measure the image changes caused by modifying plaintext pixels, two indicators are introduced: number of pixel change rate (NPCR)) and unified average changing intensity (UACI)), defined as follows:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%, \tag{23}$$

$$\mathrm{UACI} = \frac{1}{M \times N}\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{24}$$

where C_1 and C_2 are two ciphertext images corresponding to two plaintext images that differ by only one bit. $D(i,j) = 1$ if $c_1(i,j) \neq c_2(i,j)$, otherwise $D(i,j) = 0$. According to calculation, the theoretical values for NPCR and UACI are 99.6093% and 33.4635%, respectively.

The test results using our proposed encryption scheme are very close to these ideal values. Table 4 presents our test results and compares them with other schemes, demonstrating the superior performance of our scheme in resisting differential attacks.

Table 4. NPCR and UACI test results.

Test image	NPCR (%)	UACI (%)
01	99.6017	34.4432
02	99.6292	34.3227
03	99.6094	35.1442
04	99.6170	34.7242
Ref. [26]	99.5400	33.5200
Ref. [27]	99.5800	33.1800
Ref. [28]	99.6700	33.5100

4.2.5. Peak signal-to-noise ratio test

Peak signal-to-noise ratio (PSNR) is a metric for evaluating image quality. For images with grayscale values ranging from 0 to 255, PSNR is calculated using the mean square error (MSE) between the plaintext image and its corresponding ciphertext image. The specific calculation methods are

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right), \tag{25}$$

$$\mathrm{MSE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j) - Y(i,j)]^2, \tag{26}$$

where $X(i,j)$ and $Y(i,j)$ represent the pixel values of the plaintext image and the decrypted image, respectively. The PSNR value can indirectly measure the degree of image encryption

confusion. Generally, a lower PSNR value indicates greater difference between the encrypted image and the original image, suggesting better encryption performance. The high MSE values (> 11000) confirm substantial differences between the original and encrypted images, which is desirable for secure encryption. These values are consistent with the low PSNR values (approximately 7.5 dB), indicating effective concealment of the original image information.

As shown in Table 5, compared with other encryption methods, our test results show significantly lower PSNR values, indicating poor quality of the ciphertext images with virtually no effective information retained.

Table 5. PSNR and MSE test results.

Test image	PSNR (dB)	MSE
01	7.4953	11575.7872
02	7.5204	11509.0659
03	7.3359	12008.6243
04	7.4274	11758.1326

5. Conclusion

This paper puts forth a pioneering fingerprint template protection scheme that integrates the 4CSCS, dynamic DNA coding, Hilbert fractal curves, and Zernike moment invariants. The scheme's innovative design generates key streams through an enhanced 4CSCS system, utilizes the space-filling property of Hilbert curves to achieve pixel scrambling, and incorporates dynamic DNA coding to bolster the encryption efficacy. The experimental results demonstrate that this scheme possesses a substantial key space (2^{528}), the entropy of the encrypted image information exceeds 7.9970, and it exhibits robust resistance to statistical and differential attacks. Additionally, it has a low PSNR, which effectively safeguards the security of fingerprint template data. A comparative analysis with existing methods reveals significant advantages in terms of encryption performance and security, thereby providing a reliable protection scheme for fingerprint authentication systems in the IoT environment.

References

[1] Sun W, Cai Z, Li Y, Liu F, Fang S and Wang G 2018 *Security and Communication Networks* **2018** 5978636

[2] Byeon H, Seno M E, Nimma D, Ramesh J V N, Zaidi A, AlGhamdi A, Keshta I, Soni M and Shabaz M 2025 *Image and Vision Computing* **154** 105420

[3] Gong L H and Luo H X 2023 *Optics & Laser Technology* **167** 109665

[4] Zou J Z, Chen M X and Gong L H 2025 *Neurocomputing* **614** 128834

[5] Zavvos E, Gerding E H, Yazdanpanah V, Maple C, Stein S, *et al.* 2021 *IEEE Transactions on Intelligent Transportation Systems* **23** 10126

[6] Marasco E, Albanese M, Patibandla V V R, Vurity A and Sriram S S 2023 *Security and Privacy* **6** e261

[7] Ren H, Sun L, Guo J and Han C 2022 *IEEE Transactions on Information Forensics and Security* **17** 2030

[8] Bedari A, Wang S and Yang W 2022 *Sensors* **22** 7609

[9] Trivedi A K, Thounaojam D M and Pal S 2020 *Computers & Security* **90** 101690

[10] Yang W, Wang S, Hu J, Zheng G and Valli C 2019 *Symmetry* **11** 141

[11] Natgunanathan I, Mehmood A, Xiang Y, Beliakov G and Yearwood J 2016 *IEEE Access* **4** 880

[12] Hellekalek P and Wegenkittl S 2003 *ACM Transactions on Modeling and Computer Simulation (TOMACS)* **13** 322

[13] Yan X, Hu Q and Teng L 2025 *Nonlinear Dyn.* **113** 1799

[14] Tao Y, Cui W, Wang S and Wang Y 2025 *PloS One* **20** e0310279

[15] Wang Y, Zhao Q, Zhang H, Li T, Xu W, Liu S and Su Y 2023 *Applied Optics* **62** 1009

[16] Ye G and Guo L 2024 *Nonlinear Dyn.* **112** 14593

[17] Hu L L, Chen M X, Wang M M and Zhou N R 2024 *Chaos, Solitons & Fractals* **188** 115521

[18] Subramanian R, Çiçek S, Akgul A, Adam G, Karthikeyan A and Rajagopal K 2024 *Complexity* **2024** 2005801

[19] Hagras E A, Aldosary S, Khaled H and Hassan T M 2023 *Sensors* **23** 7843

[20] Ding C, Xue R and Niu S 2023 *International Journal of Bifurcation and Chaos* **33** 2350084

[21] Zhou N R, Hu L L, Huang Z W, Wang M M and Luo G S 2024 *Expert Systems with Applications* **238** 122052

[22] Guo Z, Chen S H, Zhou L and Gong L H 2024 *Applied Mathematical Modelling* **131** 49

[23] Vijayakumar M and Ahilan A 2024 *Ain Shams Engineering Journal* **15** 102620

[24] Wang M, Fu X, Yan X and Teng L 2024 *Mathematics* **12** 638

[25] Zhu Y, Wang C, Sun J and Yu F 2023 *Mathematics* **11** 767

[26] Jiang D, Tsafack N, Boulila W, Ahmad J and Barba-Franco J 2024 *Expert Systems with Applications* **236** 121378

[27] Kumar S and Sharma D 2024 *Artificial Intelligence Review* **57** 87

[28] Alawida M 2023 *Journal of King Saud University-Computer and Information Sciences* **35** 101595