frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 09 September 2024
DOI 10.3389/fphy.2024.1469418



OPEN ACCESS

EDITED BY
Fei Yu,
Changsha University of Science and Technology, China

REVIEWED BY
Jun Mou,
Dalian Polytechnic University, China
Li Xiong,
Hexi University, China
Mengjiao Wang,
Xiangtan University, China

*CORRESPONDENCE
Tianxiu Lu,
lubeeltx@163.com

RECEIVED 23 July 2024
ACCEPTED 19 August 2024
PUBLISHED 09 September 2024

CITATION
Chen Y, Lu T, Chen C and Xiang Y (2024) A novel image encryption method based on improved two-dimensional logistic mapping and DNA computing.
*Front. Phys.* 12:1469418.
doi: 10.3389/fphy.2024.1469418



# A novel image encryption method based on improved two-dimensional logistic mapping and DNA computing

Yuanlin Chen[1], Tianxiu Lu[1]*, Caiwen Chen[1] and Yi Xiang[1,2]

[1]College of Mathematics and Statistics, Sichuan University of Science and Engineering, Zigong, China, [2]South Sichuan Applied Mathematics Research Center, Zigong, China

In the digital era, the significance of cryptographic algorithms has grown significantly within the realm of cybersecurity. This research presents an innovative approach to image encryption that eliminates the security limitations of the conventional one-dimensional logistic mapping. This approach relies on an enhanced two-dimensional logistic-fraction hybrid chaotic mapping (2D-LFHCM) and deoxyribonucleic acid (DNA) computing. Initially, the improved 2D-LFHCM is utilized to effectively scramble the image by incorporating chaotic sequences. Then, two novel algebraic DNA computing rules are introduced to enhance diffusion encryption. Experimental findings show that this approach offers superior security performance, even with renowned attacks.

KEYWORDS

**image encryption, chaotic system, DNA computing, logistic mapping, 2D-LFHCM**

## 1 Introduction

Chaos, which refers to complex and unpredictable behavior displayed by nonlinear dynamic systems, is a phenomenon characterized by the inherent unpredictability of deterministic nonlinear systems. The slightest change in the initial state can lead to unforeseen results. Chaos is not restricted to a particular domain but can be observed in various aspects of human society. The profound exploration of chaos has given rise to a natural problem: what are the potential applications of chaos? This query stands as a paramount concern not only in the present world but also in the future. As fundamental and applied sciences progress, chaos theory has evolved into a crucial focal point within the realm of nonlinear science, blossoming into a discipline that has thrived over the past few decades. Contemporary electronic engineering and image processing heavily draw upon chaos theory, utilizing its principles to yield numerous innovative and advantageous advancements in these fields.

The characteristics of chaos systems include nonlinearity, ergodicity, pseudo-random behavior, and a high sensitivity to initial conditions. As a result, chaos theory serves as a solid foundation for the development of excellent image encryption algorithms. However, it has been observed that employing a single chaotic system often leads to a limited range of possible encryption keys, thereby rendering the algorithm susceptible to attacks from malicious entities. Consequently, to ensure the creation of a robust and efficient image encryption algorithm, researchers frequently integrate chaotic systems with other disciplines, including the analysis of deoxyribonucleic acid (DNA) sequences [1–4], the

utilization of optical maps [5,6] or cellular automata (CA) [7,8], the application of compressed sensing [9,10], and chaotic circuits [11–17].

Therefore, chaos theory holds immense potential for research and practical significance in the domain of image encryption. Ever since R. Matthews [18] introduced a broader logistic map and relied on it in the data encryption domain, a new era of chaotic systems generating pseudo-random numbers is beginning. Thus, fresh impetus is provided to cryptography. Consequently, chaos and cryptography became intertwined. Subsequently, Alvarez [19] formulated the fundamental requisites and rules of chaotic cryptosystems, gaining recognition from experts in the field of cryptography. Since then, there has been a robust development regarding chaotic digital image encryption. In 2012, Wang [20] invented a novel technique employing a traditional logistic map for the encryption of color images. Nevertheless, the key space induced by one-dimensional chaos is limited, and the algorithm's handling of chaotic sequences is not sufficient, resulting in unsatisfactory robustness of the algorithm. In an attempt to address this issue, Wang [21] put the latest method for creating high-dimensional digital chaotic systems, but the drawback lies in the complexity of the system structure and the inefficiency of the algorithms. More recently, Huang [22] proposed a fine-tuned cubic color image encryption scheme that operates jointly by chaos and hyperchaos. Its core idea is based on an improved logistic-fraction hybrid chaotic mapping (LFHCM) proposed to address the limitations of one-dimensional chaotic mapping and expand the key space. This mapping is then linked with a four-dimensional hyperchaotic system to generate the key stream, which is used to rotate and shift the rows and columns of each component in the red (R), green (G), and blue (B) channels of the color image. Wang [23] attempted to accomplish global scrambling by creating a chaotic sequence using the Lorenz system for binary and Gray code translation. Remarkably, this algorithm exhibits a favorable encryption effect on grayscale images. Building upon these advancements, Gao [24] introduced a multi-image encryption technique founded on single-channel scrambling, diffusion, and chaotic systems. Performance investigation validates that this technique demonstrates exceptional capabilities in ensuring security and achieving efficient encryption speed. Furthermore, in his study [25], Alexan proposes a method for encrypting color images. This approach effectively combines KAA mapping with various chaotic mappings in a synergistic manner. Notably, this approach maximizes the utilization of Shannon's security idea and encrypts the image through bit obfuscation and diffusion.

However, amidst a plethora of algorithms, our specific interest lies in encryption methods rooted in chaotic dynamics and deoxyribonucleic acid (DNA) sequences. The encryption performance of this algorithm, proposed by Chai [26], is not only exceptional but also demonstrates the ability to withstand a range of conventional attacks. In 2018, an image encryption algorithm was introduced by Wu [27], which employed a combination of DNA coding and Henon-Sine mapping. To increase the complexity of the encryption process and strengthen the algorithm's security, XOR operations and DNA coding were added to the diffusion process. In 2020, Patel [28] introduced a novel algorithm for encrypting images, which combined DNA coding and a three-dimensional chaotic mapping technique. In addition to utilizing the idea of eight complementary encodings for picture encryption, this approach employed a chaotic sequence to jumble the image. Both of these algorithms are applicable for encrypting grayscale and color images. Liu [29] then applies an improved Arnold transformation to scramble the three components and uses the DNA sequence generated through the chaotic sequence to conduct diffusion encryption of the color image. Hua [30] presented an innovative dynamic image encryption technique that enhanced the security of image data by utilizing quantum walk and chaos-induced DNA. Inspired by them, a plagiarism detection method is presented utilizing an improved two-dimensional logistic-fraction hybrid chaotic mapping (2D-LFHCM) and DNA computation. This method incorporates DNA chaotic diffusion and scrambling techniques.

The organization of this paper is outlined below. Section 2 delves into the 2D-LFHCM and analyzes its chaotic characteristics. The fundamental principles of encryption and decoding are covered in Section 3. Section 4 presents the devised method for key creation as well as the encryption and decryption methods for DNA images. Section 5 elucidates the numerical simulation findings of the proposed cryptosystem, supplemented by a comprehensive exploration of its security analysis. Ultimately, Section 6 furnishes a thorough recapitulation of the study's content and outlines potential directions for future research.

The main contributions of this paper are highlighted below:

(i) Development of an enhanced two-dimensional logistic-fraction hybrid chaotic mapping (2D-LFHCM) for image encryption.
(ii) Design and implementation of novel deoxyribonucleic acid (DNA) computing techniques in the proposed encryption method, including right shift addition, right shift subtraction, right shift XOR, and other DNA computing methods.
(iii) A comprehensive performance analysis of the encryption algorithm was conducted, including aspects such as encryption speed, key space, histograms, information entropy, and correlation coefficients.

# 2 An improved 2D-LFHCM

## 2.1 The definition of 2D-LFHCM

Parabolic mapping is a generic term used to describe a kind of chaotic maps. The classical insect population model (or logistic mapping, shortly, LM) is represented as Equation 1.

$$x_{n+1} = r x_n (1 - x_n), \tag{1}$$

where $r \in (0, 4)$, with initial value $x_0 \in (0, 1)$. Another classic 2D-LMM (two-dimensional logistic mixing mapping) [31], is a discrete chaotic map in two dimensions derived from the traditional logistic map. The difference equation's mathematical model is represented as Equation 2.

$$\begin{cases} x_{n+1} = t(3y_n + 1)x_n(1 - x_n); \\ y_{n+1} = t(3x_{n+1} + 1)y_n(1 - y_n), \end{cases} \tag{2}$$

where $t$ is a control parameter, $x_n$ and $y_n$ denote the state variables within the iterative process of the difference equation. Compared with the traditional 2D-LMM, the newly proposed 2D-LM (two-dimensional logistic mapping) by Ye [32] is a two-dimensional chaotic mapping with a simpler equation structure. Its model is described below.

$$\begin{cases} x_{n+1} = ux_n(1 - x_n); \\ y_{n+1} = vx_n(1 - y_n). \end{cases} \tag{3}$$

In Equation 3, $u$ and $v$ are the control parameters of the proposed 2D-LM, $x_n$ and $y_n$ are the state variables, and $n$ is the number of iteration steps. When $u = 3.99$ and $v = 1.4$, starting from $(0.1, 0.1)$, the 2D-LM demonstrates chaotic behavior.

Based on the original one-dimensional logistic map, the LFHCM (logistic-fraction hybrid chaotic mapping) derived from the logistic map and fraction map is proposed by Huang [22]. The fraction mapping is proposed by Lu et al. [33] to address the practical needs of multi-objective optimization and multi-model issues. The definition equation of fraction mapping is Equation 4.

$$z_{n+1} = F(c, z_n) = \frac{1}{z_n^2 + 0.1} - cz_n, \tag{4}$$

where $c \in (0, 1]$ is a control parameter, and the output range of all chaotic sequences $z_n \in [-10.0025, 10.0025]$. The definition equation of LFHCM constructed by combining logistic mapping and fraction mapping is Equation 5.

$$x_{n+1} = L(a, x_n) = ax_n(1 - x_n)^2 \times \frac{1}{x_n^2 + 1}, \tag{5}$$

where $a \in (0, 11.5]$ is a control parameter, and the sequence output value $x_n \in [0, 1.56]$.

Thanks to their excellent chaotic performance, LM, 2D-LM, 2D-LMM, and LFHCM are often used as pseudo-random signal generators in engineering fields such as cryptography and dynamics. However, LFHCM has not yet been extended to two-dimensional. The traditional logistic-fraction mapping serves as the fundamental basis for the 2D-LFHCM described in this study, and its difference equation is

$$\begin{cases} x_{n+1} = \lambda x_n(1 - x_n)^2 \times \frac{1}{x_n^2 + 1}; \\ y_{n+1} = \mu x_n(1 - y_n)^2 \times \frac{1}{x_n^2 + 1}, \end{cases} \tag{6}$$

where, $\lambda$ and $\mu$ serve as the control parameters, and $x_n$ and $y_n$ stand for the state variables. When $u = 3.99$ and $v = 1.4$, starting from the initial point $(0.1, 0.1)$, chaotic behavior is observed in the 2D-LFHCM.

## 2.2 Analysis and comparison of chaotic properties of 2D-LFHCM

In the preceding section, different classical maps were defined, and enhancements were made to the two-dimensional map, referred to as 2D-LFHCM. This section assesses and compares the chaotic properties of the following chaotic maps: 2D-LM, 2D-LFHCM, 2D-LMM, and LFHCM. The study is done from the perspectives of the phase trajectory diagrams, Lyapunov exponents, bifurcation diagrams, and chaotic analysis of the iterative sequences. It will be shown that the improved two-dimensional chaotic map 2D-LFHCM has better chaotic characteristics.

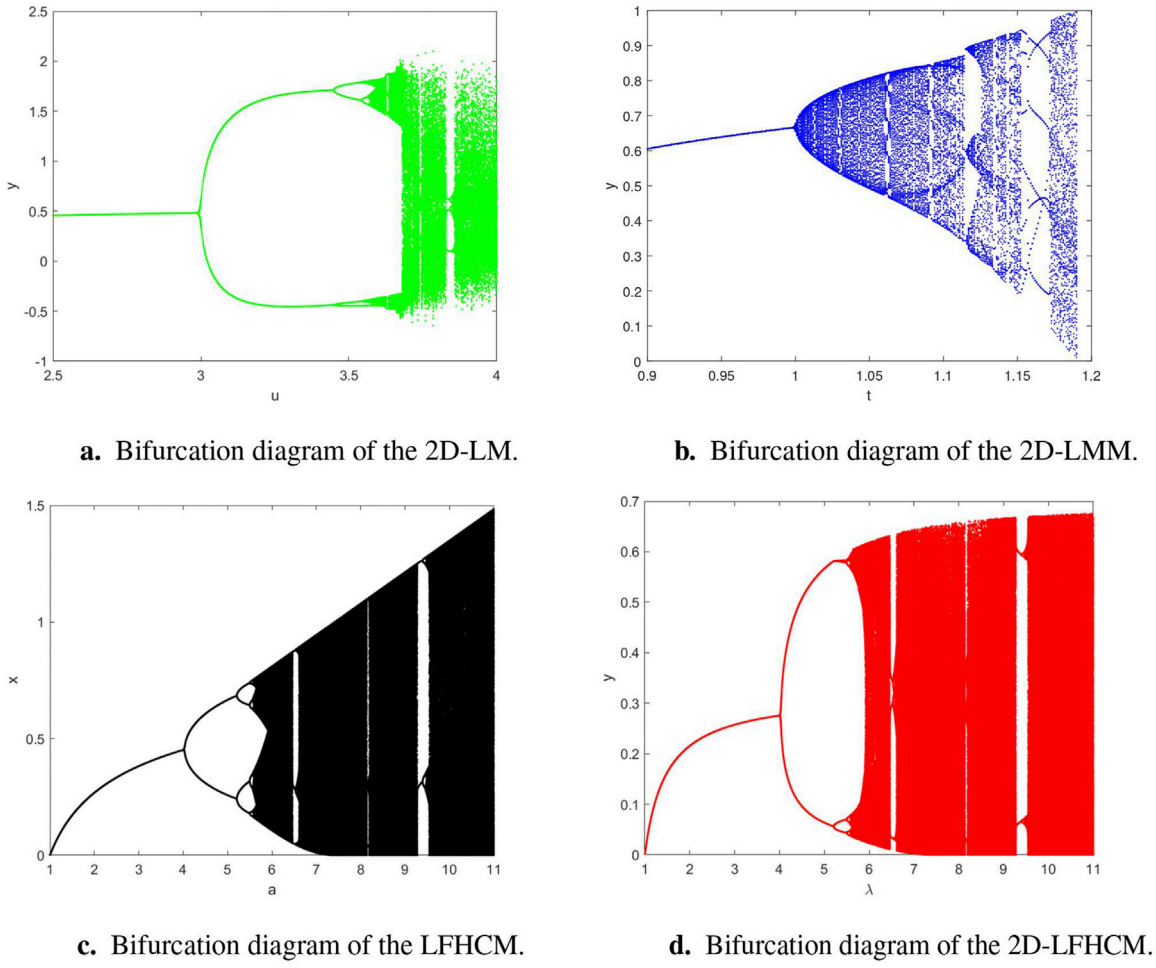
## 2.3 Bifurcation diagrams

Assume that the initial conditions of the following four mappings are (0.1, 0.1), and their control parameters are $a$, $t$, $u$, and $\lambda$, respectively. Then, their bifurcation diagrams are shown in Figure 1. The bifurcation diagram of 2D-LM is shown in Figure 1A. When $u = 2.99$, the system transitions from a period-1 to a period-2 state. At $u = 3.464$, the system enters a period-4 orbit. When $u = 3.554$, the system enters a period-8 orbit and then transitions into a chaotic orbit. The maximum amplitude of 2D-LM is 2.491. The bifurcation diagram for the 2D-LMM is presented in Figure 1B. As the control parameter $t$ increases from 0.9 to 1.19, the trajectory of point $y$ of 2D-LMM undergoes a transition, shifting from a periodic orbit to a chaotic orbit, and the maximum amplitude is 0.995. The bifurcation diagram for LFHCM is displayed in Figure 1C. When $a = 5.9$, LFHCM enters a chaotic state. The 2D-LFHCM model proposed in this paper, as shown in Figure 1D, when the control parameters $\lambda = 5.206$ and $\lambda = 5.509$, the tangent bifurcation of the mapping occurs, and the obvious period-2 window and period-4 window are formed, respectively. Then the mapping forms the period-8 window, and then enters the chaotic state. Changing the parameter $\lambda$, it can be observed that the mapping has rich nonlinear dynamic phenomena such as period-doubling bifurcation, tangent bifurcation, periodic window, chaos, and so on. In addition, it can be seen that whether 2D-LMM or 2D-LM, the length of the chaotic interval is less than 1, and there are some glaringly visible blank windows even inside the narrow chaotic region. It is evident from a comparison of the newly proposed 2D-LFHCM with the above chaotic maps that it has a broader chaotic region, a longer chaotic interval, and fewer blank windows. The comparison of their chaotic intervals is shown in Table 1. Where, the chaotic region area of 2D-LM is regarded as unit 1.

## 2.4 Lyapunov exponents spectrum

In general, the Lyapunov exponent is a very important statistical feature. It characterizes the stability of dynamic systems and can be used to judge whether the system presents chaotic behavior and the degree of chaos. The Lyapunov exponent describes the exponential growth rate of the system under small changes in initial conditions, which reflects the sensitivity and predictability of the system. To rephrase, determining the Lyapunov exponent spectrum can aid in our comprehension of the system's dynamic behavior, as well as in determining whether or not chaos exists inside the system and to what extent. For a discrete chaotic mapping $L(x)$ of dimension $m$ (see Equation 7),

$$L(x): \begin{cases} x_{n+1}^1 = L_1(x_n^1, \ldots x_n^m); \\ x_{n+1}^2 = L_2(x_n^1, \ldots x_n^m); \\ \vdots \\ x_{n+1}^m = L_m(x_n^1, \ldots x_n^m), \end{cases} \tag{7}$$




**a.** Bifurcation diagram of the 2D-LM. **b.** Bifurcation diagram of the 2D-LMM.

**c.** Bifurcation diagram of the LFHCM. **d.** Bifurcation diagram of the 2D-LFHCM.

FIGURE 1
The bifurcation diagrams of 2D-LM **(A)**, 2D-LMM **(B)**, LFHCM **(C)**, and 2D-LFHCM **(D)**.

**TABLE 1** Comparison of chaotic regions of four chaotic maps.

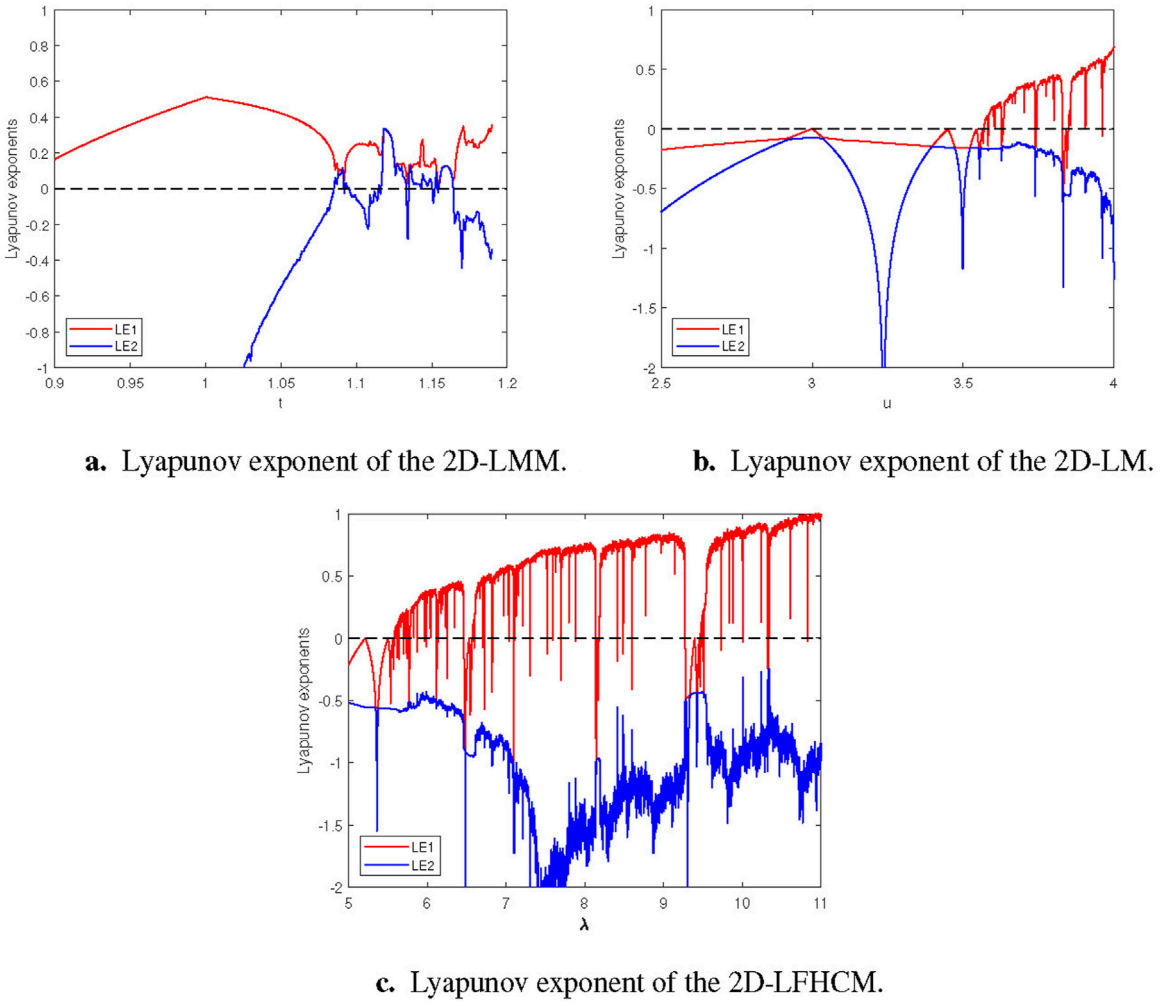
| Chaotic map | Chaotic interval | Chaotic region area ratio |
|---|---|---|
| 2D-LM | $[3.567, 3.738] \cup [3.749, 3.828] \cup [3.848, 4]$ | 1 |
| 2D-LMM | $[0.999, 1.089] \cup [1.089, 1.113] \cup [1.128, 1.152] \cup [1.172, 1.189]$ | 1.374 |
| LFHCM | $[5.569, 6.464] \cup [6.577, 8.123] \cup [8.214, 9.274] \cup [9.461, 11]$ | 1.921 |
| 2D-LFHCM | $[5.583, 6.454] \cup [6.565, 9.274] \cup [9.481, 11]$ | 2.441 |

the Lyapunov exponent can be expressed as Equation 8.

$$LE_j = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln|\lambda_j|, \tag{8}$$

where $j = 1, 2, \ldots, m$, and $\lambda_1, \lambda_2, \ldots, \lambda_m$ are the $m$ eigenvalues of the Jacobian matrix of $L(x)$ at the $n$-th iteration.

Two Lyapunov exponents, $LE_1$ and $LE_2$, correspond to a two-dimensional discrete chaos mapping. In terms of the Lyapunov exponent, a system will only exhibit chaotic properties when it has a positive number of states. Furthermore, the system performs more chaotically the higher the Lyapunov exponent. Selecting the control parameters $\nu = \mu = 4$, the initial point is (0.1, 0.1), Figure 2 shows the Lyapunov exponents spectrum of three two-dimensional chaotic maps. The largest Lyapunov exponent ($LE_1$) is shown by the red line, while the second Lyapunov exponent ($LE_2$) is represented by the blue line. The comparative analysis reveals that the average Lyapunov exponent of the 2D-LFHCM introduced in this study surpasses that of both the 2D-LMM and 2D-LM. Consequently, the 2D-LFHCM exhibits superior chaotic performance. Moreover, the Lyapunov exponent values within the parameter range of $\lambda$ for the 2D-LFHCM are predominantly positive, confirming its heightened suitability for image encryption.




**a.** Lyapunov exponent of the 2D-LMM. **b.** Lyapunov exponent of the 2D-LM.

**c.** Lyapunov exponent of the 2D-LFHCM.

FIGURE 2
Lyapunov exponents spectrum of 2d-LMM **(A)**, 2D-LM **(B)**, 2D-LFHCM **(C)**.

## 2.5 Iteration sequence and phase diagram

For the 2D-LFHCM, with fixed parameters $\lambda = 4.5$, $\mu = 1.4$ and $\lambda = 6$, $\mu = 1.4$, the chaotic sequence is obtained after 300 iterations, as shown in Figure 3. The black curve $S_1$ represents the trajectory starting from the initial value (0.1, 0.1). The green curve $S_2$ represents the trajectory starting from the initial value $(0.1, -0.1)$. To make the image clear, the curve of $S_1$ is intentionally translated upward. From Figure 3B, it becomes apparent that upon reaching a specific iteration count, the two running paths become indistinguishable. Indeed, this phenomenon arises when certain conditions are met by the initial value.

Based on diverse parameters, maps in the specified interval can generate chaotic effects, resulting in a chaotic phase diagram. Figure 4 illustrates the chaotic phase portraits of 2D-LMM, 2D-LM, and 2D-LFHCM under specific conditions ($t = 1.19$, $u = 3.99$, $v = 1.4$, and $\lambda = 9$, $\mu = 1.4$, respectively).

By analyzing the numerical simulation results presented in Figure 4, it becomes evident that the 2D-LFHCM proposed in this research exhibits a larger chaotic range in the phase plane compared to 2D-LMM and 2D-LM. This observation indicates that the 2D-LFHCM can generate a more diverse range of chaotic pseudo-random outcomes, thereby enhancing ergodicity. This improvement is valuable for potential applications, including signal generation and the utilization of chaotic systems in image encryption.

# 3 The basic principles of encryption and decryption

In the field of biology, deoxyribonucleic acid (DNA) stands as a fundamental biomolecule present within the cells of all organisms, serving as the genetic material for the majority of living entities. It is gratifying that DNA also plays an indispensable role in cryptography [34]. If the nucleotide bases in DNA information are matched to the binary digits 00, 01, 10, and 11, there are a total of 8 DNA coding rules [35], each corresponding to its own rules for addition, subtraction, and XOR operations. DNA primarily achieves the genetic code through the arbitrary combination of four bases: adenine (A), cytosine (C), guanine (G), and thymine (T), where A and T are complementary, C and G are complementary. The binary numerals 0 and 1, which complement each other, also serve a

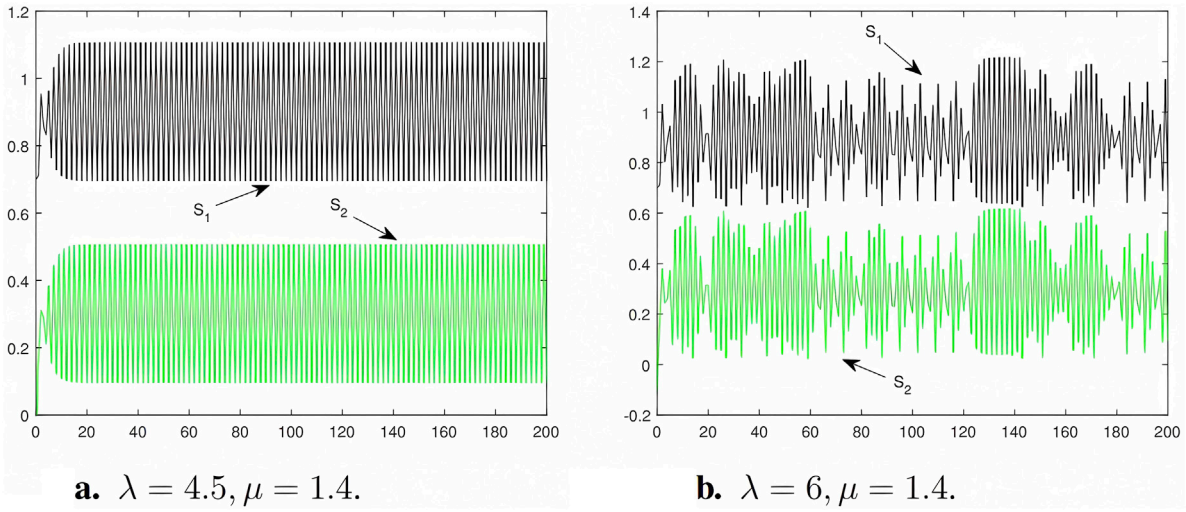



FIGURE 3
Two iterative sequences of the 2D-LFHCM for $\mu = 1.4$ ($\lambda = 4.5$ **(A)** and $\lambda = 6$ **(B)**, respectively).

purpose in computers to store information. By leveraging these characteristics, when implementing DNA's quaternary encoding with four bases, there can be a total of eight pairing rules. The coding table is shown in Table 2.

In a computer, the quaternary system is a digital system based on the number 4. The four numbers 0, 1, 2, 3, and A, T, C, G one-to-one mapping. If four bases in DNA are used for four-image coding, there are a total of eight rules that can be paired with each other. The coding table is shown in Table 2. Following the rules provided in Table 2, a 4-digit quaternary number can be directly represented by a 4-length DNA sequence. As an example, the quaternary number "1320" can be used to represent the decimal 120 Gy value. Since the numbers 0, 1, 2, and 3 are mapped one by one with A, T, C, and G, they are eventually converted into TGCA.

The cryptosystem in modern cryptography can be succinctly denoted as a five-tuple $P, C, K$, $Enc, Dec$, where $P$ denotes the plaintext sequence, $C$ represents the ciphertext sequence, $K$ embodies the key system, $Enc$ signifies the encryption algorithm, and $Dec$ denotes the decryption algorithm. The core idea of modern cryptography involves encrypting a sequence of plaintext using a designated encryption algorithm. Subsequently, the encrypted file can be decrypted by the recipient, using a specific decryption key, to retrieve the original plaintext sequence. Table 3 displays the DNA operation rules, when A = 0, C = 1, G = 2, and T = 3, of addition "+," subtraction "−", exclusive or "xor," right shift '→', and left shift "←".

Mathematically, the well-known technique of the right cyclic shift involves rearranging a collection of data sequences. The specific procedure entails relocating the final number to the initial position and shifting all the remaining elements to the right, aligning them with their corresponding positions. On the other hand, the left circulation shift is similar. Throughout the shifting process, the cyclicity is maintained, ensuring that the removed element reappears at the opposite end of the sequence.

Let $R((s_0, s_1, \ldots, s_{n-1}), k)$ represents the $k$-th right cyclic shift, that is, the right cyclic shift $k$ times. Then,

$$R((s_0, s_1, \ldots, s_{n-1}), k) = \left(s_{\mathrm{mod}(0-k,n)}, s_{\mathrm{mod}(0-k,n)+1} \ldots, s_{\mathrm{mod}(n-1-k,n)}\right).$$

Correspondingly, $L((s_0, s_1, \ldots, s_{n-1}), k)$ represents the $k$th left cyclic shift. Then,

$$L((s_0, s_1, \ldots, s_{n-1}), k) = \left(s_{\mathrm{mod}(0+k,n)}, s_{\mathrm{mod}(0-k,n)+1} \ldots, s_{\mathrm{mod}(n-1+k,n)}\right).$$

As per the operational guidelines provided in Table 3, DNA left shift and DNA right shift algebraic operators, grounded in DNA sequences, facilitate the definition of six DNA algebraic operations. These include DNA right (left) shift addition, DNA right (left) shift subtraction, and DNA right (left) shift XOR.

As an illustration, for the DNA operation before the shift and the DNA right shift XOR, one can get

$$\begin{aligned}
&((A,C,G,T),(A)_4) = ((A,C,G,T),0) \rightarrow (A,C,G,T) \rightarrow (A,A,A,A),\\
&((A,C,G,T),(C)_4) = ((A,C,G,T),1) \rightarrow (T,A,C,G) \rightarrow (T,C,T,C),\\
&((A,C,G,T),(G)_4) = ((A,C,G,T),2) \rightarrow (G,T,A,C) \rightarrow (G,G,G,G),\\
&((A,C,G,T),(T)_4) = ((A,C,G,T),3) \rightarrow (C,G,T,A) \rightarrow (C,T,C,T).
\end{aligned}$$

The DNA right shift addition $f_{r+}$ is expressed as

$$\begin{aligned}
f_{r+} &= \begin{bmatrix} R_+((A,C,G,T),(A)_4) \\ R_+((A,C,G,T),(C)_4) \\ R_+((A,C,G,T),(G)_4) \\ R_+((A,C,G,T),(T)_4) \end{bmatrix}\\
&= \begin{bmatrix} R_+((A,C,G,T),0) \\ R_+((A,C,G,T),1) \\ R_+((A,C,G,T),2) \\ R_+((A,C,G,T),3) \end{bmatrix} \rightarrow \begin{bmatrix} A & A & C & C \\ T & C & T & A \\ G & G & G & G \\ C & T & A & T \end{bmatrix}
\end{aligned}$$

The DNA right shift subtraction $f_{r-}$ is expressed as

$$\begin{aligned}
f_{r-} &= \begin{bmatrix} R_-((A,C,G,T),(A)_4) \\ R_-((A,C,G,T),(C)_4) \\ R_-((A,C,G,T),(G)_4) \\ R_-((A,C,G,T),(T)_4) \end{bmatrix}\\
&= \begin{bmatrix} R_-((A,C,G,T),0) \\ R_-((A,C,G,T),1) \\ R_-((A,C,G,T),2) \\ R_-((A,C,G,T),3) \end{bmatrix} \rightarrow \begin{bmatrix} A & A & A & A \\ T & C & G & C \\ G & G & T & T \\ C & T & C & G \end{bmatrix}
\end{aligned}$$

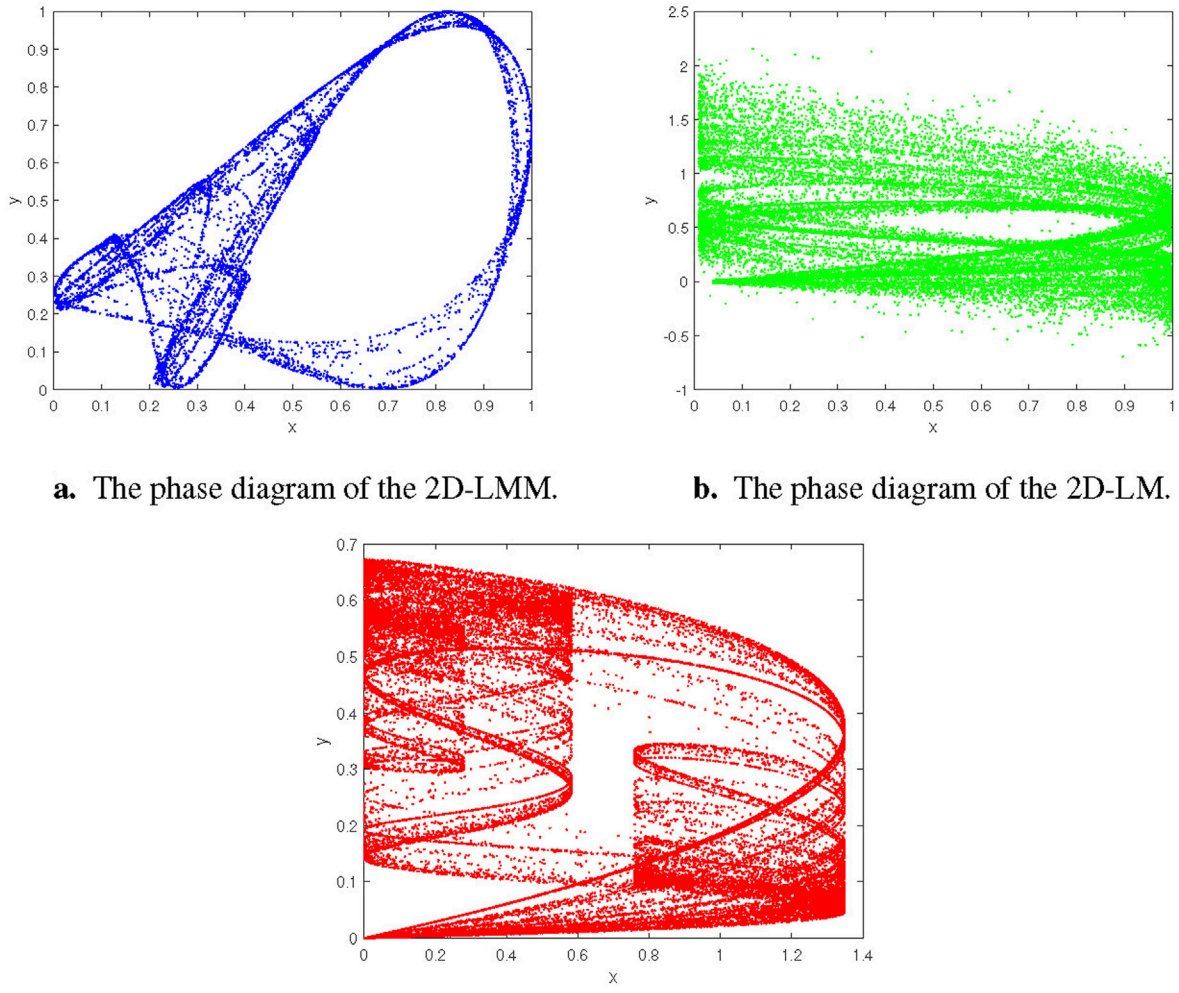



FIGURE 4
The phase diagram of 2D-LMM **(A)**, 2D-LM **(B)**, 2D-LFHCM **(C)** in the $x-y$ plane.

TABLE 2 DNA code table.

| Quaternary number | Rule 1 | Rule 2 | Rule 3 | Rule 4 | Rule 5 | Rule 6 | Rule 7 | Rule 8 |
|---|---|---|---|---|---|---|---|---|
| 0 | A | A | T | T | C | C | G | G |
| 1 | C | G | C | G | A | T | A | T |
| 2 | G | C | G | C | T | A | T | A |
| 3 | T | T | A | A | G | G | C | C |

The DNA right shift XOR $f_{rX}$ is expressed as

$$f_{rX} = \begin{bmatrix} R_X((A,C,G,T),(A)_4) \\ R_X((A,C,G,T),(C)_4) \\ R_X((A,C,G,T),(G)_4) \\ R_X((A,C,G,T),(T)_4) \end{bmatrix} = \begin{bmatrix} R_X((A,C,G,T),0) \\ R_X((A,C,G,T),1) \\ R_X((A,C,G,T),2) \\ R_X((A,C,G,T),3) \end{bmatrix} \rightarrow \begin{bmatrix} A & A & A & A \\ T & C & T & C \\ G & G & G & G \\ C & T & C & T \end{bmatrix}$$

## 4 Proposed image encryption scheme

This section includes a thorough overview of the important parts of the encryption mechanism, such as key creation, chaotic DNA scrambling, and diffusion. Specifically, the scrambling operation exchanges the position and interference of pixels in the ordinary image, minimizing the strong correlation between adjacent pixel values. The pixel data diffusion serves as a critical measure to enhance security. By integrating scrambling and diffusion, both

TABLE 3 DNA operation rules table.

| Addition | | | | | Subtraction | | | | | Exclusive or | | | | | Right shift | | | | | Left shift | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| + | A | C | G | T | – | A | C | G | T | xor | A | C | G | T | A | C | G | T | → | A | C | G | T | ← |
| A | A | C | G | T | A | A | C | T | G | A | A | C | G | T | A | C | G | T | A | A | C | G | T | A |
| C | C | A | T | G | C | C | A | G | T | C | C | A | T | G | T | A | C | G | C | T | A | C | G | C |
| G | G | T | C | A | G | G | T | A | C | G | G | T | A | C | G | T | A | C | G | G | T | A | C | G |
| T | T | G | A | C | T | T | G | C | A | T | T | G | C | A | C | G | T | A | T | C | G | T | A | T |

the position and grayscale value of the pixel are simultaneously altered, ensuring that the grayscale information of any pixel is concealed within numerous other pixels.

Let $I_1$ denote a grayscale image of size $M \times N$, where $N$ represents the number of columns and $M$ is the number of rows. The encryption and decryption process based on the principles outlined in Section 3 is detailed below, and the flow chart of the entire encryption process is shown in Figure 5.

**Step 1.** Key stream generation.

(i) Let $(x_0^1, y_0^1) = (0.1, 0.1)$, $(x_0^2, y_0^2) = (0.2, 0.2)$, $(x_0^3, y_0^3) = (0.3, 0.3)$, $\lambda = 6$ and $\mu = 1.4$ serve as the initial conditions and control parameters employed for iterating Equation 6.

(ii) After iterating $n_0 + 4MN$ times, three pseudo-random generated sequences $\{y^1_{n_0+4MN}\}$, $\{y^2_{n_0+4MN}\}$, and $\{y^3_{n_0+4MN}\}$ are obtained separately.

(iii) To eliminate transient effects for increased security, the first $n_0$ or $n_0 + 3MN$ iterations of sequences $\{y^1_{n_0+4MN}\}$, $\{y^2_{n_0+4MN}\}$, and $\{y^3_{n_0+4MN}\}$ (where $n_0 = 800$) are discarded. New sequences $y_1$, $y_2$, and $y_3$, respectively, of length $4MN$, $MN$, and $4MN$ are obtained.

(iv) The encrypted chaotic sequence $s_1$ is produced by Equation 9. The $y_1$ elements are sorted in ascending order, $y_{new}$ is the newly formed sequence after sorting, and $s_1$ is the index value of $y_{new}$.

$$[y_{new}, s_1] = sort(y_1), \tag{9}$$

where, the function sort is employed to arrange the data and provide the corresponding index values.

(v) Generation of the encrypted chaotic sequence $s_2$. By applying the following Equation 10 to compute the obtained pseudo-random sequence $y_2$, ensuring that the values of $y_2$ are within $\{0, 1, 2, 3\}$, a new sequence $s_2$ is obtained.

$$s_2(i) = floor(mod(y_2(i) \times 10^3, 4)), \tag{10}$$

where $i = 1, 2, 3, \ldots, MN$, and $floor(x)$ denotes the function that outputs the largest integer less than $x$.

(vi) The generation of an encrypted chaotic sequence, referred to as $s_3$, involves several steps. First, the sequence $y_3$ is processed using Equation 11 to ensure that the resulting sequence, denoted as $y_3^*$, only consists of values within the range $\{0, 1, 2, 3\}$. Second, the processed sequence $y_3^*$ undergoes encoding into a DNA sequence following rule 1 presented in Table 2. Finally, Equation 12 is applied to the encoded sequence to obtain the desired chaotic sequence, referred to as $s_3$. In other words, sequence $s_3$ is generated sequentially from sequence $y_3^*$, taking groups of four.

$$y_3^*(i) = mod(floor((y_3(i) + 100)^* 10^3), 4), \quad i = 1, 2, 3, \ldots, 4MN, \tag{11}$$

$$s_3(j) = y_3^*(4j - 3{:}\ 4j), \quad j = 1, 2, 3, \ldots, MN. \tag{12}$$

**Step 2.** DNA encoding of the original image.

(i) Let $I_1$ be a grayscale image with dimensions $M \times N$.

(ii) Reshape the original image $I_1$ of size $M \times N$ into a $1 \times MN$ vector $I_2$.

(iii) Encode each pixel value of $I_2$ into a 4-bit quaternary number, transforming vector $I_2$ into a quaternary matrix $I_3$ of size $1 \times 4MN$.

(iv) The DNA image $I_4$, with a size of $1 \times 4MN$, is produced by encoding each element of the image $I_3$ into quaternary, which corresponds to the four nucleotides A, C, G, and T depending on rule 1 in Table 2.

**Step 3.** DNA chaotic confusion and diffusion.

(i) To initiate the initial chaotic confusion, the following Equation 13 is employed to disrupt the positions of $I_4$.

$$I_5(i) = I_4(s(i)), \ i = 1, 2, 3, \ldots, 4MN. \tag{13}$$

(ii) The sequence $I_5$ is extracted and grouped consecutively into sets of four. This new sequence is then denoted as $I_6$, as illustrated in Equation 14.

$$I_6(i) = I_5(4i - 3{:}\ 4i), \ i = 1, 2, 3, \ldots, 4MN. \tag{14}$$

(iii) The implementation of the DNA diffusion operation between the DNA sequence $I_6$ and the key DNA sequences $s_2$ and $s_3$ are conducted using Equation 15.

$$I_7(i) = \begin{cases} R_+(I_6(i), (A)_4) = R_+(I_6(i), 0) \text{ if } s_2(i) = 0; \\ L_-(I_6(i), (C)_4) = L_-(I_6(i), 1) \text{ if } s_2(i) = 1; \\ R_X(I_6(i), (G)_4) = R_X(I_6(i), 2) \text{ if } s_2(i) = 2; \\ L_X(I_6(i), (T)_4) = L_X(I_6(i), 3) \text{ if } s_2(i) = 3, \end{cases} \tag{15}$$

(iv) To further scramble the positions, we employ the method presented in (i), which is Equation 16 in this case, to disrupt

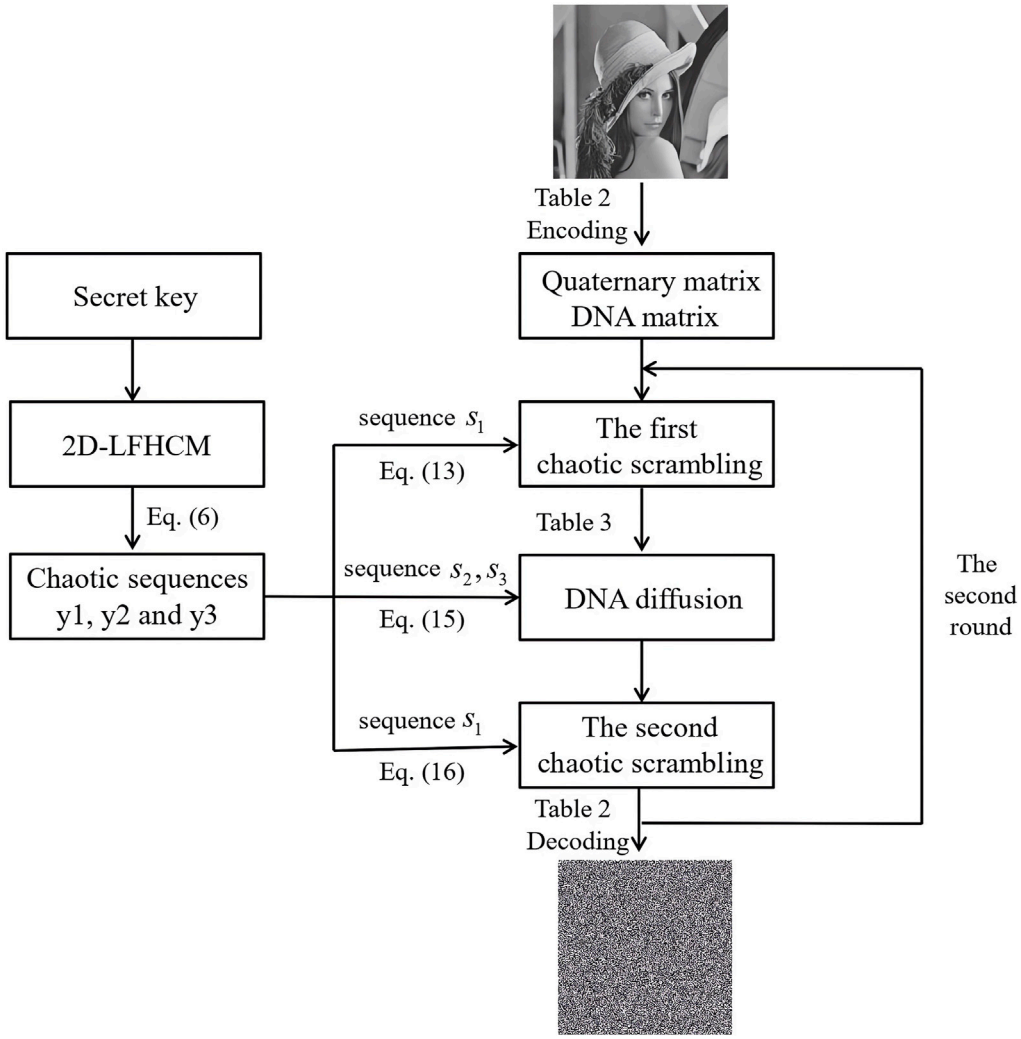



FIGURE 5
Flowchart of the encryption process (where the picture of Lena is sourced from [38]).

the position of $I_7$, effectively achieving the second chaotic scrambling.

$$I_8(i) = I_7(s(i)),\ i = 1, 2, 3, \ldots, 4MN. \tag{16}$$

(v) Following rule 1 in Table 2, every nucleotide A, C, G, and T in the diffused DNA image $I_8$ is decoded into a quaternary number, resulting in an encrypted quaternary image $I_9$ of size $1 \times 4MN$.

(vi) Encoded as integer values in the range of 0–255 for every 4 bits, these values are then transformed into a grayscale cipher image $I_{10}$ with dimensions $1 \times MN$.

**Step 4.** Cipher image.

The gray cipher image $I_{10}$, which is $1 \times MN$ in size, is reshaped into a gray cipher image $I_{11}$ with dimensions $M \times N$.

The image decryption process closely mirrors the encryption procedure, involving the sequential inversion of steps utilized in encryption and relying on the application of a cryptographic key. Similarly, if DNA right shift addition is utilized in the encryption phase, it would be reversed in the decryption phase.

## 5 Performance evaluation

In this section, various images (such as Lena, Onion, and Cameraman) will be utilized to evaluate the performance of the proposed cryptosystem based on image statistical performance and security analysis. All experimental results were calculated using MATLAB 2018b on a compatible computer with Windows 10, 8.00 GB RAM, and Intel (R) Core (TM) i5-7300HQ CPU @ 2.50 GHz. Figure 6 displays the encryption performance of the proposed cryptographic system. Each part begins with a row displaying the plain image, followed by the encrypted image, and concludes with the decrypted image, from left to right. The second line exhibits histograms for both the plain and encrypted images. We have documented all experimental data in a table, which provides evidence of the outstanding capabilities of our cryptographic system in effectively addressing various security and statistical risks.

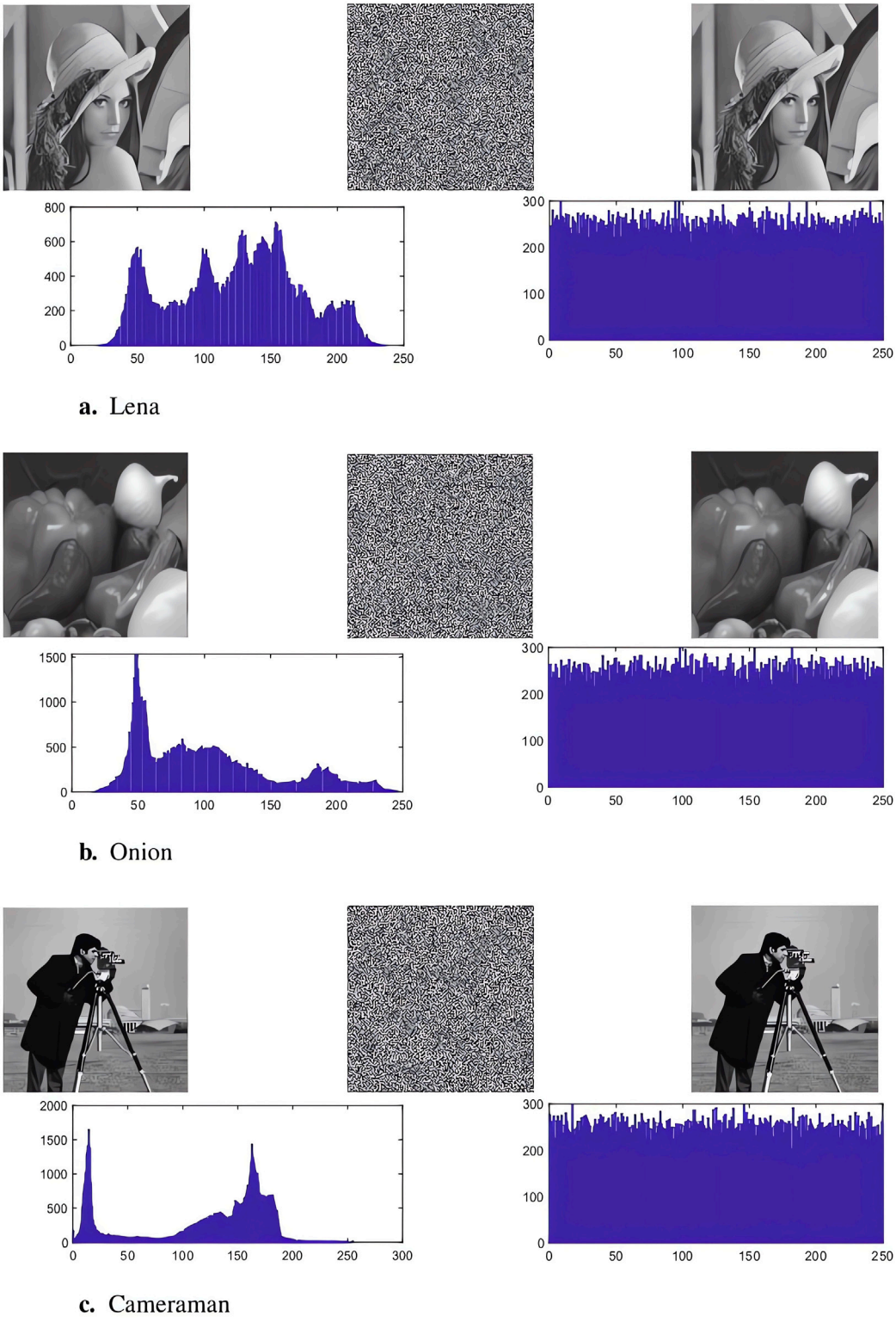



FIGURE 6
The original images, encrypted images, decrypted images, and histograms of the original and encrypted images of Lena **(A)**, Onion **(B),** and Cameraman **(C)**, respectively (where the pictures of Lena, Onion, and Cameraman are sourced from [38], [43], and [27], respectively).

TABLE 4 Comparison of encryption time of different algorithms.

| Encryption algorithm | Time cost (units in s) | Encryption speed (units in Kbit/s) |
|---|---|---|
| Proposed in this paper | 0.4753 | 1077.2144 |
| Reference [38] | 0.4862 | 1053.0646 |
| Reference [39] | 3.6240 | 141.2804 |
| Reference [40] | 0.5683 | 900.9326 |

## 5.1 Key space analysis

The extent of the key space in an image encryption scheme is a pivotal factor in determining its security. The key space encompasses all authorized keys for the scheme. Evidently, an expanded key space augments the scheme's resilience against exhaustive attacks, thereby ensuring an elevated level of security for the encrypted image algorithm. As a general rule, if the key space exceeds $2^{100} \approx 10^{30}$, the encryption mechanism becomes impervious to brute force attempts. In this paper, the encryption scheme's initial key comprises two control parameters, namely, $\lambda$ and $\mu$, along with two initial values, $x_0$ and $y_0$. By adhering to the Institute of Electrical and Electronic Engineers' (IEEE) recommendation of using 64-bit double-precision numbers, the key space for this scheme can amount to $(10^{15})^4 = 10^{60}$. This immense value far surpasses $10^{30}$, thereby ensuring that the image encryption scheme presented in this study possesses a suitably extensive key space, affording it robust protection against severe attacks.

## 5.2 Time cost and speed analysis

A superior encryption scheme should not sacrifice encryption time but instead strive to minimize it while ensuring security. In certain application scenarios, such as image transmission, real-time performance is paramount. This necessitates that encryption algorithms be capable of completing data encryption within a short timeframe to ensure real-time transmission. The average encryption time for the aforementioned grayscale images of size $256 \times 256$ were calculated and compared with several established encryption algorithms, including DNA encoding or *S*-box. The amount of data of a gray image with a size of $256 \times 256$ is about 512 Kbit, so the encryption speed can be obtained. All results are presented in Table 4. It can be observed from the table that the proposed solution exhibits the shortest encryption duration, indicating its superior encryption efficiency.

## 5.3 Histogram analysis

During everyday practical use, there is a potential risk of theft or attack on encrypted images while they are being transmitted. Thus, it becomes crucial to assess both the statistical properties and security of these encrypted images. One of the most basic and intuitive techniques for examining the frequency distribution in plaintext and encrypted images is histogram analysis. Examining the histogram is instrumental in assessing the performance of the encryption algorithm. In case the histogram of the encrypted image exhibits an even or irregular distribution, it indicates that the statistical characteristics have been concealed or destroyed, suggesting that the encryption algorithm might be more efficient. If the histogram of the ciphertext image displays noticeable characteristics or exhibits a notably dissimilar distribution pattern compared to that of the plaintext image, it could indicate potential vulnerabilities in information leakage or the encryption algorithm. Such observations are valuable in identifying encryption issues and enhancing the encryption scheme. In Figure 6, the histograms for various images (Lena, Onion, and Cameraman) can be observed. From an intuitive perspective, it becomes apparent that encrypted images exhibit a uniform histogram, while the histograms of plaintext images vary. If the histogram of encrypted images exhibits an approximately uniform distribution, indicating a lack of discernible regularity in pixel value distribution, it signals the heightened robustness of the encryption scheme against statistical attacks.

## 5.4 Chi-square analysis

Non-uniformly distributed pixel values can imply that there are some specific features or structures in the image, which may make it easier for the encrypted image to infer some information from the histogram, thereby compromising the encryption's security level. On the contrary, when pixel values are uniformly distributed, potential intruders are prevented from extracting reliable information from the histogram, because the histogram lacks discernible peaks or features, indicating that the image's statistical characteristics are to some extent concealed. Consequently, inferring information about the original image from the histogram becomes challenging.

The $\chi^2$ statistic (one-sided hypothesis test) is frequently employed to quantify the difference between the two in terms of quantity. Chi-square represents a statistical method utilized to measure such differences. If the frequency distribution of a given set of samples is denoted by $f_i$, $i = 1, 2, \ldots, n$, the theoretical frequency distribution is assumed to be $g_i$, $i = 1, 2, \ldots, n$. Assumption $H_0$: The sample comes from the theoretical distribution. When $H_0$ is assumed to hold Equation 17,

$$\chi^2 = \sum_{i=1}^{n} \frac{(f_i - g_i)^2}{g_i}, \tag{17}$$

is called the Pearson $\chi^2$ statistic and obeys the $\chi^2$ distribution with $n - 1$ degrees of freedom.

Given the image dimensions as $M \times N$, we posit that the pixel frequency $f_i$ associated with each gray value in the histogram

TABLE 5 The entropy values and scores of the original images and encrypted images of Lena, Onion, and Cameraman, respectively.

| Images | P/E | Size | Information entropy | Chi-square score |
|---|---|---|---|---|
| Lena | Plain | 256 × 256 | 7.4508 | $4.0523 \times 10^4$ |
| Lena | Encrypted | 256 × 256 | 7.9997 | 278.7568 |
| Onion | Plain | 256 × 256 | 7.3426 | $6.8641 \times 10^4$ |
| Onion | Encrypted | 256 × 256 | 7.9971 | 262.9375 |
| Cameraman | Plain | 256 × 256 | 7.1048 | $9.8781 \times 10^4$ |
| Cameraman | Encrypted | 256 × 256 | 7.9984 | 264.9377 |

TABLE 6 Results of the correlation coefficient between original and encrypted images of Lena, Onion, and cameraman in various directions.

| Images | Direction | Plain image correlation | Encrypted image correlation |
|---|---|---|---|
| Lena | Horizontal | 0.9757 | 0.0021 |
| Lena | Vertical | 0.9552 | 0.0102 |
| Lena | Main diagonal | 0.9229 | 0.0006 |
| Lena | Secondary diagonal | 0.9372 | −0.0148 |
| Onion | Horizontal | 0.9926 | 0.0032 |
| Onion | Vertical | 0.9934 | −0.0179 |
| Onion | Main diagonal | 0.9840 | 0.0056 |
| Onion | Secondary diagonal | 0.9892 | 0.0228 |
| Cameraman | Horizontal | 0.9596 | 0.0339 |
| Cameraman | Vertical | 0.9284 | 0.0003 |
| Cameraman | Main diagonal | 0.8921 | −0.0164 |
| Cameraman | Secondary diagonal | 0.9076 | −0.0063 |

conforms to a uniform distribution. At this time, $g_i = g = MN/256,\ i = 0, 1, 2 \ldots, 255$, then,

$$\chi^2 = \sum_{i=0}^{255} \frac{(f_i - g_i)^2}{g_i} = \sum_{i=0}^{255} \frac{\left(f_i - \frac{MN}{256}\right)^2}{\frac{MN}{256}} = \frac{1}{256} \sum_{i=0}^{255} \frac{(256 f_i - MN)^2}{MN}. \tag{18}$$

Equation 18 obeys the $\chi^2$ distribution with a degree of freedom of 255. The significance level $\alpha$ is given such that $P\{\chi^2 \geqslant \chi_\alpha^2(n-1)\} = \alpha$, that is, the null hypothesis $H_0$ is accepted when $\chi^2 < \chi_\alpha^2(n-1)$. In instances where the level of significance $\alpha = 0.01, \alpha = 0.05$, and $\alpha = 0.1$, the degree of freedom is 255, the $\chi^2$ distribution value $\chi_{0.01}^2(255) = 310.457$, $\chi_{0.05}^2(255) = 293.248$, and $\chi_{0.1}^2(255) = 284.336$.

The generally used significance level is $\alpha = 0.05$. An encrypted image with a chi-square score of $\chi_{0.05}^2(255) = 293.248$ indicates a highly uniform pixel distribution. Table 4 presents the chi-square scores for various encrypted images, namely, Lena, Onion, and Cameraman, demonstrating that the pixel values of our proposed encryption scheme are evenly distributed between 0 and 255 in different rounds of encryption. As a consequence, the ciphertext histogram exhibits an even distribution, suggesting that the image encryption method employed in this study demonstrates increased resilience against statistical attacks. The outcomes of the $\chi^2$ test can be found in the provided Table 5.

## 5.5 Information entropy

The unpredictability of image information is reflected in information entropy. It is widely accepted that higher entropy corresponds to increased uncertainty, greater disorder within the information, and reduced visual information. The calculation formula for information entropy can be expressed as Equation 19.

$$H = -\sum_{i=0}^{L} p(i) \log_2 p(i), \tag{19}$$

where, $L$ represents the gray level of the image, and $p(i)$ denotes the probability of gray level $i$.

For a randomly generated grayscale image with a gray level of $L = 256$, the theoretical information entropy value $H$ is 8. The information entropy is computed for plain images of Lena, Onion, Cameraman, and their corresponding encrypted

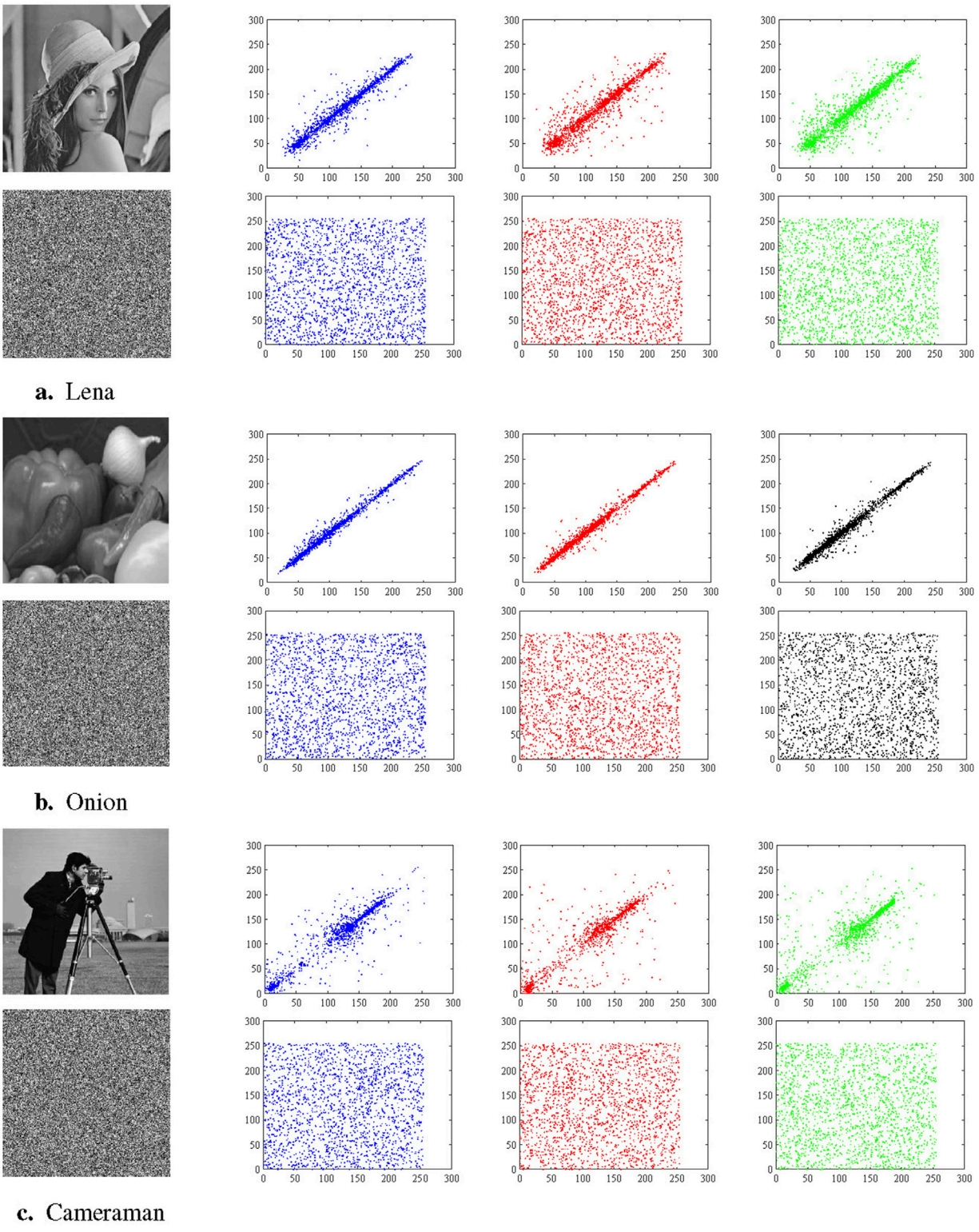



FIGURE 7
The first row of the three sets of images Lena **(A)**, Onion **(B)**, and Cameraman **(C)**, from left to right, are the original images and the correlation of adjacent pixels of the original images in the horizontal, vertical, and diagonal direction, respectively. The second row is the same, only for their encrypted images. (The pictures of Lena, Onion, and Cameraman are sourced from [38], [43], and [27], respectively).

versions. The results of the calculations are presented in Table 5, revealing that the information entropies of encrypted images closely approach 8. This suggests that encrypted images exhibit a more advantageous random distribution. Therefore, the encryption method proposed by us exhibits strong resistance to entropy-based attacks.

TABLE 7 Comparison of encryption performance of different algorithms (Lena, and size: 256 × 256).

| Algorithm | Adjacent pixel correlation | | | Information entropy | Time cost | Encryption speed |
|---|---|---|---|---|---|---|
| | Horizontal | Vertical | Diagonal | | | |
| Proposed in this paper | 0.0021 | 0.0102 | **0.0006** | **7.9997** | **0.4753** | **1077.2144** |
| Reference [25] | −0.0017 | −0.0009 | −0.0019 | 7.9962 | 0.9170 | 558.3424 |
| Reference [39] | −0.0031 | 0.0084 | −0.0007 | 7.9971 | — | — |
| Reference [38] | 0.0068 | −0.0054 | 0.0010 | 7.9967 | 0.4862 | 1053.0646 |
| Reference [41] | −0.0036 | 0.0026 | 0.0012 | 7.9995 | 0.9510 | 538.3807 |
| Reference [42] | **−0.0006** | −0.0057 | 0.0009 | 7.9938 | — | — |
| Reference [43] | 0.0013 | **0.0002** | 0.0033 | 7.9972 | — | — |
| Reference [44] | 0.0105 | −0.0023 | 0.0052 | **7.9997** | — | — |

Note: Bold font indicates the best result in each column. "-" indicates that the reference did not record this test result for the Lena image.

## 5.6 Correlation

Evaluating the correlation properties of both the original and encrypted images is essential, complementing the analysis of the image's histogram and information entropy. Neighboring pixels in the horizontal, vertical, main diagonal, and sub-diagonal directions exhibit a strong correlation in the original image. The objective of image encryption algorithms is to minimize the correlation between adjacent pixels in the encrypted image, providing a defense against statistical attacks. A correlation value of zero is ideal. This study randomly samples 2000 pairs of neighboring pixels along the horizontal, vertical, main diagonal, and secondary diagonal directions from both the plain and encrypted images. In this study, 2000 pairs of adjacent pixels are randomly selected from both the original and encrypted images in the horizontal, vertical, main diagonal, and secondary diagonal directions. The correlation coefficient between the two adjacent pixels can be computed by applying Equation 20.

$$\begin{cases} E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i; \\ D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2; \\ cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)); \\ r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \end{cases} \tag{20}$$

where $N$ is the number of pixel pairs, $x$ and $y$ denote the gray values of two adjacent pixels, $E(x)$ is the mean value, $D(x)$ represents variance, $\mathrm{cov}(x, y)$ stands for covariance, and $r_{xy}$ is correlation coefficient of $x$ and $y$. The correlation coefficients for both plain and encrypted images of Lena, Onion, and Cameraman in the horizontal, vertical, main diagonal, and secondary diagonal directions are presented in Table 6.

The correlation between adjacent pixels in the original and encrypted images of Lena, Onion, and Cameraman is depicted in Figure 7 for the horizontal, vertical, and main diagonal directions (from left to right). The experimental results indicate a lack of significant correlation between neighboring pixels in the encrypted images, in contrast to the noticeable correlation present in the original images. The efficacy of the encryption system described in this study is highlighted by this conclusion. It's important to note that these results are obtained after only a single round of encryption. If multiple encryptions are performed, the effect may be more significant.

## 5.7 Comparison and analysis

The algorithm in this paper is used to encrypt and test the performance of image Lena, and compared with other encryption algorithms. The test results of other algorithms are directly quoted from the corresponding papers. The comparison results are shown in Table 7. It can be observed that the performance difference of adjacent pixel correlation analysis of each algorithm is small. In terms of information entropy and other resistance to statistical attacks and encryption speed, the algorithm in this paper has better performance, indicating that the algorithm in this paper has better security.

# 6 Conclusion

The hybrid image encryption method described in this paper integrates DNA computing theory with the improved 2D-LFHCM. Furthermore, the security, histogram, correlation coefficient, and information entropy aspects of the proposed scheme are examined to demonstrate its rationality. Numerical simulations demonstrate the notable efficacy of the image encryption technique introduced in this study.

A feasible idea for future work is to apply the proposed method to multi-image encryption [24,36], which can improve efficiency while ensuring security. Another possibility is to combine encryption with quantum technology. In light of the advancements in quantum information technology, numerous technologies have been proposed to enhance traditional image encryption algorithms. The exponentially accelerating

capabilities of quantum technology, as opposed to traditional computing, are critical for mitigating the vulnerability of encryption algorithms to decipherment. To harness the potential benefits of combining quantum computing with conventional image encryption approaches, Hua Hua et al. [30] came up with dynamic image encryption via quantum walks and chaos-induced DNA to boost image security. Wen Wen and Lin [37] analyzed the security of an existing image encryption algorithm based on quantum chaotic map and DNA coding (QCMDC-IEA), and proposed a low-complexity attack method, which provides some theoretical tips and suggestions for improving the security of the system based on DNA coding and chaotic image encryption. Our upcoming study aims to investigate the potential synergy between quantum walking and the recently proposed DNA computing principles to develop an innovative encryption method. This novel approach is expected to enhance the security measures for image encryption, thus carrying significant implications.

## Data availability statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

## Author contributions

YC: Software, Validation, Writing–original draft. TL: Funding acquisition, Supervision, Writing–review and editing. CC: Conceptualization, Formal Analysis, Writing–review and editing. YX: Investigation, Writing–review and editing.

## Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. This work was funded by Sichuan Science and Technology Program (No. 2023NSFSC0070), the Opening Project of Sichuan Province University Key Laboratory of Bridge Non-destruction Detecting and the Engineering Computing (No. 2023QYJ06), and Innovation Team Program of Sichuan University of Science and Engineering (No. SUSE652B002).

## Acknowledgments

Many thanks to Prof. Simin Yu, Prof. Yong Wang, and Prof. Xiaoyuan Wang for their help in achieving this work.

## Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## Publisher's note



## References

1. Chen L, Li CQ, Li C. Security measurement of a medical communication scheme based on chaos and dna coding. *J Vis Commun Image Representation* (2022) 83:103424. doi:10.1016/j.jvcir.2021.103424

2. Wang S, Peng Q, Du B. Chaotic color image encryption based on 4d chaotic maps and dna sequence. *Opt Laser Technology* (2022) 148:107753. doi:10.1016/j.optlastec.2021.107753

3. Wen H, Lin Y. Cryptanalyzing an image cipher using multiple chaos and dna operations. *J King Saud University-Computer Inf Sci* (2023) 35:101612. doi:10.1016/j.jksuci.2023.101612

4. Zhang Z, Tang J, Zhang F, Ni H, Chen J, Huang Z. Color image encryption using 2d sine-cosine coupling map. *IEEE Access* (2022) 10:67669–85. doi:10.1109/access.2022.3185229

5. Huang Z, Cheng S, Gong L, Zhou N. Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. *Opt Lasers Eng* (2020) 124:105821. doi:10.1016/j.optlaseng.2019.105821

6. Wu C, Hu K, Wang Y, Wang J, Wang QH. Scalable asymmetric image encryption based on phase-truncation in cylindrical diffraction domain. *Opt Commun* (2019) 448:26–32. doi:10.1016/j.optcom.2019.05.009

7. Li X, Li C, Lee I-K. Chaotic image encryption using pseudo-random masks and pixel mapping. *Signal Process.* (2016) 125:48–63. doi:10.1016/j.sigpro.2015.11.017

8. Supreeti K, Sukanta D. A study of chaos in non-uniform cellular automata. *Commun Nonlinear Sci Numer Simulation* (2019) 76:116–31. doi:10.1016/j.cnsns.2019.04.020

9. Chai X, Zheng X, Gan Z, Han D, Chen Y. An image encryption algorithm based on chaotic system and compressive sensing. *Signal Process.* (2018) 148:124–44. doi:10.1016/j.sigpro.2018.02.007

10. Gong L, Qiu K, Deng C, Zhou N. An image compression and encryption algorithm based on chaotic system and compressive sensing. *Opt Laser Technology* (2019) 115:257–67. doi:10.1016/j.optlastec.2019.01.039

11. Chen Y, Lu T, Wang Q. The chaotic properties and circuit design of a generalized high-dimensional integer-domain system. *Chaos, Solitons and Fractals* (2024) 181:114610. doi:10.1016/j.chaos.2024.114610

12. Li C, Gao Y, Lei T, Li RYM, Xu Y. Two independent offset controllers in a three-dimensional chaotic system. *Int J Bifurcation Chaos* (2024) 34:2450008. doi:10.1142/s0218127424500081

13. Li Y, Li C, Zhong Q, Liu S, Lei T. A memristive chaotic map with only one bifurcation parameter. *Nonlinear Dyn* (2024) 112:3869–86. doi:10.1007/s11071-023-09204-0

14. Kong X, Yu F, Yao W, Cai S, Zhang J, Lin H. Memristor-induced hyperchaos, multiscroll and extreme multistability in fractional-order hnn: image encryption and fpga implementation. *Neural Networks* (2024) 171:85–103. doi:10.1016/j.neunet.2023.12.008

15. Wang X, Zhang X, Gao M, Iu HHC, Wang C. A color image encryption algorithm based on hash table, halbert curve and hyper-chaotic synchronization. *Mathematics* (2023) 11:567. doi:10.3390/math11030567

16. Yu F, Kong X, Yao W, Zhang J, Cai S, Lin H, et al. Dynamics analysis, synchronization and fpga implementation of multiscroll hopfield neural networks with non-polynomial memristor. *Chaos, Solitons and Fractals* (2024) 179:114440. doi:10.1016/j.chaos.2023.114440

17. Wang MJ, Gu L. Multiple mixed state variable incremental integration for reconstructing extreme multistability in a novel memristive hyperchaotic jerk system with multiple cubic nonlinearity. *Chin Phys B* (2024) 33:020504. doi:10.1088/1674-1056/acddd0

18. Matthews R. On the derivation of a chaotic encryption algorithm. *Cryptologia* (1989) 13:29–42. doi:10.1080/0161-118991863745

19. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int J Bifurcation Chaos* (2006) 16:2129–51. doi:10.1142/s0218127406015970

20. Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos. *Signal Process.* (2012) 92:1101–8. doi:10.1016/j.sigpro.2011.10.023

21. Wang Q, Yu S, Li C, Lu J, Fang X, Guyeux C, et al. Theoretical design and fpga-based implementation of higher-dimensional digital chaotic systems. *IEEE Trans Circuits Syst Regular Pap* (2016) 63:401–12. doi:10.1109/tcsi.2016.2515398

22. Huang L, Wang S, Xiang J. A tweak-cube color image encryption scheme jointly manipulated by chaos and hyper-chaos. *Appl Sci* (2019) 9:4854. doi:10.3390/app9224854

23. Wang X, Su Y, Zhang H, Zou C. A new hybrid image encryption algorithm based on gray code transformation and snake-like diffusion. *Vis Computer* (2021) 38:3831–52. doi:10.1007/s00371-021-02224-0

24. Gao X, Mou J, Xiong L, Sha Y, Yan H, Gao Y. A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. *Nonlinear Dyn* (2022) 108:613–36. doi:10.1007/s11071-021-07192-7

25. Alexan W, Elkandoz M, Mashaly M, Azab E, Aboshousha A. Color image encryption through chaos and KAA map. *IEEE Access* (2023) 11:11541–54. doi:10.1109/access.2023.3242311

26. Chai X, Chen Y, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt Lasers Eng* (2017) 88:197–213. doi:10.1016/j.optlaseng.2016.08.009

27. Wu J, Liao X, Yang B. Image encryption using 2d henon-sine map and dna approach. *Signal Process.* (2018) 153:11–23. doi:10.1016/j.sigpro.2018.06.008

28. Patel S, Bharath K-P, Kumar R. Symmetric keys image encryption and decryption using 3d chaotic maps with dna encoding technique. *Multimedia Tools Appl* (2020) 79:31739–57. doi:10.1016/j.cnsns.2019.04.020

29. Liu Q, Liu L. Color image encryption algorithm based on dna coding and double chaos system. *IEEE Access* (2020) 8:83596–610. doi:10.1109/access.2020.2991420

30. Hua N, Liu H, Xiong X, Wang JL, Liang JQ. A dynamic image encryption scheme based on quantum walk and chaos-induced dna. *Quan Eng* (2023) 2023:1–15. doi:10.1155/2023/3431107

31. Wu Y, Yang G, Jin H, Noonan JP. Image encryption using the two-dimensional logistic chaotic map. *J Electron Imaging* (2012) 21:013014. doi:10.1117/1.jei.21.1.013014

32. Ye X, Wang X. Design a novel image encryption algorithm based on a prng with high performance. *IEEE MultiMedia* (2022) 99:1–11. doi:10.1109/mmul.2022.3232180

33. Lu J, Wu X, Lv J, Kang L. A new discrete chaotic system with rational fraction and its dynamical behaviors. *Chaos, Solitons and Fractals* (2004) 22:311–9. doi:10.1016/j.chaos.2004.01.010

34. Watson JD, Crick FHC. Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid. *Nature* (1953) 171:737–8. doi:10.1038/171737a0

35. Lone PN, Singh D, Mir UH. Image encryption using dna coding and three-dimensional chaotic systems. *Multimedia Tools Appl* (2022) 81:5669–93. doi:10.1007/s11042-021-11802-2

36. Chen X, Mou J, Cao Y, Banerjee S. Chaotic multiple-image encryption algorithm based on block scrambling and dynamic dna coding. *Int J Bifurcation Chaos* (2023) 33:2350190. doi:10.1142/s0218127423501900

37. Wen H, Lin Y. Cryptanalysis of an image encryption algorithm using quantum chaotic map and dna coding. *Expert Syst Appl* (2024) 237:121514. doi:10.1016/j.eswa.2023.121514

38. Sun S. A novel hyperchaotic image encryption scheme based on dna encoding, pixel-level scrambling and bit-level scrambling. *IEEE Photon J* (2018) 10:1–14. doi:10.1109/jphot.2018.2817550

39. Xu L, Li Z, Li J, Hua W. A novel bit-level image encryption algorithm based on chaotic maps. *Opt Lasers Eng* (2016) 78:17–25. doi:10.1016/j.optlaseng.2015.09.007

40. Brindha M, Gounden NA. A chaos based image encryption and lossless compression algorithm using hash table and Chinese remainder theorem. *Appl Soft Comput* (2016) 40:379–90. doi:10.1016/j.cnsns.2019.04.020

41. Zarebnia M, Pakmanesh H, Parvaz R. A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images. *Optik* (2019) 179:761–73. doi:10.1016/j.ijleo.2018.10.025

42. Kaur G, Agarwal R, Patidar V. Chaos based multiple order optical transform for 2d image encryption. *Eng Sci Technol Int J* (2020) 23:998–1014. doi:10.1016/j.jestch.2020.02.007

43. He P, Sun K, Zhu C. A novel image encryption algorithm based on the delayed maps and permutation-confusion-diffusion architecture. *Security Commun Networks* (2021) 2021:1–16. doi:10.1155/2021/6679288

44. Kumar K, Roy S, Rawat U, Malhotra S. Iehc: an efficient image encryption technique using hybrid chaotic map. *Chaos, Solitons and Fractals* (2022) 158:111994. doi:10.1016/j.chaos.2022.111994