Hindawi
Journal of Chemistry
Volume 2023, Article ID 9812601, 1 page
https://doi.org/10.1155/2023/9812601

Retraction

Retracted: A Double-Layer Image Encryption Scheme Based on Chaotic Maps and DNA Strand Displacement

Journal of Chemistry

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

Copyright © 2023 Journal of Chemistry. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Z. Tang, Z. Yin, R. Wang, X. Wang, J. Yang, and J. Cui, "A Double-Layer Image Encryption Scheme Based on Chaotic Maps and DNA Strand Displacement," *Journal of Chemistry*, vol. 2022, Article ID 3906392, 10 pages, 2022.

Hindawi
Journal of Chemistry
Volume 2022, Article ID 3906392, 10 pages
https://doi.org/10.1155/2022/3906392

RETRACTED

Research Article

A Double-Layer Image Encryption Scheme Based on Chaotic Maps and DNA Strand Displacement

Zhen Tang,[1] Zhixiang Yin,[2] Risheng Wang,[1] Xiyuan Wang,[1] Jing Yang,[1] and Jianzhong Cui[3]

[1]*School of Mathematics and Big Data, Anhui University of Science and Technology, Huainan, Anhui 232001, China*
[2]*School of Mathematics,Physics and Statistics, Shanghai University of Engineering Science, Shanghai 201620, China*
[3]*Department of Computer, Huainan Union University, Huainan, Anhui 232001, China*

Correspondence should be addressed to Zhixiang Yin; zxyin66@163.com

Received 18 December 2021; Accepted 12 January 2022; Published 28 January 2022

Academic Editor: Haidar Ali

Copyright © 2022 Zhen Tang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The image encryption schemes combining chaotic maps, DNA coding, and DNA sequence operation can effectively protect the image. In this paper, a double-layer image encryption scheme is proposed by combining chaotic maps with DNA strand displacement (DSD). Chaotic maps are used to generate pseudorandom sequences and perform routine scrambling and diffusion operations on the plaintext image. We propose three DSD-based encryption rules according to the diversity of DNA strand displacement, and these three encryption rules are used to encrypt the image at the DNA sequence level. The plaintext image can be transformed into the cipher image, which is difficult to be recognized without the correct keys through the double-layer encryption at the level of chaotic maps and DNA. Simulation results and security analysis show that the proposed encryption scheme can effectively protect image information and resist conventional information attacks.

1. Introduction

The ways of information storage and transmission are diversified. While modern information technology brings convenience, it also faces severe challenges form information security. Different from one-dimensional text information, image data has the characteristics of strong correlation and redundancy between adjacent pixels, which makes the traditional encryption schemes such as AES and DES cannot improve the effective encryption protection. The emergence of chaos theory breaks the limitations of traditional encryption schemes [1–5]. Chaotic image encryption usually goes through two stages of scrambling and diffusion, but some typical chaotic image encryption schemes are broken or threatened with the update of various decryption methods. Therefore, researchers actively explore the use of the hyperchaotic maps, combination of chaotic maps, graph theory, quantum communication, and cross-disciplinary technology to design the more effective image encryption schemes [6–13]. Among them, the application of DNA sequence and DNA computing in image encryption has become a hot research subject [14–19]. At present, the technology of information coding, reading and writing with DNA molecule as storage medium, and information hiding and encryption techniques based on diverse DNA structures and reactions are becoming increasingly available [20–24]. But the single use of DNA encryption technology for information encryption requires complex biological experiments to complete, which undoubtedly increases the cost of information encryption. The combination of chaotic maps and DNA computing can not only improve the effect of encryption, but also save the cost of experiment. In recent years, DNA coding, DNA addition and subtraction, DNA subsequence operation, and DNA deletion and insertion have become an important part of image encryption [25–29]. However, the diversity of DNA reactions and structures is rarely addressed in image encryption schemes [30].

This paper aims to apply more DNA reactions to image encryption schemes to enrich image encryption methods. We propose a double-layer image encryption scheme by combining DNA strand displacement (DSD) with chaotic maps. The emphasis of this paper is on the construction of new encryption rules based on DSD. At first, Lorenz chaotic map and Lorenz hyperchaotic map are used for routine scrambling and diffusion of the image, and then DNA coding and DSD-based encryption rules are used for secondary encryption. Simulation results show that the proposed double-layer image encryption scheme based on chaotic maps and DSD has better encryption effect.

2. Materials and Methods

2.1. Lorenz Maps

2.1.1. Lorenz Chaotic Map.

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

where the letters a, b, and c in equation (1) are parameters of the Lorenz chaotic map. When the parameters $a = 10$, $b = 8/3$, and $c = 28$, Lorenz map is in chaotic state and can generate three chaotic sequences. Figure 1 is the attractor graph of the Lorenz map. The four-order Runge–Kutta method is used to solve Lorenz equation.

2.1.2. Lorenz Hyperchaotic Map.

$$\begin{cases} \dot{x} = a(y - x) + w, \\ \dot{y} = cx - y - xz, \\ \dot{z} = xy - bz, \\ \dot{w} = -yz + rw, \end{cases} \tag{2}$$

when the parameters $a = 10$, $b = 8/3$, $c = 28$, and $-1.52 \leq r \leq -0.06$, Lorenz hyperchaotic map is in chaotic state. Figure 2 is the phase diagram of Lorenz hyperchaotic map with $r = -1$.

2.2. DNA Encoding Rules and DSD. DNA Encoding. DNA contain four bases: A (adenine), T (thymine), C (cytosine), and G (guanine), which strictly follow the Watson–Crick base complementary pairing principle; that is, A and T are complementary; G and C are complementary [14]. T, A, C, and G can be used to encode binary numbers, and there are eight such coding rules due to the need to satisfy the base complementary pairing principle, as shown in Table 1. For example, if a decimal number "200" is converted to the 8-bit binary sequence "11001000," and binary sequence is encoded using rule 2; the sequence "TAGA" can be obtained. Similarly, if the above sequence is decoded using rule 2, the 8-bit binary sequence "11001000" can be obtained, and the two processes are completely reversible. But the correct binary sequence could not be obtained using the other seven DNA coding rules to decode the sequence. These eight coding rules are themselves the form of encryption, regardless of the DNA computing or operation.

DSD. DSD is a DNA hybridization reaction through toehold-mediated branch migration. A long, single-stranded DNA that is fully complementary to the substrate is used as input and is connected to the dangling toehold domain in the prehybridized partially complementary DNA substrate, and then the DSD is triggered. Unlike most DNA-based reactions, DSD is diverse and can be directed either from the 5' terminal toehold of the substrate or from the 3' terminal toehold, as shown in Figures 3(a) and 3(b). In addition, DSD is cascaded. The input and output of DSD are single-strand DNA, and the single-strand output can be used as the input of the next cascade, as shown in Figure 3(c).

3. Results and Discussion

3.1. Scheme Description. The encryption scheme is divided into two parts: encryption at the level of chaotic maps and encryption at the level of DSD. At the level of chaos, Lorenz hyperchaotic map and Lorenz chaotic map are used to perform pixel position scrambling and XOR diffusion, respectively. At the level of DSD, the diversity of DSD is used to form different DSD-based encryption rules. Figure 4 is the encryption flowchart. The encryption steps are as follows:

Step 1. A gray image T of size $M \times N$ is the plaintext image.

Step 2. A group values of Lorenz hyperchaotic map's initial values x_0, y_0, z_0, w_0 are chosen as the keys, and the hyperchaotic map equations are iterated by the fourth-order Runge–Kutta method for $M \times N + t$ times. The effect of chaos is enhanced by removing the first t iterations. Starting from $t + 1$, after 3000 iterations, the chaotic state x_0 is slightly perturbed by equation (3), and h is the step length; then, we can get a pseudorandom chaotic sequence S of length $M \times N$. The pseudorandom sequences X are obtained by normalizing the pseudorandom sequences S to the integer interval $[1, M \times N]$. The repeated pseudorandom numbers in the sequences X retain only the first occurrence, while the numbers in the integer interval $[1, M \times N]$ that do not appear in the sequences X are arranged at the end of the sequences X in ascending numerical order from small to large, and there are no duplicate values in sequences X.

$$x_0 = x_0 + h * \sin(y_0). \tag{3}$$

Step 3. The original plaintext image matrix $T(M, N)$ is scrambled by sequences X and equation (4), and the resulting matrix is denoted as $A(M, N)$.

$$\begin{aligned} &t = T(X(i)); T(X(i)) = T(X(M * N - i + 1)); \\ &T(X(M * N - i + 1)) = t. \end{aligned} \tag{4}$$

Step 4. A group values of Lorenz chaotic map's initial values x_0, y_0, z_0 are chosen as the keys, and the chaotic map equations are iterated by fourth-order Runge–Kutta method

RETRACTED

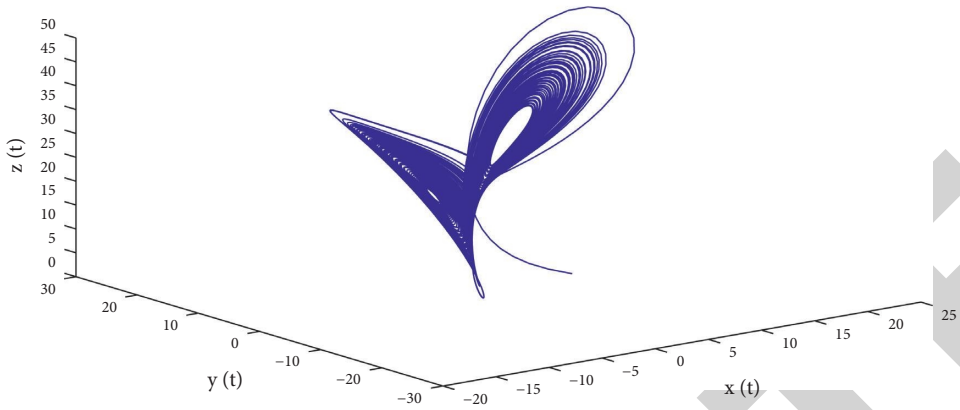
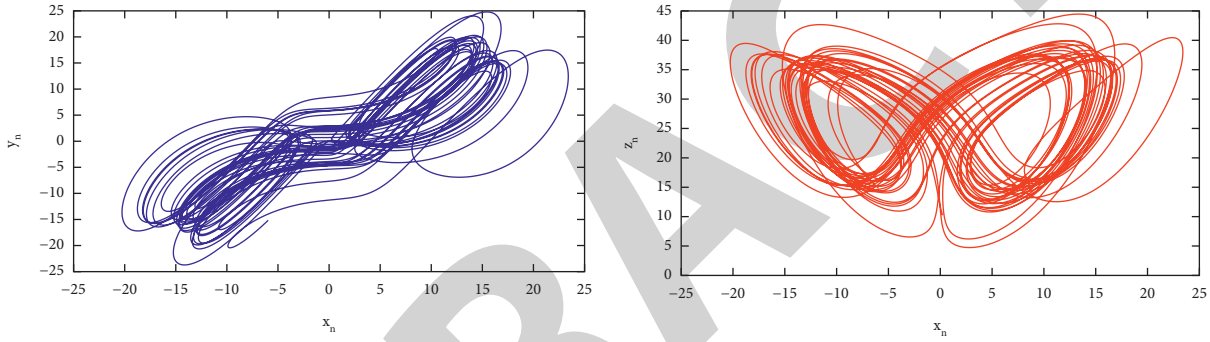


Figure 1: The attractor graph of the Lorenz chaotic map.



(a) (b)

Figure 2: The phase diagram of Lorenz hyperchaotic map with $r = -1$.

Table 1: DNA encoding rules.

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

for $M \times N + t$ times. Three pseudorandom chaotic sequences Lx, Ly, and Lz with length of $M \times N$ can be obtained by removing the previous t iterations. Lx, Ly, and Lz are mapped to integer interval [0, 255] and the three pseudorandom sequences are reconstructed into the matrices with the size of $M \times N$, denoted as Lxm, Lym, and Lzm. The matrix A (M, N) in Step 3 is treated as B (M, N) by XOR operation with the matrix Lxm.

Step 5. The matrix B (M, N) is first transformed into the binary matrix and transformed into DNA matrix C (each location in the DNA sequence matrix C is no longer a decimal number, but four bases). The DNA sequence matrix C is partitioned by columns, one block for every four columns, and we get the DNA sequence matrices $D_1, D_2, D_3, \ldots, D_{N/4}$. The size of the matrix D_i $(i = 1 \sim (N/4))$ is $M \times (N/4)$, and it has four bases at each position, so each row of the matrix D_i is a 16 nt DNA sequence. Set the direction of DNA sequences from left to right to be 5′ terminal to 3′ terminal. The principle of encrypting the DNA sequence by DSD is as follows: suppose that the DNA sequence of a row in matrix D_i, from left to right, is TCTCACCATTCCCACG, and is denoted as the original DNA sequence: 5′-TCTCACCATTCCCACG-3′. When DSD-Figure 3(a) is chosen for encryption, the DNA substrate involved in the reaction can be used as the key, but not all sequences on the substrate can be chosen at random to be the key. In Figure 5, the original DNA sequence determines the sequence of toehold (green, the sequence from left to right is AGAG) and complementary regions (blue region, the sequence in the blue region below is TGGTAAGGGTGC, and the sequence in the blue region above is ACCATTCCCACG) on the substrate, and the length of the toehold is set at 4 nt. The red region of the substrate is the core region of the key, which is the same length as the toehold and is 4 nt, to ensure that the displaced DNA sequence remains the same length as the original DNA sequence. The four bases in the red region have 256 possibilities. The sequences of red region in Figure 5 are AGCT. The original sequence 5′-TCTCACCATTCCCACG-3′ is encrypted to 5′-ACCATTCCCACGAGCT-3′. We refer to the encryption rule generated based on this type of DSD as DSD-rule a, as shown in Table 2.

RETRACTED

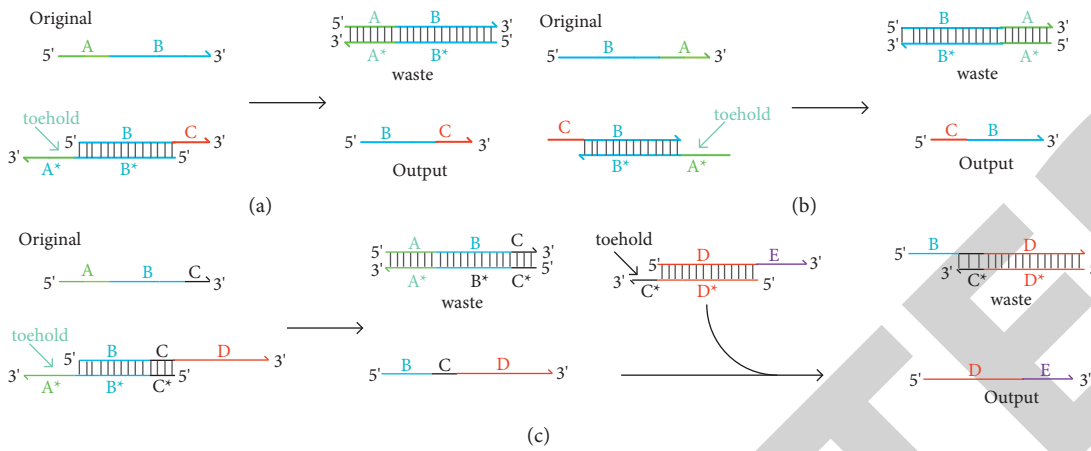


Figure 3: Basic reaction principle of DSD. (a) DSD starts at the 3' terminal toehold of the substrate. (b) DSD starts at the 5' terminal toehold of the substrate. (c) Cascade DSD.

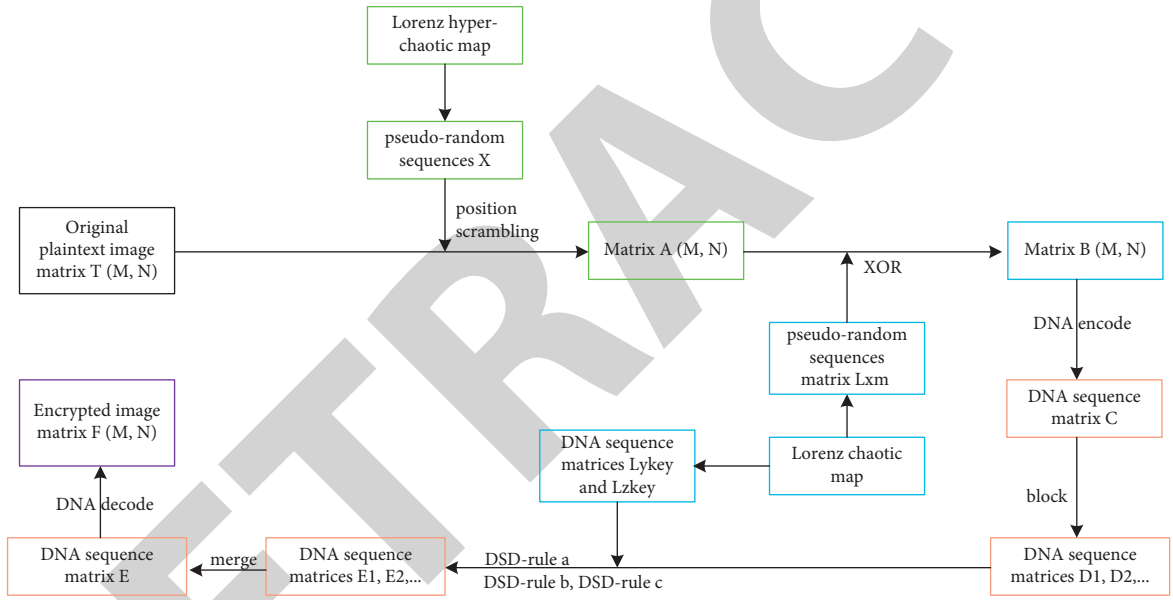


Figure 4: Flowchart of the proposed scheme.

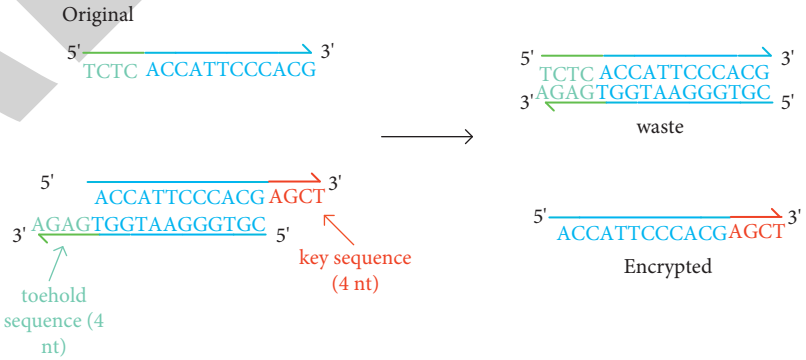


Figure 5: The DNA sequence encryption principle of DSD-rule a.

When DSD in Figure 3(b) is chosen for encryption, it is similar to DSD-rule a. In Figure 6, the original DNA sequence determines the sequence of the toehold (green, the sequence from left to right is CACG) and complementary regions (blue region, the sequence in the blue region below is AGAGTGGTAAGG, and the sequence in the blue region

RETRACTED

Table 2: DSD-based encryption rules.

Original DNA sequence	DSD-rule	Encrypted DNA sequence
TCTCACCATTCCCACG	DSD-rule a	ACCATTCCCACG ****
TCTCACCATTCCCACG	DSD-rule b	**** TCTCACCATTCC
TCTCACCATTCCCACG	DSD-rule c	**********

above is TCTCACCATTCC) on the substrate. The red region of the substrate is the core region of the key, and the sequence assigned to the red region in Figure 6 is AGCT. The original sequence is encrypted to 5′-AGCTTCTCAC-CATTCC-3′. We refer to the encryption rule generated based on this type of DSD as DSD-rule b, as shown in Table 2.

When DSD in Figure 3(c) is chosen for encryption, the two DNA substrates involved in the reaction each carry part of the key. As shown in Figure 7, the toehold on the first substrate (green region) is 6 nt in length and the sequence is AGAGTG. The red region is the core region of the key, and its length is 10 nt, there are 4^{10} possibilities. The original DNA sequence strand reacts with the first DNA substrate and the displaced single strand continues DSD with the second substrate. The toehold on the second substrate (black region) is 3 nt in length and the sequence is TGC. The purple region is the core region of the key, and its length is 6 nt, there are 4^6 possibilities. The original sequence is encrypted to 5'-AGCTTGGAGGTTAGGC-3'. We refer to the encryption rule generated based on this type of DSD as DSD-rule c, as shown in Table 2.

In DSD-based encryption rules, the keys of DSD-rule a and DSD-rule b are composed of four bases, and the key of DSD-rule c is composed of 16 bases. Due to the pseudo-random of chaotic sequences, we use the matrices *Lym* and *Lzm* in Step 4 to generate the keys required by DSD-based encryption rules. The matrices *Lym* and *Lzm* are first transformed into the 8-bit binary matrices and transformed into the DNA sequence matrices Lykey and Lzkey with the size of $M \times N$. Each location in matrix Lykey contains four bases, so there are $M \times N$ keys required for the DSD-rule a and DSD-rule b in matrix Lykey. Each location in matrix Lzkey also contains four bases, so there are $(M \times N/4)$ keys required for the DSD-rule c in matrix Lzkey. For any matrix $D_i\,(i = 1 \sim (N/4))$, there are three types of DSD-based encryption rules that it can select. In order to realize encryption more quickly, matrices $D_1, D_4, \ldots, D_{1+3n}$ (n is natural number, and $1 + 3n \in [1, (N/4)]$) are encrypted by DSD-rule a, matrices $D_2, D_5, \ldots, D_{2+3n}$ (n is natural number, and $2 + 3n \in [2, (N/4)]$) are encrypted by DSD-rule b, and matrices $D_3, D_6, \ldots, D_{3+3n}$ (n is natural number, and $3 + 3n \in [3, (N/4)]$) are encrypted by DSD-rule c.

For matrices $D_1, D_4, \ldots, D_{1+3n}$, delete the first column of each block matrix according to DSD-rule a, the original matrices with 4 columns in row M are changed into 3 columns in row M, and the first n columns of matrix Lykey are inserted into the fourth column of each block matrix to get the encrypted block matrices $E_1, E_4, \ldots, E_{1+3n}$. For matrices $D_2, D_5, \ldots, D_{2+3n}$, delete the fourth column of each block matrix according to DSD-rule b, and the $n + 1$ column to $n + 3n$ column of matrix Lykey are inserted into the first column of each block matrix to get the encrypted block matrices $E_2, E_5, \ldots, E_{2+3n}$. For matrices $D_3, D_6, \ldots, D_{3+3n}$, they are all displaced by the first $3n$ columns of matrix Lzkey according to DSD-rule c, and the encrypted block matrices $E_3, E_6, \ldots, E_{3+3n}$ are obtained.

Step 6. The encrypted block matrices $E_i\,(i = 1 \sim (N/4))$ obtained in Step 5 are merged into DNA sequence matrix E of size $M \times N$.

Step 7. A random DNA coding rule is selected to decode the DNA sequence matrix E, and then it is transformed into the decimal matrix F, and finally the encrypted image is obtained.

3.2. Simulation Results. A 256×256 gray image "Lena" is the plaintext image, and the above chaotic maps and DSD-based encryption rules are used to encrypt it. The initial values x_0, y_0, z_0, and w_0 of Lorenz hyperchaotic map are set to 1.1, 2.2, 3.3, and 4.4, and x_0, y_0, z_0 of Lorenz chaotic map are set to 10, 1, and 0. The simulation results are realized by MATLAB R2014a; the operating system of computer is Windows 10, as shown in Figure 8. The encryption steps are reversible. In the DSD-based encryption rules, the encryption keys are provided by matrices Lykey and Lzkey. The decryption keys are the complement sequences of the toehold. From the visual effect, the encrypted image is not easy to get information.

3.3. Security Analysis. Key Space. In general, a key space larger than 2^{100} can resist brute-force attack. The key space is the total number of keys used in an encryption scheme. The keys in this paper consist of two parts: (1) at the level of chaos: 7 chaotic keys, the key space is $(10^{14})^7 = 10^{98}$; (2) at the level of DNA. In Step 5, matrix B is converted to DNA sequence matrix C using a DNA encoding rule, while matrices *Lym* and *Lzm* use a DNA encoding rule when convert to DNA sequence matrices Lykey and Lzkey, respectively. In Step 7, the DNA sequence matrix E uses a DNA coding rule when converting to the decimal matrix F. As a result, the DNA coding rules are used four times during the whole encryption process. In Step 5, there are three DSD-based encryption rules that any block matrix $D_i\,(i = 1 \sim (N/4))$ can choose. When the size of the plaintext image is 256×256, it has 3^{64} possibilities. The key space at the DNA level is $8 \times 8 \times 8 \times 8 \times 3^{64} \approx 1.4 \times 10^{34}$. Thus, the total key space is 1.4×10^{132}, which is much larger than 2^{100}, and this key space is large enough to resist brute-force attack.

Sensitivity Analysis of Key. Chaotic maps are sensitive to initial values. For example, when the initial value x_0 of Lorenz map changes from 10 to 10.0000000000001, the decryption result is shown in Figure 9(a). z_0 changes from 0 to 0.0000000000001, the decryption result is shown in Figure 9(b). Based on these results, we can find that the keys of the proposed encryption scheme are sensitive enough to resist exhausting attack.

RETRACTED

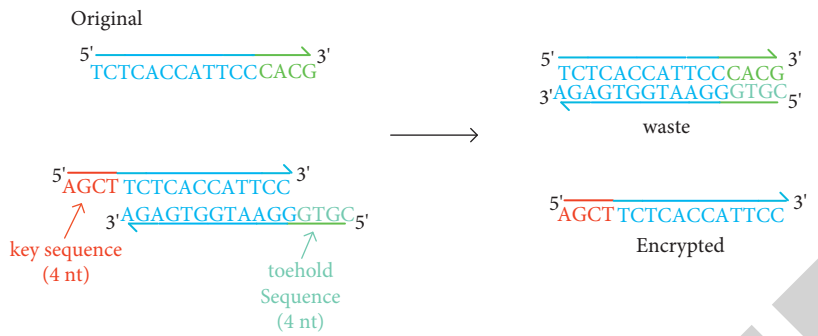


Figure 6: The DNA sequence encryption principle of DSD-rule b.

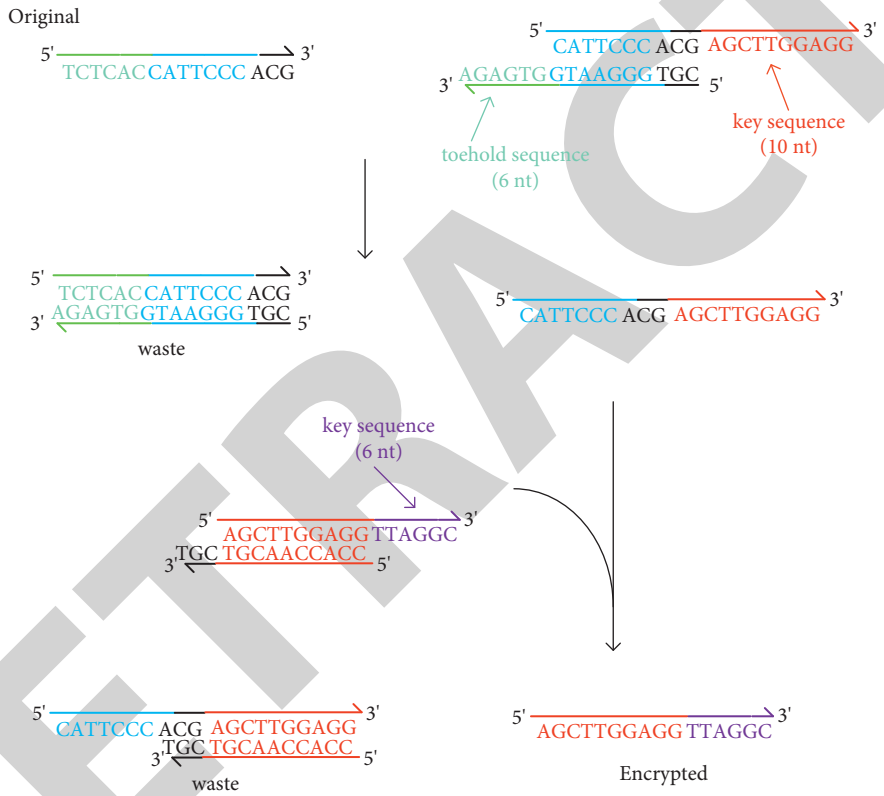
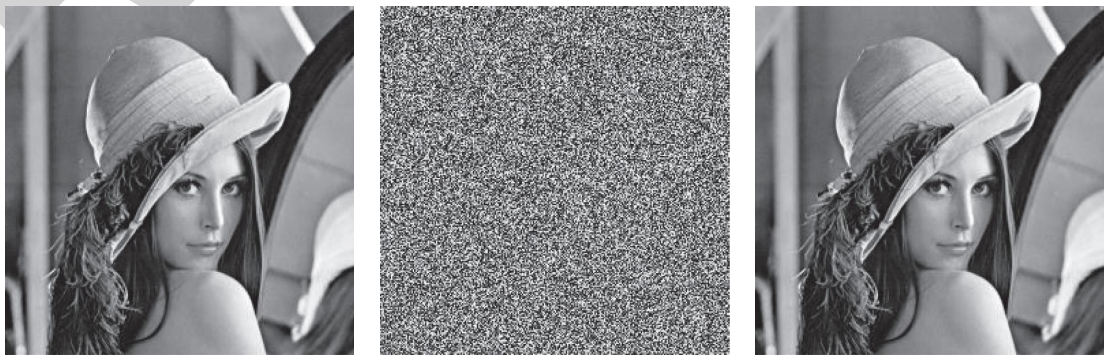


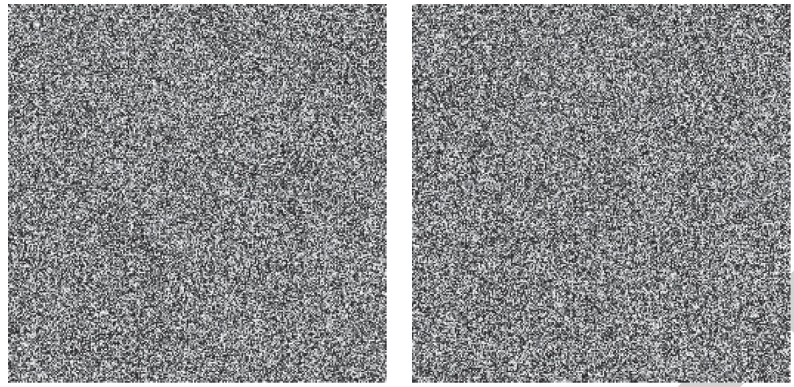
Figure 7: The DNA sequence encryption principle of DSD-rule c.



(a) (b) (c)

Figure 8: Simulation results. (a) Plaintext image "Lena" (256 × 256). (b) Encrypted. (c) Decrypted.

RETRACTED



(a) (b)

Figure 9: Sensitivity analysis. (a) The decrypted image when x_0 of Lorenz map changes from 10 to 10.0000000000001. (b) The decrypted image when z_0 of Lorenz map changes from 0 to 0.0000000000001.

The Gray Histogram Analysis. Histogram analysis is a method to evaluate the ability of proposed scheme to resist statistical attack. If the histogram distribution of the encrypted image is not uniform, the attacker can obtain the statistical features of the encrypted image through statistical analysis and then decrypt the image. Figure 10 are the gray histograms of plaintext and encrypted images. Comparing these two histograms, the histogram of encrypted image is distributed more uniform.

Correlation Coefficient Analysis. Another important approach to resist statistical analysis is to eliminate the correlation in plaintext image. 10,000 pairs of adjacent pixel values are randomly selected in each direction of plaintext and encrypted images, and equation (5) is used to calculate the correlation, the results are shown in Figure 11 and Table 3. Compared with [15], [18], [26], and [28], our encryption scheme is more effective in removing correlation.

$$\begin{cases} r_{xy} = \dfrac{\operatorname{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \\ E(x) = \dfrac{1}{N} \sum_{i=1}^{N} x_i \\ D(x) = \dfrac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \\ \operatorname{cov}(x, y) = \dfrac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \end{cases}. \quad (5)$$

Information Entropy. Information entropy is used to evaluate the randomness of information:

$$H(m) = -\sum_{i=1}^{n} P(m_i) \log P(m_i), \quad (6)$$

where m_i is the ith gray value of L level gray image and $P(m_i)$ is the emergence probability of m_i, so $\sum_{i=1}^{L} P(m_i) = 1$. The ideal value of information entropy approaches 8. The information entropy of encrypted image is 7.9971, as shown in Table 4. Therefore, our encryption scheme is effective.

Differential Attack Analysis. Differential attack is a common attack in which attackers make small changes to the image and encrypts it. By comparing two encrypted images to find out the difference, it can help the attackers qualitatively observe the difference between the two images. NPCR and UACI are used as two criterions to evaluate the ability to resist differential attack. They can be calculated by the following equation:

$$\begin{cases} \text{NPCR}(P_1, P_2) = \dfrac{\sum_{i=1}^{M} \sum_{i=1}^{N} |\text{Sign}(P_1(i, j) - P_2(i, j))|}{M \times N} \times 100\% \\ \text{UACI}(P_1, P_2) = \dfrac{\sum_{i=1}^{M} \sum_{i=1}^{N} |\text{Sign}(P_1(i, j) - P_2(i, j))|}{255 \times M \times N} \times 100\% \\ \text{Sign}(x) = \begin{cases} 1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases} \end{cases}, \quad (7)$$

where the size of images P_1 and P_2 is $M \times N$. The ideal value of NPCR is 99.6094% and UACI is 33.4635%. NPCR and UACI between Lena (Figure 8(a)) and encrypted image (Figure 8(b)) are shown in Table 5. The results show that the proposed scheme can resist differential attack.

RETRACTED

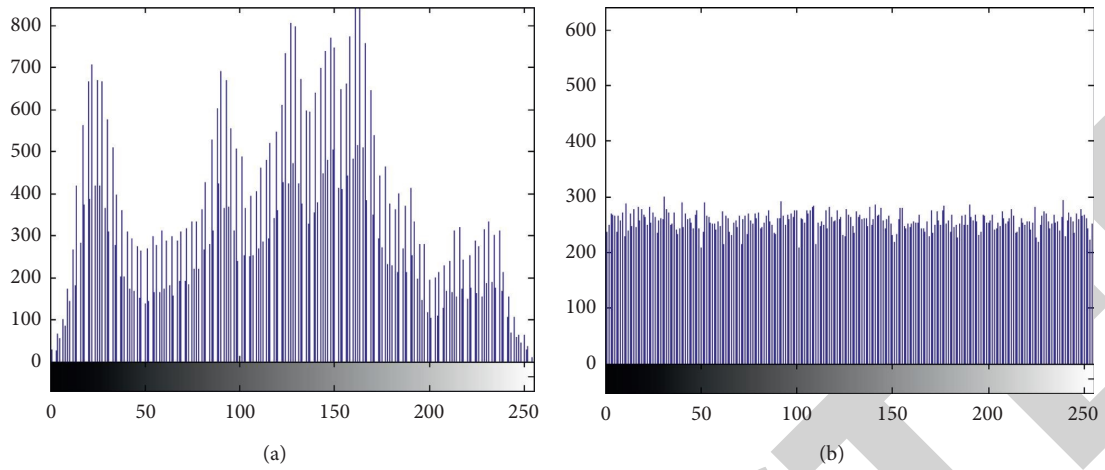


Figure 10: The gray histogram. (a) The gray histogram of the plaintext image "Lena." (b) The gray histogram of the encrypted image.

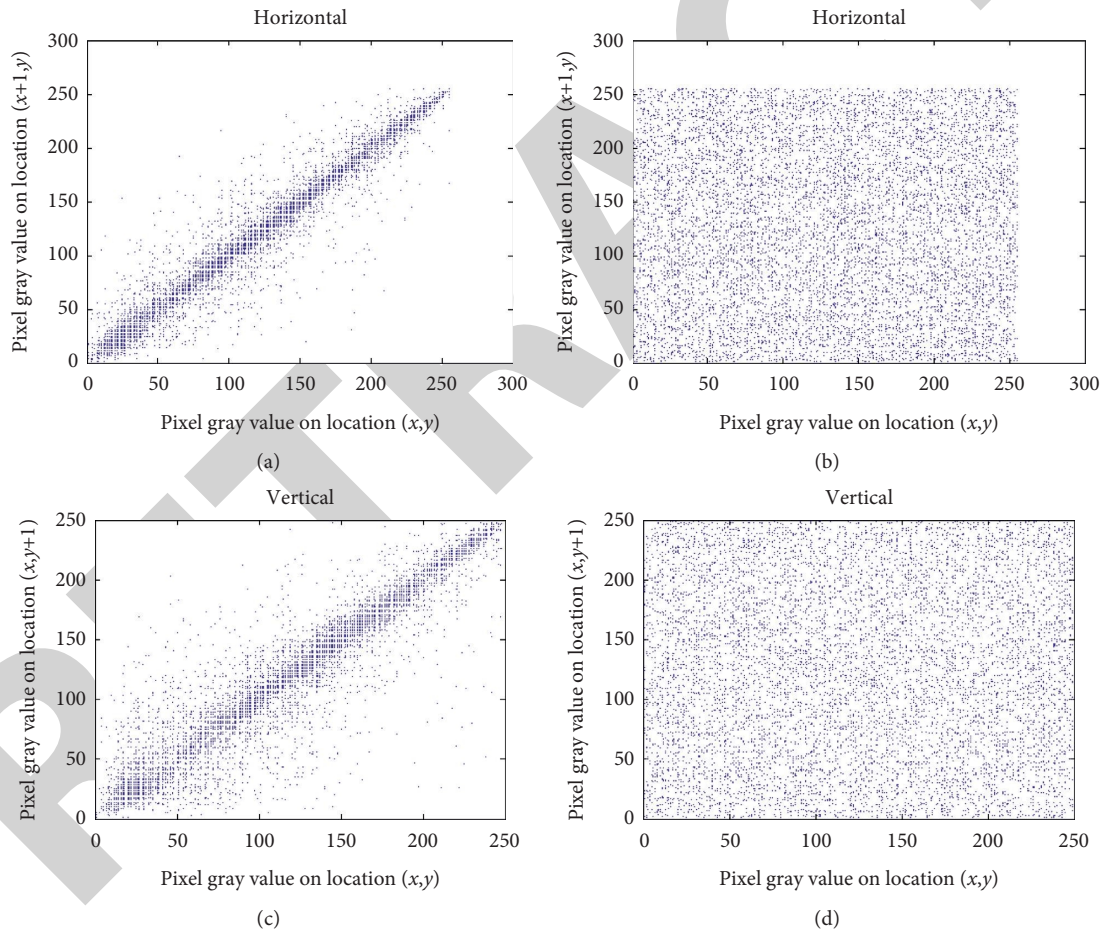


Figure 11: Continued.

RETRACTED

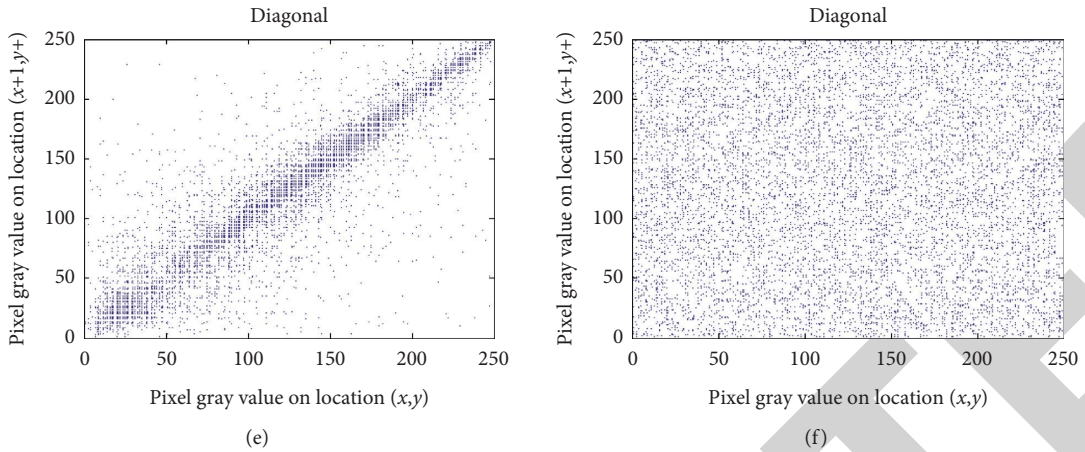


Figure 11: Correlation of adjacent pixels in plaintext and encrypted images.

Table 3: Correlation of adjacent pixels in plaintext and encrypted images.

Correlation	Original	Proposed	Ref. [15]	Ref. [18]	Ref. [26]	Ref. [28]
Horizontal	0.9719	−0.0002	0.0004	−0.0021	0.0024	−0.0077
Vertical	0.9444	0.0052	0.0021	0.0009	0.0012	0.0002
Diagonal	0.9163	0.0018	−0.0038	0.0003	0.0016	−0.0055

Table 4: Information entropy.

Information entropy	Proposed	Ref. [15]	Ref. [18]	Ref. [26]
Plain image	7.3740	—	—	—
Encrypted image	7.9971	7.9874	7.9971	7.9970

Table 5: NPCR and UACI.

Image	NPCR (%)	UACI (%)
Figures 8(a) and 8(b)	99.6475	31.2188
Ref. [15]	99.6017	28.1370
Ref. [25]	99.6100	38.0000

4. Conclusions

The types and forms of DNA reactions are diverse. In order to introduce more DNA-based operations into image encryption to enrich image encryption methods, we propose three DSD-based encryption rules according to the diversity of DSD, and a double-layer image encryption scheme based on chaotic maps and DSD is proposed. The results show that the proposed scheme has good encryption effect. Our next work is expected to propose more DNA-level sequence encryption rules based on DNA reactions and more encryption methods for image encryption.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 62072296).

References

[1] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences*, vol. 20, no. 2, pp. 130–141, 1963.
[2] D. D. Wheeler, "Problems with chaotic cryptosystems," *Cryptologia*, vol. 13, no. 3, pp. 243–250, 1989.
[3] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcat. Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.
[4] C. Park and L. L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.
[5] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on Josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018.
[6] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "An image encryption algorithm based on compound homogeneous

RETRACTED

hyper-chaotic system," *Nonlinear Dynamics*, vol. 89, no. 1, pp. 61–79, 2017.

[7] J.-B. Liu, X.-F. Pan, and F.-T. Hu, "The {1}-inverse of the Laplacian of subdivision-vertex and subdivision-edge coronae with applications," *Linear and Multilinear Algebra*, vol. 65, no. 1, pp. 178–191, 2017.

[8] J. B. Liu, S. Wang, C. Wang, and S. Hayat, "Further results on computation of topological indices of certain networks," *IET Control Theory & Applications*, vol. 11, no. 13, pp. 2065–2071, 2017.

[9] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.

[10] J. B. Liu, J. Zhao, and Z. X. Zhu, "On the number of spanning trees and normalized Laplacian of linear octagonal-quadrilateral networks," *International Journal of Quantum Chemistry*, vol. 119, no. 17, Article ID e25971, 2019.

[11] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-based image encryption scheme," *Information Sciences*, vol. 520, pp. 130–141, 2020.

[12] J. B. Liu, "Network coherence analysis on a family of nested weighted n-polygon networks," *Fractals*, vol. 29, no. 8, Article ID 2150260, 2021.

[13] J. B. Liu, X. B. Peng, and S. Hayat, "Topological index analysis of a class of networks analogous to alicyclic hydrocarbons and their derivatives," *International Journal of Quantum Chemistry*, vol. 122, no. 2, Article ID e26827, 2022.

[14] J. D. Watson and F. H. C. Crick, "Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid," *Nature*, vol. 171, no. 4356, pp. 737-738, 1953.

[15] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.

[16] X.-Y. Wang, Y.-Q. Zhang, and Y.-Y. Zhao, "A novel image encryption scheme based on 2-D logistic map and DNA sequence operations," *Nonlinear Dynamics*, vol. 82, no. 3, pp. 1269–1280, 2015.

[17] A. Alghafis, F. Firdousi, M. Khan, S. I. Batool, and M. Amin, "An efficient image encryption scheme based on chaotic and Deoxyribonucleic acid sequencing," *Mathematics and Computers in Simulation*, vol. 177, pp. 441–466, 2020.

[18] X. Wang, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Optics and Lasers in Engineering*, vol. 125, Article ID 105851, 2020.

[19] X. Y. Wang and Y. P. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Optics and Lasers in Engineering*, vol. 137, no. 11, Article ID 106393, 2021.

[20] Y. Zhang, F Wang, J Chao et al., "DNA origami cryptography for secure communication," *Nature Communications*, vol. 10, pp. 5469–5478, 2019.

[21] K. J. Tomek, K. Volkel, A. Simpson et al., "Driving the scalability of DNA-based information storage systems," *ACS Synthetic Biology*, vol. 8, no. 6, pp. 1241–1248, 2019.

[22] K. Chen, J. Zhu, F. Bošković, and U. F. Keyser, "Nanopore-based DNA hard Drives for rewritable and secure data storage," *Nano Letters*, vol. 20, no. 5, pp. 3754–3760, 2020.

[23] S. Fan, J. Cheng, Y. Liu et al., "Proximity-induced pattern operations in reconfigurable DNA origami domino array," *Journal of the American Chemical Society*, vol. 142, no. 34, pp. 14566–14573, 2020.

[24] K. L. Berk, S. M. Blum, V. L. Funk et al., "Rapid visual authentication based on DNA strand displacement," *ACS Applied Materials & Interfaces*, vol. 13, no. 16, pp. 19476–19486, 2021.

[25] Q. Zhang, L. Guo, and X. P. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11-12, pp. 2028–2035, 2010.

[26] Q. Zhang and X. Wei, "A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system," *Optik*, vol. 124, no. 23, pp. 6276–6281, 2013.

[27] Q. Zhang, L. Liu, and X. Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps," *AEU-International Journal of Electronics and Communications*, vol. 68, no. 3, pp. 186–192, 2014.

[28] T. Hu, Y. Liu, L.-H. Gong, S.-F. Guo, and H.-M Yuan, "Chaotic image cryptosystem using DNA deletion and DNA insertion," *Signal Processing*, vol. 134, pp. 234–243, 2017.

[29] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the feistel network and dynamic DNA encoding," *IEEE Photonice Journal*, vol. 10, no. 4, Article ID 3901014, 2018.

[30] C. Zou, X. Wei, Q. Zhang, C. Zhou, and S. Zhou, "Encryption algorithm based on DNA strand displacement and DNA sequence operation," *IEEE Transactions on NanoBioscience*, vol. 20, no. 2, pp. 223–234, 2021.

RETRACTED