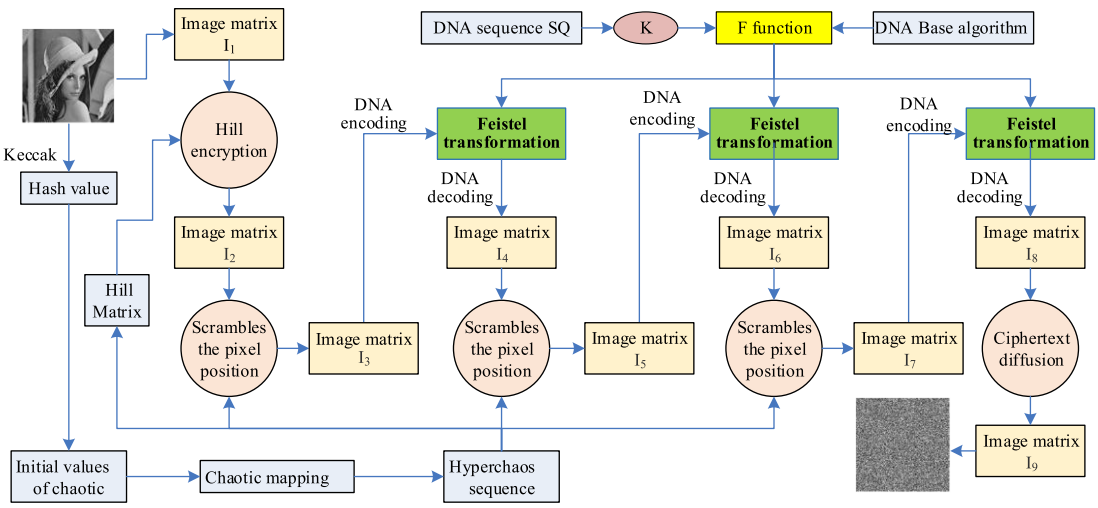
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding

Volume 10, Number 4, August 2018

Xuncai Zhang
Zheng Zhou
Ying Niu



DOI: 10.1109/JPHOT.2018.2859257
1943-0655 © 2018 IEEE

IEEE photonics SOCIETY

IEEE

An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding

Xuncai Zhang, Zheng Zhou, and Ying Niu

School of Electrics and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China

DOI:10.1109/JPHOT.2018.2859257

Manuscript received May 31, 2018; revised July 13, 2018; accepted July 18, 2018. Date of publication July 24, 2018; date of current version August 6, 2018. This work was supported in part by the National Natural Science Foundation of China under Grants 61602424, 61472371, 61572446, and 61472372, in part by the Plan for Scientific Innovation Talent of Henan Province under Grant 174100510009, in part by the Program for Science and Technology Innovation Talents in Universities of Henan Province under Grant 15HASTIT019, and in part by the Key Scientific Research Projects of Henan High Educational Institution under Grant 18A510020. Corresponding author: Xuncai Zhang (e-mail: zhangxuncai@pku.edu.cn).

Abstract: Based on the Feistel network and dynamic deoxyribonucleic acid (DNA) encoding technology, an image encryption method is proposed using the "permutation–diffusion–scrambling" structure. First, the SHA-3 algorithm is used to calculate the hash value of the plaintext image as the initial value of the hyperchaotic system, and the chaos-generated sequence is used to generate the Hill cipher matrix to replace the image pixel. Second, the DNA sequence operation is used as the *F* function of the Feistel network. The DNA sequence database is used as the key *K* of Feistel network, and the image pixel value diffusion is realized by the Feistel network. Finally, further diffusion is carried out through the ciphertext feedback and through the ciphertext confusion and diffusion of three rounds of "chaotic scrambling-DNA encoding-Feistel transformation-DNA decoding," making the ciphertext more random and resistant to attacks and ensuring that the encrypted ciphertext is more secure. The experimental results show that the proposed method can effectively encrypt the image and has prominent characteristics, such as strong plaintext sensitivity, a large key space, and excellent ciphertext statistical properties.

Index Terms: Image encryption, Feistel network, dynamic DNA encoding, Hill matrix, chaotic sequence.

1. Introduction

Information security is a major issue affecting national security, social stability, economic development and personal property. Measures must be taken to ensure the integrity, availability, confidentiality and reliability of information resources. A digital image is one common information communication method that has features that are intuitive, easy to recognize, vivid, and highly redundant and have a large data capacity, among other features. Due to the large amount of data and high redundancy of digital images, the existing classical encryption methods, such as DES, AES, Feistel and RSA, do not satisfy the needs of image encryption because of their low encryption efficiency and low security [1].

With the development of deoxyribonucleic acid (DNA) molecular computing technology and biotechnology research, scientists have found that the sequence of nucleic acids has a natural

quaternary combination, similar to the binary system formed by the semiconductor's on and off [2]. Therefore, the information can be stored and calculated using the permutation and combination of nucleotides [3], [4]. The huge parallelism, ultrahigh storage density and ultra-low energy consumption of DNA are being developed for molecular computing, data storage, cryptography and other fields, which may eventually lead to the birth of new computers, new data storage and new cryptography systems, triggering a new information revolution [5]–[8]. In 1999, Gehani *et al.* proposed a one-time pad (OTP) mechanism based on DNA and presented two kinds of OTP cryptography schemes of the substitution method and XOR method [9]. In 2003, Chen *et al.* constructed a cryptosystem based on DNA molecular sequences [10]. In 2005, Kazuo *et al.* used DNA to solve the problem of key distribution [11]. In 2009, Mousa *et al.* designed an information hiding scheme using a contrast mapping method to embed ciphertext information into any part of a nucleic acid sequence without changing the function of nucleic acid [12]. In short, the limitations of existing biotechnology and computing technologies provide multiple security guarantees for existing DNA encryption methods due to the high parallel computing power of DNA and its massive data storage capacity. However, these DNA encryption algorithms are mostly used to encrypt text information, and it is difficult for image information to be encrypted directly. In recent years, combined with the dual advantage of the DNA molecule and traditional ciphers, an image encryption algorithm based on DNA molecules and ciphers was presented. In 2014, Liu *et al.* proposed a RGB image encryption algorithm based on DNA encoding and chaos map [13]. In 2015, Wang *et al.* presented an image encryption algorithm based on 2D logistic mapping and DNA operations [14]. In 2017, Chai *et al.* presented an image encryption algorithm that is based on chaos combined with DNA operations [15]. In the same year, we proposed a type of digital image encryption technology based on hyperchaos mapping and DNA sequence database arithmetic to realize a scrambling position transformation of image pixels and the spread of the pixel values [16]. These methods displace only the positions of the image pixels and change the gray value. However, the bit's position changes are smaller, and it is not able to achieve the purpose of true diffusion [17].

Therefore, a new image encryption scheme is proposed by analyzing the characteristics of the Feistel network and DNA encoding and combining the two organically. The method first constructs the Hill encryption matrix using the hyper-chaotic sequences produced by the chaotic system and permutes the image, then uses the chaotic index sequence, the Feistel network and the dynamic DNA encoding technology to scramble and diffuse the image, and further enhances the confusion and diffusion properties of the method through the ciphertext feedback.

The target of this paper is to guarantee more security over conventional asymmetric cryptosystems like ECC, ElGamal and RSA etc using the concept of DNA. It is not intended to adopt the real DNA to carry out the process of cryptographic; instead, a novel image encryption method based on the Feistel network and dynamic DNA encoding is proposed. The method uses SHA-3 algorithm to calculate the hash value of the plaintext image as the initial value of the hyper-chaotic system, and the chaos-generated sequence is applied to generate the Hill cipher matrix to replace the image pixel; then the DNA sequence operation is employed as the F function of the Feistel network and the image pixel value diffusion is realized by the Feistel network; finally, further diffusion is carried out through the ciphertext feedback and through the ciphertext confusion and diffusion of three rounds circulation. Thus the multifold security makes the method more efficient and can be utilized in data security transmission.

The remainder of the paper is organized as follows. Related works are given in Section 2 to discuss various categories of recent works. In Section 3, the Feistel network, DNA coding and sequence operations used in the proposed method are introduced. In Section 4, the encryption method is described. The experimental results and security analysis are presented in Section 5. Finally, this paper is concluded in Section 6.

2. Related Works

With the remarkable development of DNA computing, DNA cryptography has become a relatively new field of cryptography [18], [19], in which DNA is acted as an important carrier of genetic

information in organism and the modern biological technology serves as manipulation tool. The huge parallelism and ultrahigh storage intensity that are inherent in DNA molecules are exploited for all kinds of cryptographic purposes such as encryption, signature, authentication, and so on.

There are several DNA-based algorithms that have been practically applied. An example is a multi-level image encryption algorithm based on chaos and DNA coding. Zhang *et al.* [20]–[22] proposed an improved image encryption algorithm based on DNA coding and multi-chaotic mapping. The method using the hyper-chaotic system to scramble pixel positions and pixel values, carrying out pseudo DNA operations. Finally, the encrypted image is obtained by DNA decoding.

Another example is DNA-based on watermarking using the DNA cryptography algorithm [23]. Watermarks that are based on DNA sequences are utilized to identify the unauthorized use of genetically modified organism that are protected by patents. Existing DNA cryptographic and steganographic algorithms employ synthetic DNA sequences to retrieve binary information.

An approach presents the way in which DNA binary strands is used for steganography [24], which encrypts by hiding information to provide rapid encryption and decryption. It is shown that DNA steganography based on DNA binary strands is secure under the assumption that an interceptor has the same technological capabilities as sender and receiver of encrypted messages.

The combination of DNA cryptography and traditional cryptography, such as visual cryptography, elliptic curve cryptography and Hill cipher, is also one of the hotspots in DNA cryptography research. Visual cryptography proves to be more efficient than other cryptography techniques because it is simple and does not require any key management technique. Siyam *et al.* [25], [26] presents some application of visual cryptography and extended visual cryptography applicable to several public and private sectors where image security is essential to sustain. Moreover, a special scheme of visual cryptography for color image with a minor modification of existing extended visual cryptography has been demonstrated.

3. Fundamental Theory

3.1 Feistel Network

In 1988, Luby and Rackoff first proposed the method of constructing a pseudo random permutation by using the Feistel network [27], which can realize the full diffusion and confusion of encrypted data by alternately using two basic operations of substitute and permutation and has a better security and encryption efficiency. The Feistel cipher structure is a symmetric structure used in block ciphers as shown in Figure 1. Many traditional block ciphers have adopted the Feistel structure, including DES, FEAL, RC5 and so on. The Feistel structure is a typical iterative structure and is also a product form of cryptographic transformation, which fully realizes the diffusion and scramble and constitutes a very high-strength cryptosystem.

In the Feistel cryptography scheme, the plaintext block P is divided into the left and right parts, $P = (L_0, R_0)$: for every round i of the encryption process, here $i = 1, 2, \ldots, n$, a new left half part and right half part are generated according to the following rules:

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \end{cases} \tag{1}$$

Where $\oplus$ denotes bit XOR operation, F is the round function, and K_i is the sub-key of the ith round. The sub-key is derived from the key K and follows a specific key scheduling algorithm.

For the Feistel network structure, the function of the round function F in the encryption system is to diffuse the input bits into the output so that the plaintext information can be diffused to all the blocks. Each time the information is diffused into other sub-blocks, when the number of the encryption round is n, all the information diffuses into sub-blocks. Therefore, the core of its encryption is the selection of F functions. Different F functions follow the different encryption methods of the Feistel structure. A good F function is crucial to the encryption effect. Generally speaking, the F function needs to satisfy the following points: (1) Not required reversible: that is, the F function is not required to have an inverse function; (2) Nonlinear; (3) Confusion; (4) Diffusion; (5) Avalanche:

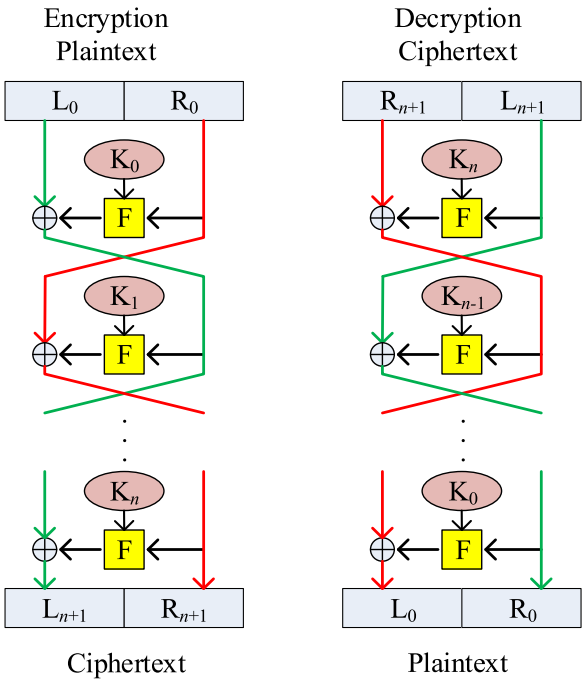


Figure 1. The Feistel network structure.

the avalanche enhancement of its encrypted effect as the number of rounds is increased; and (6) Bit independence: the encryption result of a bit does not depend on other bits. In this paper, the DNA sequence operation in DNA computing is used as the round function of the cryptographic transformation to satisfy the requirements of the *F* function, which is mainly characterized by good cryptography.

3.2 DNA Coding and Sequence Operations

The DNA molecule is composed of four DNA nucleotides, including adenine (A), cytosine (C), guanine (G), and thymine (T). For two single-stranded DNA molecules, a stable DNA molecule can be formed by hydrogen bonds between the nucleotides. The chemical structure of the base determines the principle of complementary base pairing, and it is also known as the Watson-Crick base pairing principle. In other words, A and T are paired by two hydrogen bonds, and G and C are paired by three hydrogen bonds. The natural combination is quaternary, similar to the binary semiconductor formed by on and off. Therefore, the information is stored and calculated using the permutations and combinations of the bases. The nucleic acid database is a database of all known nucleic acid information sets. It contains nucleotide sequences, single nucleotide polymorphisms, structure, properties, and related descriptions. The ID number of a sequence in a database is called the sequence code, which is unique and permanent. With the rapid development of sequencing technology, the size of the nucleic acid database is growing exponentially, with an average increase of one time in less than 9 months. In January 1998, the sequence of 15500 species was included in EMBL, with a sequence number of more than 1 million, of which more than 50% were sequence of model organisms. Thus far, public access to DNA sequences includes more than 163 million sequences [28]. This enormous database is equivalent to a natural password book. It provides a new idea and solution for image encryption.

In the image encryption method, in order to achieve the purpose of pixel confusion and diffusion, the following rules are defined.

3.2.1 DNA Encoding Rules: If we act according to the encoding rules, A → 00, C → 01, G → 10, and T → 11, then the complementary number matching is 00 ↔ 11 and 01 ↔ 10, and the complementary base pair matching is A ↔ T and C ↔ G. In this case, there are eight encoding combinations that satisfy the complementary pairing rules. For a gray image, the gray value of each pixel can be represented by an 8-bit binary number. If we use the DNA encoding, then each pixel needs four base sequence encodings. By converting the image matrix to a sequence of DNA, the operators for the sequence of the DNA can be applied to the image processing [29]. To reach the goal of pixel value disturbance, the following base operations and transformation rules are defined at the same time.

3.2.2 Base Operation Rules: According to the complementary pairing rules, by encoding A → 00, C → 01, G → 10, and T → 11, we give some base operation rules (see Tables 2–4), according to the different encoding rules, and we also establish similar operation rules.

4. Encryption Algorithms

4.1 Initial Parameters and Chaotic Sequence Generation of Hyper-Chaotic Systems

As a hash function, the Keccak algorithm is based on the sponge structure, which is one of the most basic modules in modern cryptography and generates a fixed-length hash value as the input for any length of message [30]. Its compression is not a conventional compression but an irreversible compression, and once the hash operation is complete, the results will not be restored to the original text. The key generated by the hash value, even if the original image has extremely small changes, and the hash value produced by the SHA-3 encryption are completely different and result in a completely different encryption key. Combining the original image information with the key, the brute force attack is 2^{512}, and thus, the encryption method effectively resists known plaintext attack, chosen plaintext attack and brute force attack.

Using the Keccak algorithm to generate the hash value K of the original image, which is divided into 64 blocks, and each contains a total of 8 bits, $K = \{k_1, k_2, k_3, \ldots, k_{64}\}$, the initial values of the chaotic system are computed by the following formulas for x_0, y_0, z_0, w_0:

$$h_i = \frac{\left(k_{j+1} \oplus k_{j+2} \oplus k_{j+3}\right) + k_{j+4} + k_{j+5} + k_{j+6}}{256} \tag{2}$$

$$\begin{cases} x_0 = x'_0 + abs(\text{round}\,(h_1) - h_1) \\ y_0 = y'_0 + abs(\text{round}\,(h_2) - h_2) \\ z_0 = z'_0 + abs(\text{round}\,(h_3) - h_3) \\ w_0 = w'_0 + abs(\text{round}\,(h_4) - h_4) \end{cases} \tag{3}$$

Where $j = 6(i-1)$, $i = 1, 2, 3, 4$; x'_0, y'_0, z'_0, w'_0 are given values.

When the system is in hyper-chaotic state and through iterations, we remove the start-end data from the sequence and take out the L unrepeatable values. Then, we obtain four discrete real numeric hyper-chaos sequences, including A_1: $\{a_{11}, a_{12}, \ldots, a_{1L}\}$, A_2: $\{a_{21}, a_{22}, \ldots, a_{2L}\}$, A_3: $\{a_{31}, a_{32}, \ldots, a_{3L}\}$, and A_4: $\{a_{41}, a_{42}, \ldots, a_{4L}\}$. To unify the value range of the real sequence, only by obtaining the decimal part of the four sequences, we obtain the new sequences, which are B_1: $\{b_{11}, b_{12}, \ldots, b_{1L}\}$, B_2: $\{b_{21}, b_{22}, \ldots, b_{2L}\}$, B_3: $\{b_{31}, b_{32}, \ldots, b_{3L}\}$, and B_4: $\{b_{41}, b_{42}, \ldots, b_{4L}\}$. Then, we have

$$\begin{cases} B_1 = (A_1 - [A_1]) \\ B_2 = (A_2 - [A_2]) \\ B_3 = (A_3 - [A_3]) \\ B_4 = [\text{mod}\,(10000 * (A_4 - [A_4]),\ 256)] \end{cases} \tag{4}$$

Here, $[x]$ represents the integer part of x.

TABLE 1
8 Encoding Rules

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

TABLE 2
The XOR Operation for DNA Sequences

XOR	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

TABLE 3
The Addition Operation for DNA Sequences

ADD	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

TABLE 4
The Subtraction Operation for DNA Sequences

Sub	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

4.2 Dynamic DNA Encoding

If the image has the same local pixel value, for example, there are more '00' in the plaintext, there will certainly be more 'A' after DNA encoding using the regular rule. This weak point becomes more apparent when handling medical images. If one encodes medical images using rule 1, 'A' will definitely be the most one in the converted DNA arrays. DNA encoding is performed with fixed rules, that is, the bit distribution of the plaintext cannot be disturbed.

Dynamic DNA coding technology is based on the position of the matrix to be encoded in the image matrix P and decides to select the encoding rule of Table 1. That is, the DNA encoding rule $R_{i,j}$ of the pixel $P_{i,j}$ is calculated as follows:

$$R_{i,j} = \text{Mod}\left((i\ -\ 1)^{*}\, n + j,\ 8\right) + 1 \tag{5}$$

Where $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$

Since each pixel value can be represented by an 8-bit binary, each pixel is encoded as 4 bases. Then, the encoded sequence length is 4 mn. For example, the pixel value of the element in the thirty-seventh row and the fifty-fourth column for the original image is 108, which can be expressed in binary [01101100], and according to the dynamic encoding technology, the rule $R_{37,54} = 8$

should be selected; it is encoded by the DNA encoding rule 8, and the DNA sequence of the pixel is [GCAT].

4.3 The Construction of Hill Encryption Matrix

Hill encryption is a replacement cipher using basic matrix theory, which was invented by Lester S. Hill in 1929 [31]. The Hill cipher is a kind of substitution cipher. Its advantages include the ability to conceal plain letter frequency, express conciseness, are easily implemented by computer and use a reversible matrix to encrypt and decrypt. It can be applied to image encryption. The key to the hill cipher is the encryption matrix. If the encryption matrix is irreversible, the ciphertext cannot be restored to plaintext. To avoid a strong correlation between the encryption matrix elements, we use a hyper-chaotic sequence to construct self-inverse encryption matrix to reduce the correlation between matrices so that the ciphertext is difficult to crack [32].

The image to be encrypted is blocked into every 4 pixels, and each block of pixels is transformed into a 4×1 matrix I_{4*1}. By constructing the 4×4 reversible matrix M, the Hill encryption is performed on each set of images. The encryption formula is as follows:

$$E = (M * I) \bmod 256 = \begin{bmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{bmatrix} * \begin{bmatrix} I_{11} \\ \vdots \\ I_{41} \end{bmatrix} \bmod 256 = \begin{bmatrix} E_{11} \\ \vdots \\ E_{41} \end{bmatrix} \tag{6}$$

Multiplication inverse matrix M^{-1} is used to decrypt the ciphertext: $I = (M^{-1} * E) \bmod 256 = (M * E) \bmod 256$.

The self-inverse matrix M is divided into four parts:

$$M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix},$$

Where

$$M_{11} = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix},$$

1) As a pseudo-random number generator, the hyper-chaotic system generates a hyper-chaotic sequence, selects elements from the hyper-chaotic sequence, and fills M_{11}.
2) Sub-matrix $M_{12} = I - M_{11}$.
3) Sub-matrix $M_{22} = -M_{11}$.
4) Sub-matrix $M_{21} = I + M_{11}$. Finally, the generated four sub-matrices M_{11}, M_{12}, M_{22}, and M_{21} are merged to obtain the reversible cipher matrix M.

According to the chaotic characteristics, each element of the matrix M generated by the chaos theory has good randomness. It does not simply solve the inherent regularity and has a high encryption strength. Thus, the generated key matrix based on the block matrix M_{11} is more robust. The resulting inverse matrix is used for the key, eliminating the inverse matrix for the cryptosystem.

4.4 Ciphertext Feedback

The operation of ciphertext diffusion makes small changes in plaintext spread to the whole ciphertext, thus disrupting the relationship between the plaintext and ciphertext image, which effectively resists the chosen plaintext attack and achieves ciphertext diffusion. The image matrix is converted to a one dimensional sequence $S = \{s_1, s_2, s_3, \ldots, s_{mn}\}$ in the order of row priority, and the sequence of the ciphertext diffusion is $SE = \{se_1, se_2, se_3, \ldots, se_{mn}\}$, and the formula for the diffusion of ciphertext is as follows:

$$se(i + 1) = s(i) \oplus se(i - 1) \tag{7}$$

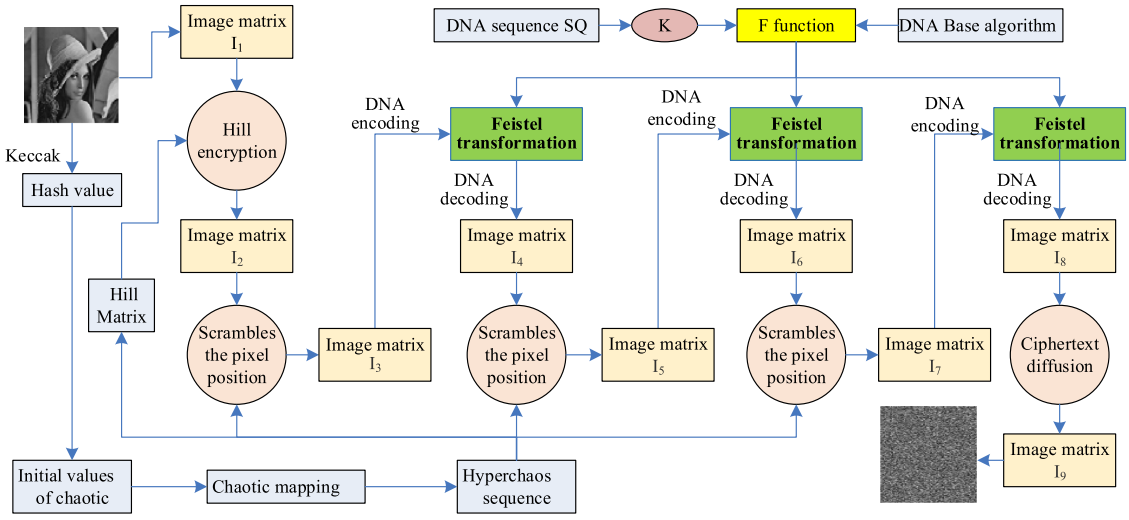


Figure 2. Description of the encryption process.

Where the initial elements $se(0) = 127$, $i = 1, 2, \ldots, m^*n$.

4.5 Encryption Algorithms

The digital image encryption algorithm proposed in this paper adopts the three-round 'scrambling-diffusion' structure. First, for the Hill matrix permutation, by using the sequence generated by the hyper-chaotic system, a Hill encryption matrix is constructed to replace the image matrix. Second, for pixel position scrambling, the permutation index of the chaotic sequence generated by the hyper-chaotic system makes the pixel position of the scrambled image. Third, for dynamic DNA encoding and Feistel transformation, the image pixels are dynamically encoded and converted to DNA sequences, the DNA sequence operations are used as F functions, and the sequence in the DNA sequence database is used as key K, which implements a block Feistel transformation for the transformed DNA sequences. Finally, for diffusion through the ciphertext feedback, the encryption flowchart is shown in Figure 2, and the specific steps are as follows:

Input: the input is the grayscale image P and the initial value of the parameter.

Output: the output is the encrypted image.

1) Convert the grayscale image P into a two-dimensional matrix P_1 with the size $m \times n$.
2) Hash function is used to calculate the hash value K of the image matrix P_1, and the chaotic initialization parameters are obtained.
3) According to sequence B_4 generated by the hyper-chaotic Chen system, construct the $T = \lceil m * n/4 \rceil$ Hill encryption matrices $KM_1, KM_2, \ldots, KM_T$.
4) For the encrypted image P_1, divide every 4 pixels into a block, and the Hill encryption matrix constructed by step (3) is encrypted and permuted according to formula (6), and the image matrix P_2 is obtained.
5) Download the DNA sequence with the ID number NZ_LOZQ01000042 from the GenBank database. The 6 mn base sequence is intercepted from the Sth base, named the sequence SQ, and is used for the key K of the Feistel transformation.
6) According to sequence B_1 generated by the hyper-chaotic Chen system, the permutation index sequence X is obtained in ascending order, and the sequence X is filled with each row m. Thus, the permutation matrix is obtained, and the pixel position in the image matrix P_2 is scrambled with the matrix; then, we can obtain the scrambled matrix P_3.
7) The image matrix P_3 is separated in every 8 blocks. For the dynamic DNA encoding for each block of pixels, after coding, each block contains 32 bases, and L and R are further divided into two blocks by Feistel transformation. Then, the DNA XOR operation is selected as the F

function of the Feistel transformation, and the DNA sequence SQ is the secret key K of the Feistel transformation. After the Feistel transformation, the DNA coding rule 1 is selected for DNA decoding, and the matrix form is restored, and the image matrix P_4 is obtained, which completes the first round of scrambling and transformation.

8) According to sequence B_2 generated by the hyper-chaotic Chen system, which is similar to step (6), the scrambling is performed, and the image matrix P_5 is obtained. The image matrix P_5 is further subjected to dynamic DNA encoding, Feistel transformation, and DNA decoding, according to the step (7), and is restored to a matrix form to obtain the image matrix P_6, which completes the second round of scrambling and transformation.
9) Similarly, according to sequence B_3 generated by the hyper-chaotic Chen system, which is similar to step (6), the scrambling is performed, and the image matrix P_7 is obtained. The image matrix P_7 is further subjected to dynamic DNA encoding, Feistel transformation, and DNA decoding, according to the step (7), and is restored to a matrix form to obtain the image matrix P_8, which completes the third round of scrambling and transformation.
10) According to the ciphertext diffusion method described in Section 4.5, the image encryption matrix P_9 is obtained by the XOR operation with the ciphertext of the previous pixel.

The decryption method is the inverse process of the above process. This process is no longer elaborated. This method can also be applied to color image encryption, by processing only the values of the pixel RGB decomposition.

5. Experimental Results and Security Analysis

In view of the method proposed in this paper, Matlab software is applied to verify the feasibility of the method. Using the standard 256∗256 Lena grayscale image as the original image, the key includes the given value $x'_0 = y'_0 = z'_0 = w'_0 = 0.00000005$, the DNA sequence ID number is NZ_LOZQ01000042 in the nucleic acid database, and the starting position is $S = 1$. The image is encrypted using this method, and the original image, the encrypted image and the deciphered image are shown in Figures 3(a), 3(b) and 3(c), respectively.

5.1 Key Space and its Sensitivity Analysis

If the computation precision is 10^{-14}, then the key space reaches 10^{100}, which shows that the method has sufficient space to resist an exhaustive attack. To test the sensitivity of the key, the initial value of the x'_0 is increased by 0.00000001, and the other keys are unchanged in the hyper-chaotic Chen system. Using the modified key to decrypt the encrypted image, the decryption results are shown in Figure 3(d). The key to the minor changes cannot correctly decrypt the original image. Furthermore, using the modified key to encrypt the image, the encrypted images shown in Figures 3(e) and 3(b) are compared between the two cipher images that correspond to different pixel rates above 99.62%. The method has a strong key sensitivity, and it can resist violent attacks; it has good key security for such attacks.

5.2 Gray Histogram Analysis

The statistical information of the image reveals the distribution of the gray value of the original image, to a certain extent, and whether it changes the statistical distribution of the original image is also an important indicator of the image encryption. The purpose of this method is to strike the attack side against a grayscale statistical attack. As shown in Figure 4, the experimental results showed that the XOR operation and the permutation operation make the grayscale distribution of the encrypted image very uniform, which shows that the method has a good ability to resist the statistical analysis in such a way that the attacker cannot analyze the original gray value distribution range.

Furthermore, the variance of the histogram is introduced to measure the uniformity of the pixel distribution of the ciphertext image. The smaller the variance, the more uniform the pixel distribution.

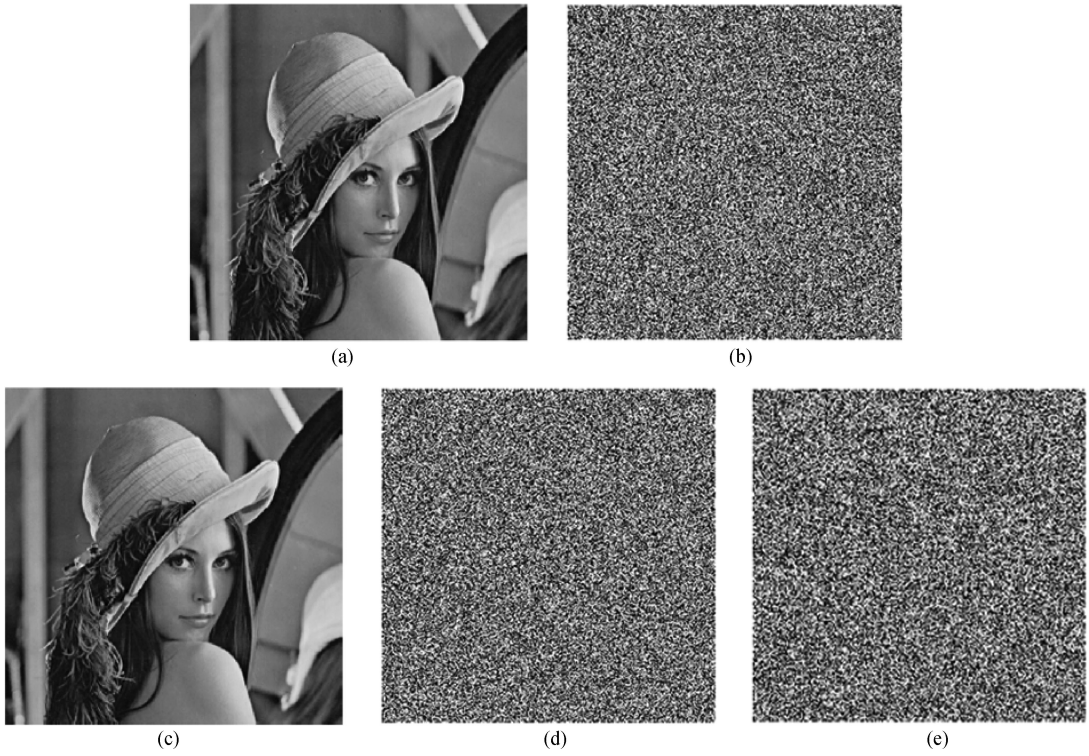


Figure 3. Lena image and ciphered Lena image. (a) Plain Lena image. (b) Ciphered Lena image. (c) Deciphered Lena image. (d) Decrypted image with the modified key. (e) Ciphered Lena image with the modified key.

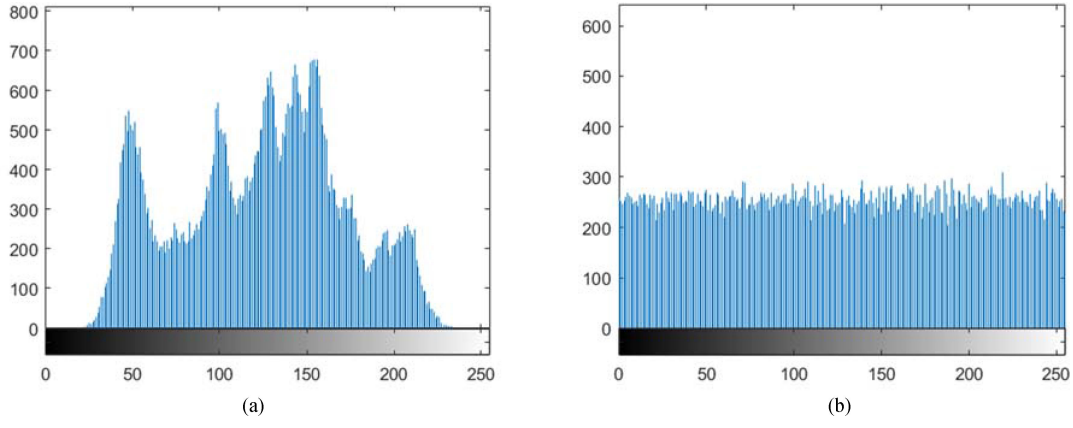


Figure 4. Histogram of the plain Lena image and ciphered Lena image. (a) Histogram of the plain Lena image. (b) Histograms of the ciphered Lena image.

Different keys are used to encrypt the same plaintext image and calculate the variance of the corresponding two ciphertext images. If the corresponding variance values of the two ciphertexts are close, it means that the ciphertext image has a higher uniform histogram when the key is changed. The histogram variance is calculated as follows:

$$\mathrm{var}(Z) = \frac{1}{n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \frac{(z_i - z_j)^2}{2} \tag{8}$$

TABLE 5
Correlation Coefficients of the Proposed Algorithm Compared With Other References

	Original image	Encryption image (proposed method)	Ref. [33] (Ye's algorithm)	Ref. [34] (Liu et al.'s algorithm)
Horizontal direction	0.9700	0.0039	0.0163	-0.0152
Vertical direction	0.9384	-0.0314	-0.0029	0.0140
Diagonal direction	0.9176	0.0158	0.0309	0.0218

Where Z is the image histogram value vector $\mathrm{Z} = \{z_0, z_1, \ldots, z_{256}\}$ and z_i and z_j are the number of pixels with gray values i and j, $n = 256$.

The histogram variance of the plaintext image is 39851.33, and the histogram variance of the encrypted image is 283.7109 when using the key given before. When we change the initial value x_0' of chaotic system, the variance is 231.7422, which shows that the encrypted pixel obtained by this method is evenly distributed.

5.3 Correlation Coefficient Analysis

The correlation between the pixels in the original image is relatively large, and to prevent the statistical analysis, we must reduce the correlation of the adjacent pixels. We randomly selected, from the original image and the encrypted image, each pixel to a 2500-pixel correlation, testing the horizontal, vertical and diagonal directions, as shown in Table 5. Table 5 shows that there is a significant correlation between the image pixels before the encryption. After the encryption, the correlation between the pixels is greatly reduced. This finding indicates that the adjacent pixels are not related to each other, and the statistical characteristics of the original image have spread to the random ciphertext image.

The correlation coefficient is calculated as follows:

$$r_{xy} = \frac{\mathrm{cov}\,(x, y)}{\sqrt{\mathrm{D}\,(x)}\sqrt{\mathrm{D}\,(y)}} \tag{9}$$

Where $\mathrm{cov}(x, y) = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}}(x_i - \mathrm{E}(x))(y_i - \mathrm{E}(y))$, $\mathrm{E}(x) = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}} x_i$, $\mathrm{D}(x) = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}}(x_i - \mathrm{E}(x))^2$.

According to the calculation, the correlation coefficient between the original image and the encrypted image is -0.00822. Table 5 and Figure 5 show the correlation comparison between the original image and the adjacent pixel of the encrypted image.

5.4 Differential Attack Analysis

A differential attack is to make a slight change to the original image and then to encrypt the original image and the changed image. The relationship between the original image and the encrypted image is obtained by comparing the two encrypted images. The two standards of number of pixel change rate (NPCR) and uniform average changing intensity (UACI) are used to measure whether the encryption method resisted the differential attack [35].

$$\mathrm{NPCR} = \frac{\sum_{\mathrm{i,j}} D\,(i, j)}{W \times H} \times 100\% \tag{10}$$

$$\mathrm{UACI} = \frac{1}{\mathrm{W} \times \mathrm{H}}\left[\sum\nolimits_{i,j} \frac{\left|\mathrm{C}\,(i, j) - \mathrm{C}'\,(i, j)\right|}{255}\right] \times 100\% \tag{11}$$

Where W and H denote the length and width of the image, respectively, and C and C' denote the ciphertext images corresponding to the two plaintext images with only a one-pixel difference. For the pixel (i, j), if $\mathrm{C}(i, j) \neq \mathrm{C}'(i, j)$, $D\,(i, j) = 1$; otherwise, $D\,(i, j) = 0$. For the Lena images, the NPCR and UACI values of the method are 99.6185% and 28.7344%, respectively, which is compared with

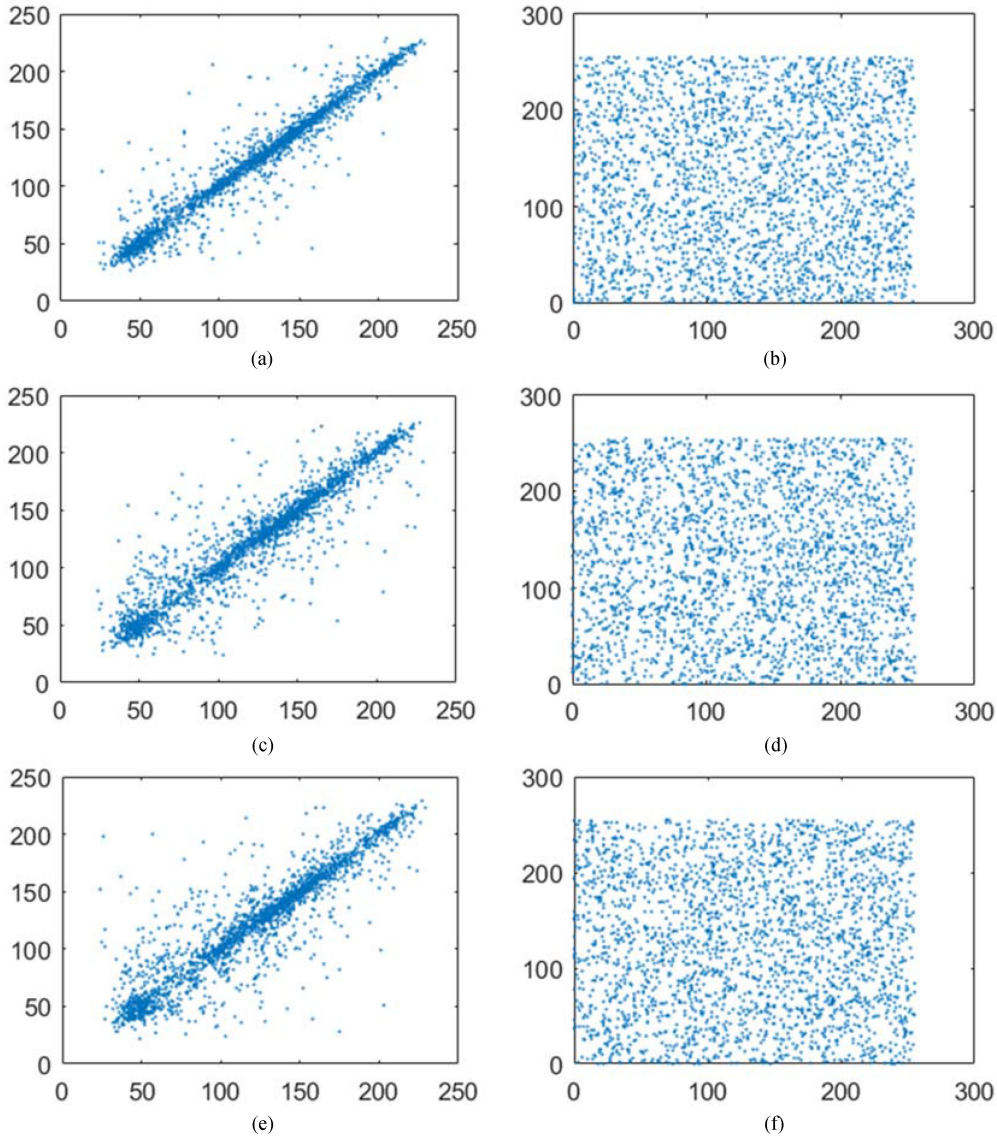


Figure 5. Correlation analysis of Lena as a ciphered image in three directions. (a) Horizontal correlation of the plain image. (b) Horizontal correlation of the ciphered image. (c) Vertical correlation of the plain image. (d) Vertical correlation of the ciphered image. (e) Diagonal correlation of the plain image. (f) Diagonal correlation of the ciphered image.

the results in Ref. [34]. The results show that the performance of the proposed method is better than the scheme in Ref. [34]. Therefore, the method has a good ability to resist differential attack.

5.5 Information Entropy Analysis

Information entropy is a measure of uncertainty. The formula is as follows:

$$H\ (m) = -\sum_{k=0}^{2^N-1} p\ (m_i)\, log_2 p(m_i) \tag{12}$$

Here, $p(m_i)$ represents the probability that the information m_i appears. For the grayscale images, the information m_i has 256 states, the minimum value is 0, and the maximum is 255. According

to the above equation, when the information entropy is 8, the information is completely random. In other words, the greater the entropy of the ciphertext information, the more secure the information is. The information entropy of the cryptographic image obtained by encrypting the Lena image is 7.989, which is compared with the results in Ref. [36]. The results show that the information entropy of the cipher image using Lian *et al.*'s scheme is 7.978, which indicates that the information leakage of the ciphertext is very small and further proves the security of the method.

5.6 Classic Attack Analysis

Generally, assuming that the attacker knows the encryption system we used, according to the information obtained by the attacker, there are 4 types of typical attacks, including a ciphertext-only attack, a known plaintext attack, a chosen plaintext attack and a chosen ciphertext attack.

We know that the intensity of the above four types of attacks increases sequentially; the ciphertext-only attack is the weakest, and the chosen ciphertext attack is the strongest. If a cryptosystem resists the chosen ciphertext attack, then we think that it can resist the remaining three attacks. The method in this paper is very sensitive to the initial parameters and initial values; once one of them is changed, the sequences of B_1, B_2, B_3 and B_4 are always different. Furthermore, in the Feistel permutation and the ciphertext diffusion phase, the encrypted value is not only related to the plaintext but also to the ciphertext of the previous pixel. This means that this method can resist the chosen plaintext attack or chosen ciphertext attack.

Here, the security of the proposed algorithm is analyzed by statistical methods. However, as described by Özkaynak [37], all of these methods are statistical methods. Statistical method is necessary, but it is not enough to show that the algorithm has high security. Özkaynak presents an analysis roadmap to analyze the security of the algorithm. The roadmap includes 12 steps. The current algorithm is classified by using this roadmap, and it is pointed out that the analyzed algorithm is contained in the weaknesses expressed in steps 7, 11, and 12 in the checklist [38], [39]. In this paper, the Feistel network of traditional cryptography is introduced to enhance the confusion and diffusion of the algorithm, and further increase the security of the algorithm. Of course, for part of the checklist, the algorithm needs to be further strengthened. We will further improve it in the future work.

6. Conclusion

A digital image encryption method based on the Feistel network and dynamic DNA encoding is proposed. The scrambling transformation of the image pixel position and the diffusion of the pixel value were realized by a Hill permutation, Feistel transformation, chaotic scrambling and dynamic DNA encoding. As the F function of the Feistel transformation, the DNA sequence operation reduced the number of encrypted rounds by multiple scrambling and DNA encoding and decoding to achieve the effect of a multi-round encryption. The security analysis showed that three rounds of Feistel transformation, scrambling and DNA encoding and decoding technology enabled the method to effectively resist a plaintext attack, differential attack and statistical attack, and it had good security and application potential.

References

[1] L. Y. Zhang *et al.*, "On the security of a class of diffusion mechanisms for image encryption," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1–13, Apr. 2017.
[2] X. Zhang, Y. Niu, C. Shen, and G. Cui, "Fluorescence resonance energy transfer-based photonic circuits using single-stranded tile self-assembly and DNA strand displacement," *J. Nanosci. Nanotechnol.*, vol. 17, no. 2, pp. 1053–1060, 2017.
[3] J. P. L. Cox, "Long-term data storage in DNA," *Trends Biotechnol.*, vol. 19, no. 7, pp. 247–250, 2001.
[4] X. Zhang, Y. Wang, G. Cui, Y. Niu, and J. Xu, "Application of a novel IWO to the design of encoding sequences for DNA computing," *Comput. Math. Appl.*, vol. 57, no. 11–12, pp. 2001–2008, 2009.

[5] Y. Erlich and D. Zielinski, "DNA fountain enables a robust and efficient storage architecture," *Science*, vol. 355, no. 6328, pp. 950–954, 2016.
[6] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with DNA binary strands," *Biosystems*, vol. 57, no. 1, pp. 13–22, 2000.
[7] B. Shimanovsky, J. Feng, and M. Potkonjak, "Hiding data in DNA," *Lecture Notes Comput. Sci.*, vol. 2578, pp. 373–386, 2008.
[8] W. L. Chang, M. Guo, and M. S. Ho, "Fast parallel molecular algorithms for DNA-based computation: Factoring integers," *IEEE Trans. NanoBiosci.*, vol. 4, no. 2, pp. 149–163, Jun. 2005.
[9] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography," in *Proc. 5th Dimacs Workshop DNA Based Comput.*, 1999, pp. 233–249.
[10] J. Chen, "A DNA-based biomolecular cryptography design," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2003, no. 3, pp. 822–825.
[11] K. Tanaka, A. Okamoto, and I. Saito, "Public-key system using DNA as a one-way function for key distribution," *Biosystems*, vol. 81, no. 1, pp. 25–29, 2005.
[12] H. Mousa, K. Moustafa, W. Abdel-Wahed, and M. Hadhoud, "Data hiding based on contrast mapping using DNA medium," *Int. Arab J. Inf. Technol.*, vol. 8, no. 2, pp. 147–154, 2008.
[13] Y. Liu, Q. Zang, and X. Wie, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Opt. Laser Technol.*, vol. 60, no. 5, pp. 111–115, 2014.
[14] 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 Dyn.*, vol. 82, no. 3, pp. 1269–1280, 2015.
[15] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, 2017.
[16] Y. Niu, X. Zhang, and F. Han, "Image encryption algorithm based on hyperchaotic maps and nucleotide sequences database," *Comput. Intell. Neurosci.*, vol. 2017, pp. 1–9, 2017.
[17] M. Xu and Z. Tian, "Security analysis of a novel fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Int. J. Light Electron. Opt.*, vol. 134, pp. 45–52, 2017.
[18] M. R. Biswas, K. M. R. Alam, A. Akber, and Y. Morimoto, "A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem," in *Proc. Int. Conf. Netw., Syst. Security*, 2017, pp. 1–8.
[19] E. M. S. Hossain, K. M. R. Alam, M. R. Biswas, and Y. Morimoto, "A DNA cryptographic technique based on dynamic DNA sequence table," in *Proc. Int. Conf. Comput. Inf. Technol.*, 2017, pp. 270–275.
[20] X. Zhang, F. Han, and Y. Niu, "Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding," *Comput. Intell. Neurosci.*, vol. 2017, Aug. 22, 2017, Art. no. 6919675, doi: 10.1155/2017/6919675.
[21] G. Cui, Y. Liu, X. Zhang, and Z. Zhou, "A new image encryption algorithm based on DNA dynamic encoding and hyper-chaotic system," in *Proc. Int. Conf. Bio-Inspired Comput. Theories Appl.*, 2017, pp. 286–303.
[22] Q. Zhang, L. Liu, and X. Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps," *AEUE–Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 186–192, 2014.
[23] D. Heider and A. Barnekow, "DNA-based watermarks using the DNA-Crypt algorithm," *Bmc Bioinf.*, vol. 8, no. 1, pp. 1–10, 2007.
[24] R. E. Vinodhini and P. Malathi, "DNA based image steganography," in *Proc. Comput. Vis. Bio Inspired Comput.*, 2018, pp. 819–829.
[25] M. T. I. Siyam, K. M. R. Alam, and T. A. Jami, "An exploitation of visual cryptography to ensure enhanced security in several applications," *Int. J. Comput. Appl.*, vol. 65, no. 6, pp. 42–46, 2013.
[26] X. Zhang, Z. Zhou, Y. Jiao, Y. Niu, and Y. Wang, "A visual cryptography scheme-based DNA microarrays," *Int. J. Performability Eng.*, vol. 14, no. 2, pp. 334–340, 2018.
[27] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," *Soc. Ind. Appl. Math.*, vol. 17, no. 2, pp. 373–386, 1988.
[28] H. J. Shiu, K. L. Ng, J. F. Fang, R. C. T. Lee, and C. H. Huang, "Data hiding methods based upon DNA sequences," *Inf. Sci.*, vol. 180, no. 11, pp. 2196–2208, 2010.
[29] K. Pujari, G. Bhattacharjee, and S. Bhoi, "A hybridized model for image encryption through genetic algorithm and DNA sequence," *Procedia Comput. Sci.*, vol. 125, pp. 165–171, 2018.
[30] X. Wang, S. Wang, Y. Zhang, and C. Luo, "A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems," *Opt. Lasers Eng.*, vol. 103, pp. 1–8, 2018.
[31] L. S. Hill, "Cryptography in an algebraic alphabet," *Amer. Math. Monthly*, vol. 36, no. 6, pp. 306–312, 1929.
[32] B. Acharya, M. D. Sharma, S. Tiwari, and V. K. Minz, "Privacy protection of biometric traits using modified hill cipher with involutory key and robust cryptosystem," *Procedia Comput. Sci.*, vol. 2, no. 1, pp. 242–247, 2010.
[33] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," *Nonlinear Dyn.*, vol. 75, no. 3, pp. 417–427, 2014.
[34] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.*, vol. 12, no. 5, pp. 1457–1466, 2012.
[35] X. Wang, L. Teng, and X. Qin, "A novel color image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, 2012.
[36] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos Solitons Fractals*, vol. 26, no. 1, pp. 117–129, 2005.
[37] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 305–313, 2018.
[38] Y. Zhang, C. Li, Q Li, D. Zhang, and S. Shu, "Breaking a chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 69, no. 3, pp. 1091–1096, 2012.
[39] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Process.* vol. 132, pp. 150–154, 2017.