Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2016, Article ID 6408741, 11 pages
http://dx.doi.org/10.1155/2016/6408741

Research Article

Image Encryption Algorithm Based on Dynamic DNA Coding and Chen's Hyperchaotic System

Jian Zhang, Dezhi Hou, and Honge Ren

College of Information and Computer Engineering, Northeast Forestry University, Harbin 150040, China

Correspondence should be addressed to Honge Ren; nefu_rhe@163.com

Received 30 April 2016; Accepted 25 August 2016

Academic Editor: Nazrul Islam

With the development of national information processes, specific image information from secret departments or individuals is often required to be confidentially transmitted. Numerous image encryption methods exist, especially since the initial value sensitivity and other characteristics of chaos theory and chaos theory-based encryption have become increasingly important in recent years. At present, DNA coding constitutes a new research direction of image encryption that uses the four base pairs of DNA code and image pixel values to establish a special correspondence, in order to achieve pixel diffusion. There are eight DNA encoding rules, and current methods of selecting the DNA encoding rules are largely fixed. Thus, the security of encoded data is not high. In this paper, we use the Lorenz chaotic system, Chen's hyperchaotic system, and the DNA encoding combination and present a new image encryption algorithm that can dynamically select eight types of DNA encoding rules and eight types of DNA addition and subtraction rules, with significant improvements in security. Through simulation experiments and histograms, correlations, and NPCR analyses, we have determined that the algorithm possesses numerous desirable features, including good encryption effects and antishear and antinoise performances.

1. Introduction

With the development of national information processes, people have paid increasing attention to secure transmission of image information. The traditional classical encryption algorithms primarily include the DES, IDEA, and RSA algorithms [1–3]. However, compared to text files, image files contain a larger amount of data, so the traditional encryption algorithms are not suitable for image encryption. While some image encryption techniques have emerged, based on mathematical transformations, nevertheless, their security is inadequate.

Chaotic encryption technology has been used as the mainstream of encryption technology in recent years [4], but the use of chaotic technology only is not safe enough [5–7]. In recent years, image encryption technology based on DNA computing has been extensively used by scholars, but work is still at the initial stages of research. At present, most of the image encryption algorithms that are based on DNA coding adopt relatively fixed coding methods, and security is not high. In this paper, DNA coding and chaotic encryption technology are combined, and a dynamic DNA coding image encryption algorithm is proposed that can improve the security of the encryption process. Based on simulation experiments, the algorithm has been shown to exhibit good encryption effects and can effectively resist statistical, shear, and other attacks.

2. Dynamic DNA Coding and Chaotic Mapping

2.1. DNA Coding. A DNA sequence consists of four different basic nucleotides, namely, A, T, C, and G [8], whereby pairing is allowed only between A and T and C and G. Additionally, each pixel point in a grayscale image can be represented by an 8-bit binary number, taking the values of 0 and 1. The binary value pair also constitutes a complementary relationship pair. Since 00 and 11 and 01 and 10 are also complementary, the DNA bases A, C, G, and T can be encoded using the digit pairs 00, 01, 10, and 11. Thus, 24 types of this coding scheme can be obtained, but the program must satisfy the pairing rules, in that A bases must be paired with T and C must be paired

Table 1: DNA coding rules.

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

Table 2: The addition operation of DNA sequence based on rule 1.

	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 3: The subtraction operation of DNA sequence based on rule 1.

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

with G, so only eight types of programs are effective. These are shown in Table 1. For example, if the grayscale value of a pixel in an image is equal to 147, it can be converted to the binary value "10010011." If the first rule in Table 1 is selected, the 8-bit binary number can be expressed as "GCAT." Furthermore, if the fourth rule is chosen, then the 8-bit of the binary number can be expressed as "ATCG."

With the development of DNA computing, some researchers have proposed algorithms based on DNA sequences for the operations of addition and subtraction, based on the basic principles of binary addition and subtraction [9, 10]. Thus, this corresponds to eight different types of DNA encoding schemes, whereby there are eight types of DNA addition operations and eight types of DNA subtraction. In this paper, we use the coding rules 1 and 4, for example, to obtain the addition operation rules and the subtraction operation rules, as shown in Tables 2–5.

2.2. Dynamic DNA Coding. Most algorithms only choose fixed DNA encoding rules to encode, and only a maximum of eight experiments can break it. In this paper, the DNA encoding rules are dynamically selected according to generated chaotic sequences. For example, a pixel value can correspond to any of the four digital values and can be converted to a binary value. Every two binary bits of this value can then use a random encoding mode, which makes the key space larger, more difficult to decipher, and with a higher image encryption security. For example, if the value of the pixel point is still 147, the value of its corresponding chaotic sequence is [1, 3, 5, 7], and then the result of the DNA encoding is "GCGG."

Table 4: The addition operation of DNA sequence based on rule 4.

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

Table 5: The subtraction operation of DNA sequence based on rule 4.

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

Based on the principle of base complementation, the nucleotide x_i in the nucleotide sequence of DNA encoding is as follows [11]:

$$x_i \neq L(x_i) \neq L(L(x_i)) \neq L(L(L(x_i))), \quad x_i = L(L(L(L(x_i)))). \tag{1}$$

In (1), x_i and $L(x_i)$ are complementary. According to (1), there are six types of base pairs that meet the requirements of the combination, as shown below:

(AT)(TC)(CG)(GA).
(AT)(TG)(GC)(CA).
(AC)(CT)(TG)(GA).
(AC)(CG)(GT)(TA).
(AG)(GT)(TC)(CA).
(AG)(GC)(CT)(TA).

During pixel diffusion, one of the six complementary rules will be selected, the complementary DNA sequences will replace operations, and the number of complementary alternative steps will be dynamically selected based on the value of the chaotic sequence, in order to achieve pixel proliferation.

2.3. Lorenz Chaotic System. The mathematical expression of the Lorenz chaotic system is [12]

$$x' = a(y - x), \quad y' = cx - xz - y, \quad z' = xy - bz. \tag{2}$$

When $a = 10$, $b = 8/3$, and $c = 28$, the Lorenz system is in a chaotic state. In this paper, the Lorenz chaotic system is used to scramble the pixel position, as well as achieve the dynamic selection of the DNA addition and subtraction rules. Correspondingly, the main operation is as follows:

(1) The use of the Lorenz chaotic system generates three pseudo-random sequences whose lengths are $M \times 2, N$,

$M \times N \times 4$: $a = \{a_1, a_2, \ldots, a_{M\times 2}\}$, $b = \{b_1, b_2, \ldots, b_N\}$, and $c = \{c_1, c_2, \ldots, c_{M\times N\times 4}\}$. Herein, M is the number of lines of the original image matrix, and N is the number of the original image matrix columns.

(2) The random sequences $a = \{a_1, a_2, \ldots, a_{M\times 2}\}$, $b = \{b_1, b_2, \ldots, b_N\}$, and $c = \{c_1, c_2, \ldots, c_{M\times N\times 4}\}$ are used in accordance with the following operation:

$$\begin{aligned} a(i) &= \operatorname{mod}\left(\operatorname{fix}\left(a(i)\times 10^3\right), 256\right) + 1, \\ &\qquad i = 1, 2, \ldots, M\times 2, \\ b(i) &= \operatorname{mod}\left(\operatorname{fix}\left(b(i)\times 10^3\right), 256\right) + 1, \\ &\qquad i = 1, 2, \ldots, N, \\ c(i) &= \operatorname{mod}\left(\operatorname{fix}\left(c(i)\times 10^3\right), 8\right) + 1, \\ &\qquad i = 1, 2, \ldots, M\times N\times 4. \end{aligned} \tag{3}$$

In these expressions, fix is the rounding operation. The sequences $a = \{a_1, a_2, \ldots, a_{M\times 2}\}$ and $b = \{b_1, b_2, \ldots, b_N\}$ are multiplied by 1000 and the results are rounded. After calculation of the remainder, following a division with respect to 256, it is added to unity. The random number in the random sequence can then be changed to any number within the range of [1–256]. The sequence $c = \{c_1, c_2, \ldots, c_{M\times N\times 4}\}$ is multiplied by 1000 and the results are rounded. After the remainder is calculated, following division by 256, it is then added to unity. The random number in the random sequence can then be changed to any number within the range of [1–8].

(3) By using the first M numbers in the sequence $a = \{a_1, a_2, \ldots, a_{M\times 2}\}$, each line of the image is transformed in accordance with

$$\begin{bmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,j} & \cdots & A_{1,n} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,j} & \cdots & A_{2,n} \\ & & & \vdots & & \\ & & & A_{i,j} & & \\ & & & \vdots & & \\ A_{m,1} & A_{m,2} & \cdots & A_{m,j} & \cdots & A_{m,n} \end{bmatrix}$$
$$\Longrightarrow \begin{bmatrix} A_{1,n-a_1} & A_{1,n-a_1+1} & \cdots & A_{1,n} & A_{1,1} & \cdots & A_{1,n-a_1-1} \\ A_{2,n-a_2} & A_{2,n-a_2+1} & \cdots & A_{2,n} & A_{1,1} & \cdots & A_{2,n-a_2-1} \\ & & & \vdots & & & \\ & & & A_{i,j} & & & \\ & & & \vdots & & & \\ A_{m,n-a_M} & A_{m,n-a_M+1} & \cdots & A_{m,n} & A_{m,1} & \cdots & A_{m,n-a_M-1} \end{bmatrix}. \tag{4}$$

Among the matrix entries, $A_{i,j}$, represents the ith row and jth column in image A. For example, if $a_1 = 50$, then the elements of the first row in the image have to be right-shifted by 50.

(4) By using each number in the sequence $b = \{b_1, b_2, \ldots, b_N\}$, each column of the image is transformed in accordance with

$$\begin{bmatrix} A_{1,n-a_1} & A_{1,n-a_1+1} & \cdots & A_{1,n} & A_{1,1} & \cdots & A_{1,n-a_1-1} \\ A_{2,n-a_2} & A_{2,n-a_2+1} & \cdots & A_{2,n} & A_{1,1} & \cdots & A_{2,n-a_2-1} \\ & & & \vdots & & & \\ & & & A_{i,j} & & & \\ & & & \vdots & & & \\ A_{m,n-a_M} & A_{m,n-a_M+1} & \cdots & A_{m,n} & A_{m,1} & \cdots & A_{m,n-a_M-1} \end{bmatrix}$$
$$\Longrightarrow \begin{bmatrix} A_{m-b_1,n-a_1} & A_{m-b_2,n-a_1+1} & \cdots & A_{m-b_{a_1},n} & A_{m-b_{a_1}+1,1} & \cdots & A_{m-b_N,n-a_1-1} \\ & & & \vdots & & & \\ A_{m,n-a_2} & A_{m,n-a_2+1} & \cdots & A_{m,n} & A_{m,1} & \cdots & A_{m,n-a_2-1} \\ & & & \vdots & & & \\ & & & A_{i,j} & & & \\ & & & \vdots & & & \\ A_{m-b_1-1,n-a_M} & A_{m-b_2-1,n-a_M+1} & \cdots & A_{m-b_{a_1}-1,n} & A_{m-b_{a_1},1} & \cdots & A_{m-b_N-1,n-a_M-1} \end{bmatrix}. \tag{5}$$

For example, if $b_1 = 90$, then each of the elements of the first column in the image is downward shifted by 90.

(5) By using the last M numbers in the sequence $a = \{a_1, a_2, \ldots, a_{M\times 2}\}$, each line of the image is transformed. The

methodology and step (3) remain the same and can be used to complete (4).

The scrambling idea introduced in this article is advanced and includes a line shift conversion, a column shift conversion, and a line shift transformation. If only two ranks of shifting are applied, this may cause some adjacent pixels in a line or column of the original image to remain adjacent in the encrypted image. Transformation can ensure full dispersion of the scrambled image.

The sequence $c = \{c_1, c_2, \ldots, c_{M\times N\times 4}\}$ that will be generated by the Lorenz chaotic system that will be used to dynamically select the DNA addition and subtraction rules in the encryption step will be described in detail.

When decrypting, only the rows and columns corresponding to the left- and upward-shift operations will be used.

2.4. Chen's Hyperchaotic System. Chen's hyperchaotic system [13] is defined as follows:

$$\begin{aligned} x' &= a(y - x), \\ y' &= -xz + dx + cy - q, \\ z' &= xy - bz, \\ q' &= x + k. \end{aligned} \tag{6}$$

In these equations, a, b, c, d, and k are the system parameters. When $a = 36$, $b = 3$, $c = 28$, $d = 16$, and $-0.7 \le k \le 0.7$, Chen's hyperchaotic system is in a chaotic state and can generate four chaotic sequences; namely, $A = \{a_1, a_2, \ldots, a_{M\times N\times 8}\}$, $B = \{b_1, b_2, \ldots, b_{M\times N\times 8}\}$, $C = \{c_1, c_2, \ldots, c_{M\times N\times 8}\}$, and $D = \{d_1, d_2, \ldots, d_{M\times N\times 8}\}$. In this paper, we mainly use the chaotic system to spread the image pixel value.

Four pseudo-random sequences generated by Chen's super chaotic system are performed as follows:

$$\begin{aligned} A &= \operatorname{mod}\left(\operatorname{fix}\left((\operatorname{abs}(A) - \operatorname{fix}(\operatorname{abs}(A))) \times 10^{10}\right), 8\right) \\ &\quad + 1, \\ B &= \operatorname{mod}\left(\operatorname{fix}\left((\operatorname{abs}(B) - \operatorname{fix}(\operatorname{abs}(B))) \times 10^{10}\right), 8\right) \\ &\quad + 1, \\ C &= \operatorname{mod}\left(\operatorname{fix}\left((\operatorname{abs}(C) - \operatorname{fix}(\operatorname{abs}(C))) \times 10^{10}\right), 10\right) \\ &\quad + 1, \\ C &= \begin{cases} 0 & C < 5, \\ 1 & C > 5, \end{cases} \\ D &= \operatorname{mod}\left(\operatorname{fix}\left((\operatorname{abs}(D) - \operatorname{fix}(\operatorname{abs}(D))) \times 10^{10}\right), 4\right), \end{aligned} \tag{7}$$

where the operation abs is used to obtain the absolute value, fix is used to obtain an integer outcome, and the expressions $C = 0$, $C < 5$; $C = 1$, $C > 5$ mean that if the value of the sequence C is less than 5, it will be changed to 0; otherwise it will become 1. The absolute value of each sequence is applied, and the fractional part is taken and then multiplied by 10^{10} times, and the remainder is then estimated. Based on these operations, the contents of the sequences $A = \{a_1, a_2, \ldots, a_{M\times N\times 8}\}$ and $B = \{b_1, b_2, \ldots, b_{M\times N\times 8}\}$ are transformed into random numbers within the range [1–8]. According to the value of the sequence, the corresponding DNA encoding rules are dynamically selected. The contents of the sequence $C = \{c_1, c_2, \ldots, c_{M\times N\times 8}\}$ are transformed into random values that are equal to either 0 or 1 and are used to generate the natural DNA matrix. The contents of the sequence $D = \{d_1, d_2, \ldots, d_{M\times N\times 8}\}$ are transformed into random numbers within the range of [0–3] and are used to dynamically select DNA complementary steps.

3. Image Encryption and Decryption Technology

3.1. Image Encryption Technology. In this paper, the image encryption technology is divided into two main parts, the scrambling and pixel diffusion, as shown in the flow chart of Figure 1.

Assuming that the initial size of the grayscale image I is $M \times N$, the specific encryption steps are as follows.

Input. Grayscale image I, initial value of the Lorenz chaotic system x_1, y_1, z_1, initial value of Chen's hyperchaotic system x_0, y_0, z_0, q_0, and parameter k are the input.

Output. Encrypted image I' is the output.

(1) The grayscale image I is converted into a two-dimensional matrix I_1 of size $M \times N$.

(2) Use (2) of the Lorenz system to generate three pseudo-random sequences with three different lengths of $M \times 2, N, M \times N \times 4$.

(3) Use (3) to extract the sequence generated in the arithmetic conversion.

(4) Use (4) and (5) to scramble the original image and obtain a new matrix I_2.

(5) Convert the matrix I_2 into the binary matrix I_3.

(6) Use (6) of Chen's hyperchaotic system and generate four pseudo-random sequences, each with a length of $M \times N \times 8$.

(7) Use (7) to arithmetically convert the four sequences.

(8) Using the value in the sequence A, the DNA encoding rules in Table 1 are dynamically selected, and the DNA code is used for each two-bit binary number in a two-dimensional matrix to generate the DNA matrix I_4.

(9) According to the value of the sequence B, the DNA encoding rules in Table 1 are dynamically selected, sequence C is encoded by DNA, and the DNA matrix I_5 is generated.

(10) According to (2), generate the sequence of c, and apply a dynamic selection of the eight types of DNA addition rules. Then apply the addition operation on matrix I_4 and matrix I_5 to obtain matrix I_6.

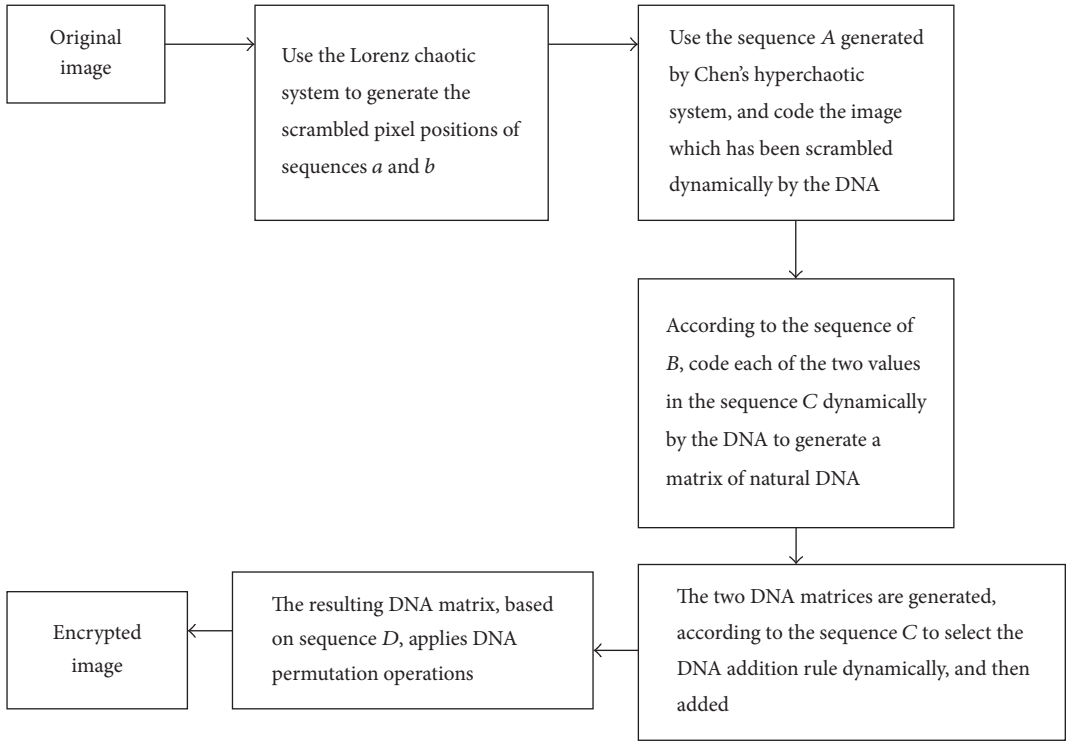


Figure 1: Flow chart of the encryption program.

(11) Generate a random number r_1 within the range of 1–6, in order to select a rule of six base-pair complementary rules. Based on (3) generate the values of sequence D and the complementary base rules selected, and apply the DNA replacement operation on the two-dimensional matrix I_6. The replacement method is in accordance with the following rule: if the value is 0, the DNA code on the bit is not replaced. If it is 1, $x_i = L(x_i)$; if it is 2, $x_i = L(L(x_i))$; if it is 3, $x_i = L(L(L(x_i)))$. A two-dimensional matrix I_7 of M rows and N columns is obtained after the complementary substitution.

(12) Generate a random number r_2 within the range of 1-2, according to the sequence of A or B (of which 1 represents A, and 2 represents B). According to each number in the sequence, choose the corresponding rules in Table 1 dynamically for the DNA decoding operation, in order to obtain matrix I_8.

(13) Convert the matrix I_8 to a decimal matrix I_9. At the end, the two-dimensional matrix I_9 is converted into an encrypted image I' and stored as the output, and the filename is saved by the user.

The encryption process is fully combined with chaos theory and DNA coding theory, by using the chaotic sequence of values, to encode by DNA, and the DNA addition rule of choice. The encoding rules are changeable, random, and not easy to crack and achieve the dynamic DNA encryption.

3.2. Image Decryption Technology. The decryption process is the inverse operation of the encryption process.

Input. The encrypted image I', the initial value of the Lorenz chaotic system x_1, y_1, z_1, the initial value of Chen's hyperchaotic system x_0, y_0, z_0, q_0, parameter k, and the random numbers r_1 and r_2 are the input.

Output. The original grayscale image I is the output.

(1) The encrypted image I' is converted into a two-dimensional binary matrix I_1.

(2) Use (2) of the Lorenz system to generate three pseudo-random sequences of lengths $M \times 2, N, M \times N \times 4$, and use (3) to define the sequence generated in the arithmetic conversion.

(3) Use (6) of Chen's hyperchaotic system to generate four pseudo-random sequences of lengths equal to $M \times N \times 8$, and use (7) to estimate the four sequences in the arithmetic conversion.

(4) According to the random number generator, select the sequence A or B (of which 1 represents A and 2 represents B). According to every value of the selected sequence, dynamically select the appropriate rules in Table 1; decode the matrix I_1 by DNA into the matrix I_2.

(5) According to random number r_1, select a rule of six base-pair complementary rules, and according to the value of each entry of the sequence D and the

(a) Lena (b) Encrypted image

(c) Cameraman (d) Encrypted image

Figure 2: Original and encrypted images.

selected base-pair complementary rules, apply the DNA replacement operation on the two-dimensional matrix I_2, and generate matrix I_3.

(6) According to each value in the sequence B, select the encoding rules from Table 1 dynamically, encode the sequence C based on the DNA encoding operation, and generate matrix I_4.

(7) According to each value in the sequence c, select the DNA subtraction rules dynamically, taking the DNA subtraction operation of the matrices I_3 and I_4, and generate matrix I_5.

(8) According to each value in the sequence A, select the encoding rules from Table 1 dynamically to decode matrix I_5, and generate matrix I_6.

(9) Convert the matrix I_6 to a decimal matrix I_7.

(10) According to (4) and (5), apply the row shift and column shift operations on the two-dimensional matrix I_7, and generate matrix I_8.

(11) Matrix I_8 is converted into an image I, the output is saved, and the filename is then saved by the user.

4. Results

In this paper, we use the grayscale images of Lena and the Cameraman, with image sizes of 256×256. The initial values of the Lorenz chaotic system are $x_1 = 0.526$, $y_1 = 0.346$, and $z_1 = 0.782$. The initial values and parameters of Chen's hyperchaotic system are $x_0 = 0.364$, $y_0 = 0.123$, $z_0 = 0.159$, $q_0 = 0.753$, and $k = 0.3$. The original and encrypted images are shown in Figure 2.

5. Technical Performance and Security Analyses

5.1. Secret Key's Space and Security Analyses. All the chaotic systems are sensitive to initial conditions. In order to encrypt images with additional security, the secret key's space must be tremendously high so that it can resist high-intensity, exhaustive types of attacks [14]. In this paper, the encryption technology is used as follows:

(1) Initialize the value of the Lorenz chaotic system x_1, y_1, z_1.

(2) Initialize the value of Chen's hyperchaotic system x_0, y_0, z_0, q_0 and parameter k.

(3) Apply DNA coding and complementary rules so that the value of the chaotic sequence can be used to determine the type of DNA encoding rules. Correspondingly, the random number r_1 can be used for selecting the type of complementary rules, and the random number r_2 can be used for selecting the types of DNA encoding and decoding rules and the values of the chaotic sequence.

The sensitivity of the Lorenz chaotic system to the initial value is 10^{-16}. When the initial value of the x_1 sensitivity is between 10^{-1} and 10^{-16}, the ratio of the values of the different elements in the matrix of the digital images attained at two different sensitivities is greater than 0.85. However, when the sensitivity of the key is 10^{-17}, the proportion of the different elements is equal to 0. Thus, the key space of the initial value of the Lorenz chaotic system is determined in accordance with $S_{x_1} = S_{y_1} = S_{z_1} = 10^{16}$.

For Chen's hyperchaotic system, when the initial value of the decryption is slightly changed with respect to the initial value of the encryption, such that $\nabla z_0 = 10^{-17}$, the decrypted image and the original image are still difficult to distinguish. However, when $\nabla z_0 = 10^{-16}$, the result of the decryption is not accurate. For example, when the image is encrypted with an initial value $x_0 = 0.364$, it can be successfully decrypted using $x_0 = 0.36400000000000001$ but cannot be successfully decrypted using $x_0 = 0.3640000000000001$. A large number of experimental data prove that the initial value key space of Chen's hyperchaotic system is $S_{x_0} = S_{y_0} = S_{z_0} = S_{q_0} = 10^{16}$. Similarly, the variation of the parameter k in the chaotic region ranges from -0.7×10^{-16} to 0.7×10^{-16}, so Chen's hyperchaotic system parameter key space is $S_k \approx 0.7 \times 10^{16}$.

There are eight types of DNA encoding rules and six types of DNA complementary rules, which carry the two DNA codes and the single DNA complementary substitution, so the key space of the random number is $S_{r_1} = 6$, and $S_{r_2} = 2$. Therefore, the total memory space of the encryption key is

$$\begin{aligned} S &= 2 \times 6 \times S_{x_1} \times S_{y_1} \times S_{z_1} \times S_{x_0} \times S_{y_0} \times S_{z_0} \times S_{q_0} \times S_k \\ &\approx 8.4 \times 10^{128} \end{aligned} \tag{8}$$

which is much larger than 2^{100}. Therefore, the secret key's space is large enough to resist an exhaustive attack.

5.2. Sensitivity Analysis of the Secret Key. Using the initial value $x_1 = 0.526$ for the encryption of the Lena image, the encrypted image shown in Figure 3(b) is obtained. If $x_1 = 0.526$ is used, the decrypted image is shown in Figure 3(c). Using $x_1 = 0.52600000000000001$ the decrypted image is shown in Figure 3(d). For a very small and visible change, keys will not correctly decrypt the encrypted image. The sensitivity of this test can be seen from the key as long as there is a small change that will make the decrypted result distinctly different. Ultimately, this indicates that the key encryption algorithm is highly sensitive.

Table 6: The comparison of the correlation coefficients of Lena's images.

Correlation	Horizontal	Vertical	Diagonal
Original image	0.93063	0.95945	0.90711
Encrypted image	0.00773	−0.01103	0.00153
Reference [15]	−0.09535	0.01454	0.00592

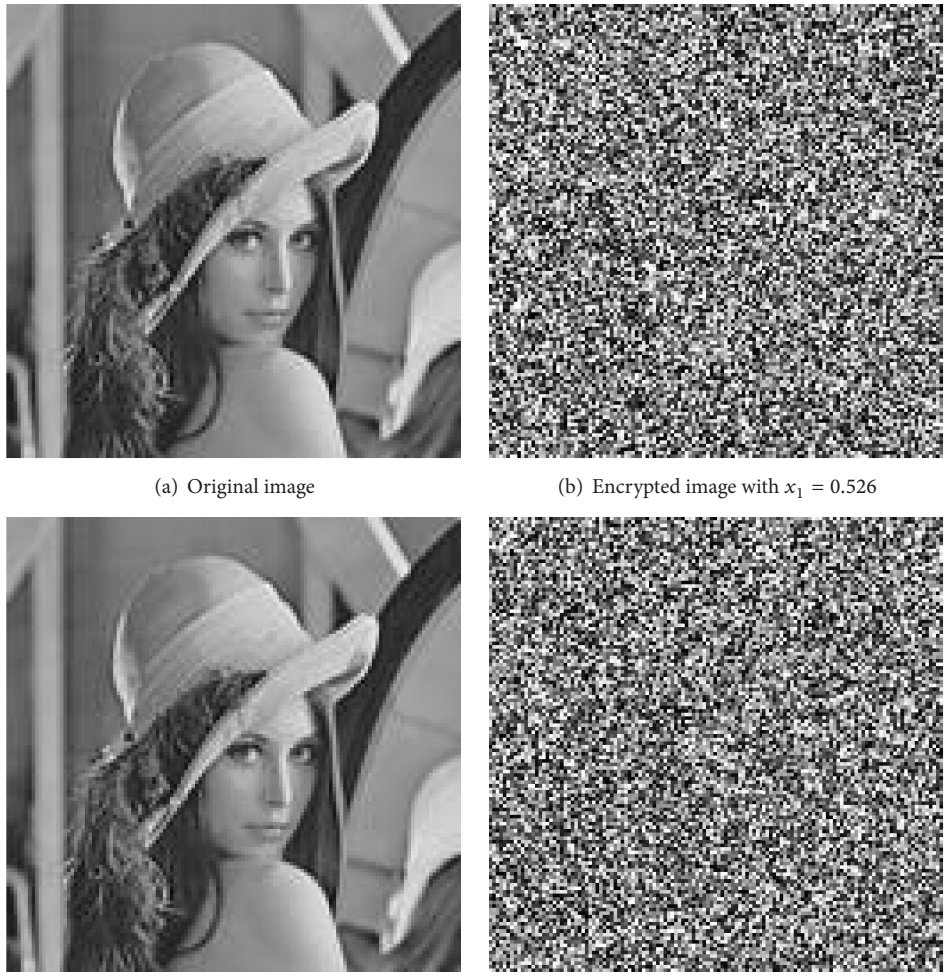
5.3. Resistance to Statistical Attack

5.3.1. The Grayscale Histogram Analysis. The grayscale histograms of the original and encrypted images of Lena and the Cameraman are shown in Figure 4. Through the comparison of their gray level histograms, it can be seen that the histogram of the original image pixel values are concentrated at specific values, but the encryption image gray level histogram of the pixel distribution is relatively balanced. Thus, the results obtained by the encryption technology used to encrypt images are difficult to be exposed to a statistical attack crack.

5.3.2. Correlation Coefficient Analysis. The correlation coefficient, r, [16] is a measure of the degree of linear correlation between two random variables. Its value is in the range of $[-1, 1]$, and $|r|$ expresses the degree of correlation between the variables. Usually when $|r|$ is in the range of $[0.7, 1]$, the two variables are highly correlated. We randomly selected 3,000 pairs of adjacent pixels (along the vertical, horizontal, and diagonal directions) from both the original and encrypted images of Lena and calculated the correlation coefficient for each pair of adjacent pixels according to (9). Table 6 shows the results of the correlation coefficients of two adjacent pixels, which are compared with the results in [15]. Experimental results show that the correlation of the image is significantly reduced. It also shows that this technique can be very good in comparison to the relevant statistics of sexual assaults. Furthermore, calculation of the correlation coefficient of the two images after encryption of the Lena and Cameraman's images yields the respective results of 0.0053741 and 0.0035124, which are much less than 0.7. This shows that the correlation between the encrypted image after the adoption of this encryption algorithm and the original image is very low. Reference [15] also uses DNA coding for image encryption and has been implemented in a standard image (Cameraman image), the encrypted image, and horizontal, vertical, and diagonal direction correlation, as shown in Table 6. A comparison shows that the encryption image generated by this algorithm and the horizontal, vertical, and diagonal directions of the correlation can be lower than the results elicited from the encrypted image generated by the use of the encryption algorithm proposed in [15]. Thus, we can prove that the algorithm in this paper is more secure,

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

where $\operatorname{cov}(x, y) = (1/N)\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$, $E(x) = (1/N)\sum_{i=1}^{N} x_i$, and $D(x) = (1/N)\sum_{i=1}^{N}(x_i - E(x))^2$.



(a) Original image

(b) Encrypted image with $x_1 = 0.526$

(c) Decrypted image with $x_1 = 0.526$

(d) Decrypted image with $x_1 = 0.5260000000000001$

Figure 3: Key sensitivity tests.

5.3.3. Number of Pixels' Change Rate Analysis. Number of pixels' change rate (NPCR) indicates the percentage number of pixel values that change in the encrypted image when one pixel is changed in the original image, in accordance with the NPCR equation (10) [17]:

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

Herein, W and H represent the length and width of the image, and $C(i, j)$ represents the pixel value of the original image. $C'(i, j)$ represents the pixel value of the encrypted image. i and j represent rows and columns of image. If $C(i, j) \neq C'(i, j)$ then $D(i, j) = 1$; otherwise $D(i, j) = 0$.

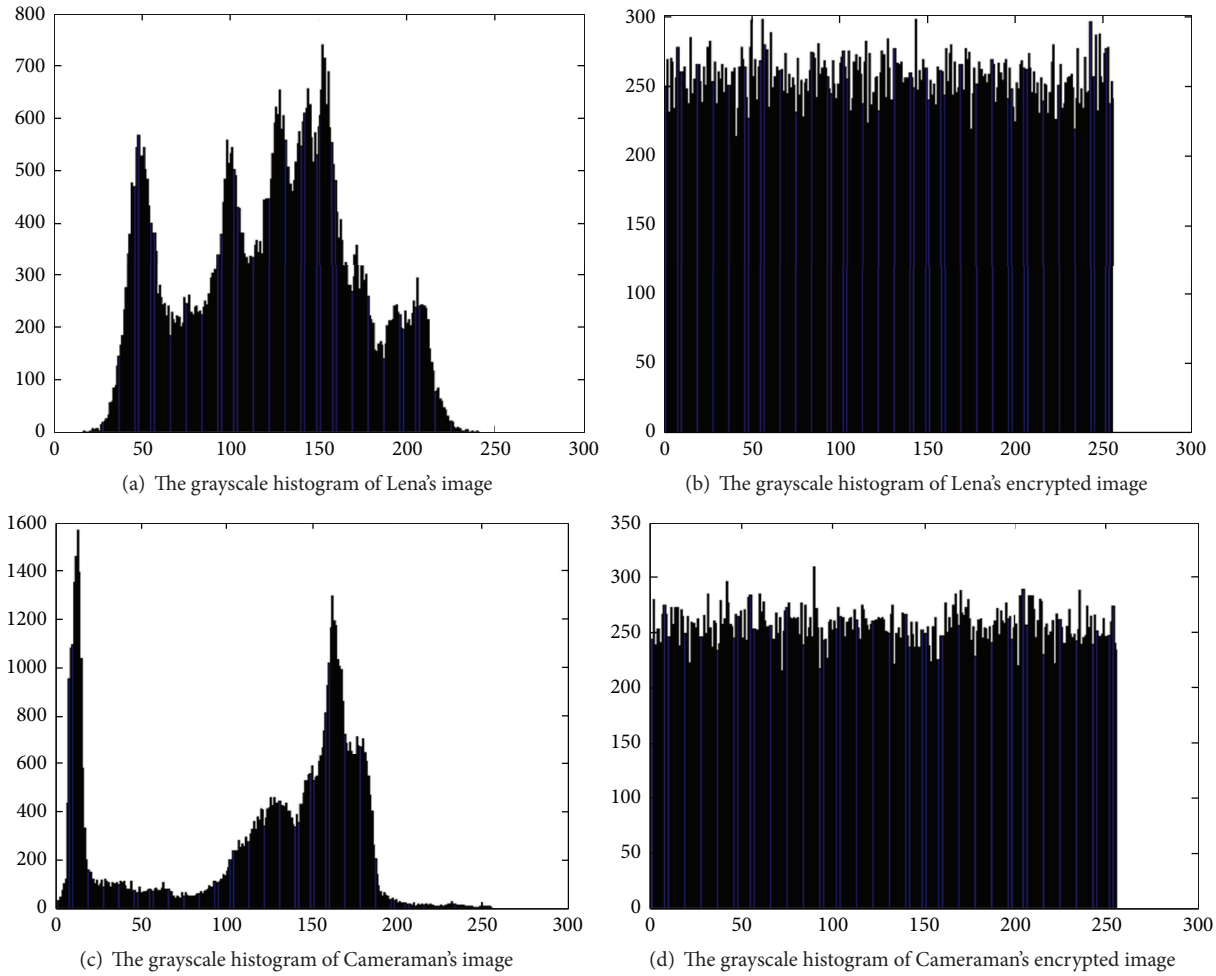
Using (10), the NPCR was calculated for the Lena and Cameraman images before and after encryption. The results are shown in Table 7. We can see that this encryption technology can manifest minor changes on the original image, yet leading to major differences on the encrypted image, which also shows the effectiveness of the algorithm. DNA coding has also been used for image encryption in [18], and the comparison data is shown in Table 7. Reference [18] is also based on the Cameraman image, but the value of NPCR is only 50.11%. According to the definition of NPCR, we know that the greater the value, the higher the security of the algorithm. Correspondingly, the elicited value of 99.6% indicates that the algorithm security is outstanding.

Table 7: NPCR values for the Lena and Cameraman images before and after the encryption.

Figure	NPCR (%)
Figures 2(a) and 2(b)	99.65
Figures 2(c) and 2(d)	99.60
Reference [18]	50.11

Some studies in the literature also use the unified average changing intensity (UACI). However, UACI cannot accurately explain the merits of the algorithm, so this article does not use UACI analysis.

5.3.4. Antishearing Attack Analysis. After the use of the encryption algorithm applied to encrypt Lena's image,



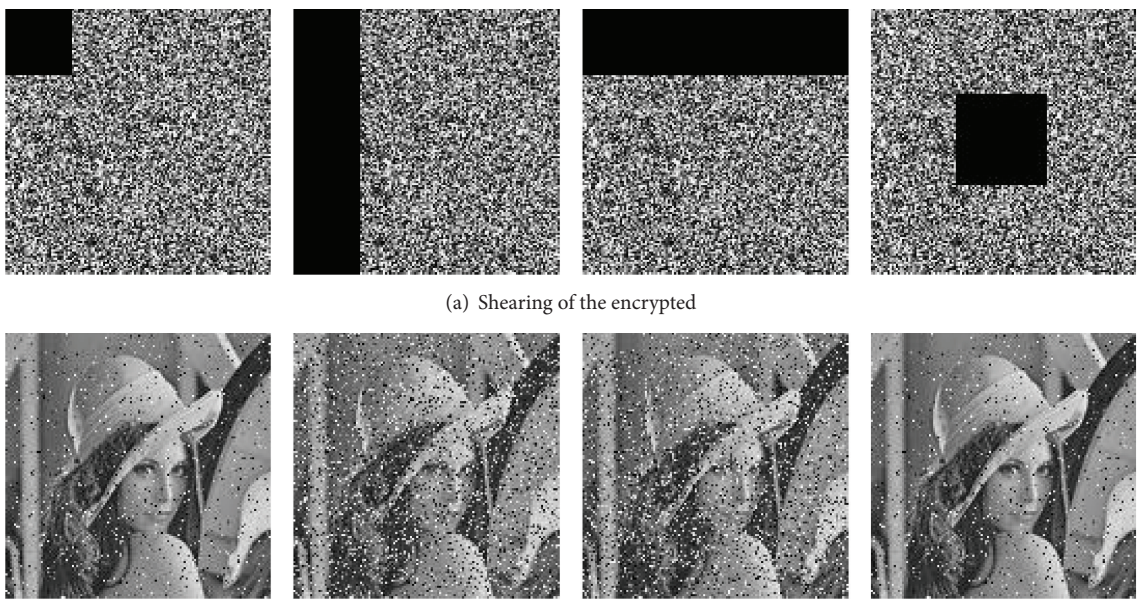
(a) The grayscale histogram of Lena's image

(b) The grayscale histogram of Lena's encrypted image

(c) The grayscale histogram of Cameraman's image

(d) The grayscale histogram of Cameraman's encrypted image

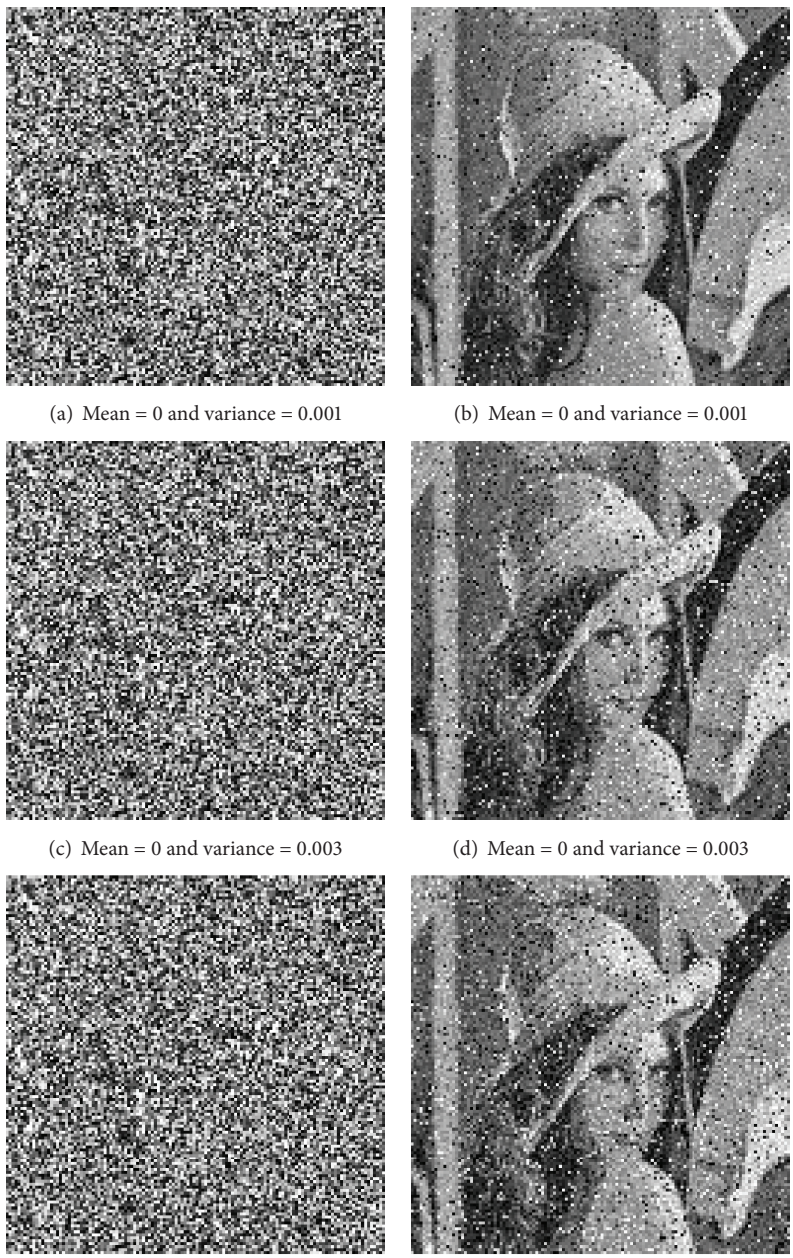
Figure 4: The histograms of Lena's and Cameraman's images.



(a) Shearing of the encrypted

(b) Restored image

Figure 5: Antishearing response.



(a) Mean = 0 and variance = 0.001 (b) Mean = 0 and variance = 0.001

(c) Mean = 0 and variance = 0.003 (d) Mean = 0 and variance = 0.003

(e) Mean = 0 and variance = 0.005 (f) Mean = 0 and variance = 0.005

Figure 6: The encrypted and decryption images after Gaussian, white noise interference.

a certain percentage of the encrypted image is cropped. The remaining sheared image was then decrypted, and the results are shown in Figure 5. Figure 5 shows that, even when the encrypted image is sheared by 25%, the algorithm can still restore the original image, indicating that the algorithm can effectively withstand the cropping, which also illustrates that the correlation of the image encrypted by this algorithm is larger [19].

5.3.5. Resistance Noise Analysis. Image noise is one the various factors that hinders image acceptance. Furthermore, the degree of reliability of the encryption algorithm also depends on the robustness of noise resistance [20]. When the picture is in the uptake or in the process of transmission, there is some image noise interference, and these disturbances may result in unpredictable error occurrences that lead to the inability to decrypt the original image.

Typically, the impact of noise on the encryption system is very obvious, and application of minor transformations on the encrypted image will likely lead to decryption failure and inability to restore the original image. An effective encryption algorithm must have a very good resistance to noise interference, so that when decrypting, the distortion of the image is as low as possible, and the impact is as little

as possible. This algorithm exhibits good robustness against noise, because image encryption encompasses scrambling of the location of the original pixels in the image, followed by dynamic encoding by DNA, and DNA addition. DNA complementation means that the value of the original image pixel is changed to achieve pixel diffusion. This prevents spreading of those pixels changed by noise in the decryption process, thereby avoiding a subsequent cascading effect. In justification of this argument, numerous experiments have been conducted that have proven the robustness of the performance to noise [20].

In this paper, the different means and variances of Gaussian white noise are selected to apply noise interference in image encryption, in order to simulate the impact of some real physical signals in the encrypted image. The results are shown in Figure 6.

Modifications of the means and variances of the Gaussian white noise interference lead to the encrypted and decrypted images shown in Figure 6. Based on the elicited results, the decrypted image visually still contains all the information of the original image, and the correlation with the original image is still high.

6. Conclusions

According to the requirement of high efficiency, safety, and reliability of the encrypted image, this paper proposes an image encryption technology based on the combination of chaotic map and DNA coding technology. Firstly, the chaotic sequences generated by the Lorenz chaotic system are used to scramble the pixels in the image. Using Chen's hyperchaotic system and DNA encoding, the pixels in the image are diffused in order to obtain the image encryption technology. The experimental results show that the key of the technique is 8.4×10^{128}, which meets the big key's space, and is able to withstand statistical analyses, offensive operations, and other requirements of the image encryption technology.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is supported by Nature Science Foundation of Heilongjiang Province (ZD201203/C1603), as well as Nature Science Foundation of Heilongjiang Province (LC2012C33).

References

[1] Y. Liu, X. Tong, and S. Hu, "A family of new complex number chaotic maps based image encryption algorithm," *Signal Processing: Image Communication*, vol. 28, no. 10, pp. 1548–1559, 2013.

[2] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

[3] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," *Optics and Lasers in Engineering*, vol. 51, no. 6, pp. 665–673, 2013.

[4] W. Chen, C. Quan, and C. J. Tay, "Optical color image encryption based on Arnold transform and interference method," *Optics Communications*, vol. 282, no. 18, pp. 3680–3685, 2009.

[5] R. Enayatifar, A. H. Abdullah, and M. Lee, "A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption," *Optics and Lasers in Engineering*, vol. 51, no. 9, pp. 1066–1077, 2013.

[6] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik—International Journal for Light and Electron Optics*, vol. 125, no. 5, pp. 1671–1675, 2014.

[7] S. Lian, "A block cipher based on chaotic neural networks," *Neurocomputing*, vol. 72, no. 4–6, pp. 1296–1301, 2009.

[8] A. N. Pisarchik and M. Zanin, "Image encryption with chaotically coupled chaotic maps," *Physica D: Nonlinear Phenomena*, vol. 237, no. 20, pp. 2638–2648, 2008.

[9] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 3998–4006, 2010.

[10] F. Zheng, X.-J. Tian, J.-Y. Song, and X.-Y. Li, "Pseudo-random sequence generator based on the generalized Henon map," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, no. 3, pp. 64–68, 2008.

[11] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," *Chaos, Solitons & Fractals*, vol. 42, no. 3, pp. 1745–1754, 2009.

[12] H. Li and Y. Wang, "Double-image encryption based on discrete fractional random transform and chaotic maps," *Optics and Lasers in Engineering*, vol. 49, no. 7, pp. 753–757, 2011.

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

[14] Q. Zhang, Q. Wang, and X. Wei, "A novel image encryption scheme based on DNA coding and multi-chaotic maps," *Advanced Science Letters*, vol. 3, no. 4, pp. 447–451, 2010.

[15] Xuguangxian and Guoxiaojuan, "The DNA image encryption algorithm based on chaotic system," *The Computer Applications*, vol. 34, no. 11, pp. 3177–3179, 2014.

[16] S. H. Jiao and R. Goutte, "Code for encryption hiding data into genomic DNA of living organisms," in *Proceedings of the 9th International Conference on Signal Processing (ICSP '08)*, pp. 2166–2169, Beijing, China, October 2008.

[17] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[18] Xuguangxian and Guoxiaojuan, "DNA image encryption algorithm improvement," *Laser Journal*, vol. 35, no. 7, pp. 23–25, 2014.

[19] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 7, pp. 2943–2959, 2012.

[20] Y. Liu, J. Tang, and T. Xie, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map," *Optics and Laser Technology*, vol. 60, pp. 111–115, 2014.