Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 917147, 10 pages
http://dx.doi.org/10.1155/2014/917147

Research Article

Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps

Jian Zhang, DongXin Fang, 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 6 November 2014; Accepted 9 December 2014; Published 31 December 2014

Academic Editor: Miguel A. F. Sanjuan

We propose a new image encryption algorithm based on DNA sequences combined with chaotic maps. This algorithm has two innovations: (1) it diffuses the pixels by transforming the nucleotides into corresponding base pairs a random number of times and (2) it confuses the pixels by a chaotic index based on a chaotic map. For any size of the original grayscale image, the rows and columns are fist exchanged by the arrays generated by a logistic chaotic map. Secondly, each pixel that has been confused is encoded into four nucleotides according to the DNA coding. Thirdly, each nucleotide is transformed into the corresponding base pair a random number of time(s) by a series of iterative computations based on Chebyshev's chaotic map. Experimental results indicate that the key account of this algorithm is 1.536×10127, the correlation coefficient of a 256×256 Lena image between, before, and after the encryption processes was 0.0028, and the information entropy of the encrypted image was 7.9854. These simulation results and security analysis show that the proposed algorithm not only has good encryption effect, but also has the ability to repel exhaustive, statistical, differential, and noise attacks.

1. Introduction

With the development of science, technology, and society, the computer industry, in which a small branch of digital images applications has become increasingly pervasive, has come to occupy a dominant position worldwide. Digital images have become one of the most popular media types and are now used extensively in various fields such as politics, economics, defense, and education [1]. However, because of the open nature of networks, image transmission security is subject to potential threats. In some fields, such as military affairs, commerce, and medical treatment, digital images also need to meet the highest requirements of confidentiality [2]. Consequently, image encryption technology has become an effective way to protect images being transmitted.

Various common image encryption algorithms are available, including text encryption technology, SCAN language-based encryption technology, quadtree image encryption technology, vector quantization encryption technology (VQ), encryption technology based on pseudorandom sequences, encryption technology based on the "key image" chaotic encryption technology, and image encryption technology based on DNA computing [3–10]. Recently, chaotic encryption technology has been attracting increasing attention. Chaos is an inner-class random process of nonlinear systems performance and is very sensitive to initial values, thus resulting in unpredictable results. The benefits of chaotic encryption technology include simple implementation, robustness, fast encryption, and high security [11]. However, although chaotic encryption technology has many advantages, it also has a number of deficiencies. For example, at present, most chaotic encryption algorithms confuse the single image pixel value or location, but the utilization of only one of the two strategies does not ensure high security for the image [12], and thus it is easy for attackers to crack an encrypted image by simply using the pixel comparison method.

In 1994, Adleman first introduced DNA computing into the encryption field, which created a new stage of information processing. DNA encryption is a new frontier and is presently at the forefront of international cryptography research [13, 14]. DNA molecules harness massive parallelism and have low energy consumption and high storage density [15, 16]. Therefore, image encryption algorithms based on DNA computing possess unique advantages that the traditional cryptographic

algorithms do not have. However, using only DNA encoding to encrypt images is not secure. Therefore, we combine chaos encryption technology and image encryption based on DNA computing to solve the hidden insecurity problems existing when images are confused using the chaotic encryption technology. First, we confuse the digital image pixels using the chaotic encryption technology. We then diffuse the confused pixels using DNA encoding. The diffusion process is also applied to the chaotic encryption technology and, finally, we obtain the encryption result.

In summary, our study successfully combines chaotic encryption technology and DNA coding techniques in a method that has been verified via a large number of experiments and security analyses to prove the security and rationality of the algorithm.

2. DNA Encoding and Chaotic Maps

2.1. DNA Encoding and Complementary Rule. DNA sequencing is the process used to map the nucleotide sequence forming a strand of DNA. Four bases, adenine (A), thymine (T), guanine (G), and cytosine (C) form the building blocks of genetic code. "A" binds with "T" and "G" binds with "C" [17]. We know that every digital image pixel can be expressed by 8-bit binary numbers [18]. Because the binary numbers "0" and "1" are complementary, "00" and "11" and "01" and "10" are also complementary. If we use the four deoxynucleotides "A," "T," "G," and "C" to represent the binary numbers "00," "11," "01," and "10," respectively, then each pixel can be encoded into a string of nucleotides. For example, the gray value of a digital image pixel is 228, and the binary corresponding to this value is "11100100." According to the above rules, the string of nucleotides that corresponds to this binary is "TCGA." There are 24 types of combinations for the four nucleotides. However, only eight coding combinations are suitable for the principle of complementarity. These rules are summarized in Table 1.

We assume that the size of the original grayscale image I is $M \times N$, transform I into a binary matrix I', and then randomly select one of the eight combinations of coding DNA to encode I'. The coded matrix is called I''. Finally, I'' is converted into a one-dimensional sequence X, which can be expressed as follows:

$$X = \{x_1, x_2, x_3, \ldots, x_{4MN}\}, \quad x_i \in \{A, T, G, C\}. \tag{1}$$

In accordance with the principle of the complementary base, we set the nucleotide string x_i of the encoding nucleotides as follows:

$$\begin{aligned} &x_i \neq P(x_i) \neq P(P(x_i)) \neq P(P(P(x_i))), \\ &x_i = P(P(P(P(x_i)))), \end{aligned} \tag{2}$$

where $P(x_i)$ and x_i are complementary; in other words, $P(x_i)$ and x_i are a pair of base pairs. These base pairs need to meet the conditions of injective mapping. According to (2), there are six types of rational complementary combinations of base pairs:

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

Table 1: The rules of DNA encoding.

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

During the pixel diffusion, the nucleotides will be substituted using the DNA complementary rule. We randomly select one rule from the six available to achieve a complementary substitution. Thus, we can achieve our objective of pixel diffusion.

2.2. Logistic Map. In this paper, we use two types of chaotic maps: logistic chaotic map and Chebyshev's chaotic map. The logistic chaotic map is a polynomial map of depth two [19]. The mathematical definition of this map is as follows [20, 21]:

$$X_{n+1} = \mu X_n(1 - X_n). \tag{3}$$

Therefore, our algorithm confuses the pixels using the logistic map and suppose that the size of the original grayscale image I is $M \times N$. In summary, the main idea is as follows.

Step 1. Suppose two arrays, R and C_l, are, respectively, used to record the rows and columns of an image:

$$\begin{aligned} R &= \{1, 2, \ldots, M\}, \\ C_l &= \{1, 2, \ldots, N\}. \end{aligned} \tag{4}$$

Step 2. Generate two pseudorandom sequences A and B, with respective sizes m and n, using the logistic map:

$$\begin{aligned} A &= \{a_1, a_2, \ldots, a_m\}, \\ B &= \{a_1, a_2, \ldots, a_n\}. \end{aligned} \tag{5}$$

Step 3. Arrange the sequences A and B in descending order and record their locations. Thus, we can obtain the descending indexes, Index 1 and Index 2, of this pseudorandom sequence:

$$\begin{aligned} \text{Index 1} &= \{i_1, i_2, \ldots, i_m\} \\ \text{Index 2} &= \{j_1, j_2, \ldots, j_n\}. \end{aligned} \tag{6}$$

The primary objective of this step is to find the index of the largest number from the sequence with size m and then

store it in i_1. Next, we find the index of the second largest number and store it in i_2. We repeat this process until the descending sequence indexes are all stored in array Index 1. Similarly, we can obtain the index array Index 2 by arranging the sequence B in descending order and taking its index.

Step 4. According to indexes Index 1 and Index 2, we exchange row R with column C_l. We can then obtain new arrays of the exchanged row R' and column C_l' and can confuse the image pixels.

2.3. Chebyshev's Map. The expression of Chebyshev's map is as follows:

$$Z_{i+1} = \cos(w \times \arccos(Z_i)), \tag{7}$$

where $-1 \le Z_i \le 1, 2 \le w \le 6$. When $w \in [2, 6]$, Chebyshev's map is chaotic [22]. In a condition of infinite computational accuracy, this map can produce an infinite-length, nonperiodic, chaotic real-valued sequence [23]. Thus, Chebyshev's map has useful applications in encryption systems.

We generated iterations of complementary replacements of encoding DNA using Chebyshev's map, which is mainly used to diffuse the pixels of an image. The main steps are as follows.

Chebyshev's map has two initial values, z_0 and q_0, and two parameters, w_z and w_q. The confused grayscale image has $M \times N$ pixels. Each pixel can be represented by four 2-bit nucleotides; therefore, the number of one-dimensional images of the encoding DNA is $M \times N \times 4$ after the coding.

Step 1. Generate two one-dimensional sequences Z and Q using (7), two initial values z_0 and q_0, and two parameters w_z and w_q:

$$\begin{aligned} Z &= \{z_1, z_2, \ldots, z_{4MN}\}, \\ Q &= \{q_1, q_2, \ldots, q_{4MN}\}. \end{aligned} \tag{8}$$

Step 2. Generate a new one-dimensional sequence P using (10), which will serve as the location that is used to obtain one digit from Z. In order to enlarge the key space, we randomly select one digit from 15 decimal digits, according to the location sequence P:

$$P = \{p_1, p_2, \ldots, p_{4MN}\}, \tag{9}$$

$$p_i = (q_i \times 10) \bmod 15 + 1. \tag{10}$$

Step 3. Obtain the sequence C using (12), which will serve as the number of iterations and has a one-to-one correspondence with the nucleotide sequence X, generated by (1):

$$C = \{c_1, c_2, \ldots, c_{4MN}\}, \tag{11}$$

$$c_i = \text{int}(\text{extract}(z_i, p_i)) \bmod 4, \tag{12}$$

where the function extract(z_i, p_i) is used to extract the number of p_i decimal digit from z_i.

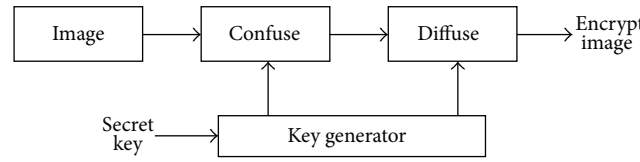


Figure 1: Block diagram of the proposed model.

3. Image Encryption and Decryption Algorithm

3.1. Image Encryption Algorithm. The overall encryption process is depicted in Figure 1.

If we suppose that the size of the original grayscale image I is $M \times N$, the encryption steps are as follows:

Input: image I, the initial values of the logistic map a_0 and b_0, the parameters μ_a and μ_b, the initial values of Chebyshev's map z_0 and q_0, and the parameters w_z and w_q.

Output: the encrypted image.

Step 1. Convert the original grayscale image I into a two-dimensional matrix called I. Let two arrays be named R and C. These are, respectively, used to record the rows and columns of image I.

Step 2. Generate the two one-dimensional descending index sequences using (3) of the logistic mapping, which is used to, respectively, exchange rows and columns of matrix I. Thus, we can obtain a confused image I'.

Step 3. Convert image I' into a binary two-dimensional matrix I''. The size of I'' is $M \times N$ rows and eight columns. Then, generate a random integer r_1 from one to eight, which is used to decide which DNA encoding rule (Table 1) should be used. Convert I'' into a DNA encoding matrix with $M \times N$ rows and four columns. Finally, convert this matrix into a one-dimensional DNA coding sequence X, whose size is $M \times N \times 4$.

Step 4. Generate a storing unit P using (7) of the Chebyshev mapping. Get a sequence of iterations C with P. Then, generate a random integer r_2 from one to six. Thus, we can decide which rule to use among the six types of complementary base pairs rules. Finally, according to each value of c_i, we can decide the method to replace the nucleotides x_i in the DNA sequence X. The method of iterative substitution is as follows:

switch c_i;

case 0, do not change x_i;

case 1, $x_i = L(x_i)$;

case 2, $x_i = L(L(x_i))$;

case 3, $x_i = L(L(L(x_i)))$.

The complementarily substituted DNA sequence is X'.

Step 5. Generate a random integer r_3 from one to eight, which is used to decide which DNA encoding rule (Table 1)

should be utilized. Then, convert the sequence X' into a one-dimensional binary sequence II'.

Step 6. Convert the sequence II' into a decimal dimensional matrix III with M rows and N columns. Finally, convert the dimensional matrix III into the encryption image III' and output the encryption image.

3.2. Image Decryption Algorithm. The decryption and encryption algorithm processes are reversed and operate as follows:

Input: encryption image III', the initial values of the logistic map a_0 and b_0, the parameters μ_a and μ_b, the initial values of Chebyshev's map z_0 and q_0, the parameters w_z and w_q, and the random integers r_1, r_2, and r_3.

Output: original grayscale image.

Step 1. Convert the encryption image III' into a one-dimensional binary sequence II'.

Step 2. Convert the sequence II' into a one-dimensional DNA coding sequence X' using the DNA encoding rule r_3.

Step 3. Generate a storing unit P using (7) of the Chebyshev mapping. Obtain a sequence of iterations C with P. Compute the complementary pair of each nucleotide $x_i \in X'$ for $(4 - c_i)$ mod 4 time(s) to obtain the DNA coding sequence X using the complementary base pairs rule r_2.

Step 4. Transform sequence X into a two-dimensional matrix I'' using the encoding DNA rule r_1. Then, transform the sequence I'' into a two-dimensional decimal matrix I'.

Step 5. Recover the rows and columns of I' according to the descending index generated by (3) of the logistic mapping to get the decrypted image I.

4. Experimental Results

In our experiment, we first set the initial values and parameters of the logistic map: $a_0 = 0.3575123321123321$, $b_0 = 0.5575123321123321$, $\mu_a = 3.775123321123321$, and $\mu_b = 3.875123321123321$. For Chebyshev's map, we set $z_0 = 0.6398711122233345$, $q_0 = 0.2298711122233345$, $w_z = 5.299233234567891$, and $w_q = 4.289233234567891$. The size of the original grayscale image was 256×256. The original gray image and the encrypted image are shown in Figures 2(a)–2(f). The 3D color image and the encrypted image are shown in Figures 2(g) and 2(h).

5. Algorithm Performance and Security Analysis

5.1. Key Space and Sensitivity Analysis. Any chaotic system is sensitive to the initial values. To make the encryption algorithm highly secure, the key space should be large enough to make any brute-force attack ineffective. Here, all the keys are from the process of confusing and diffusing the pixels. Our encryption algorithm actually does have some of the following secret keys:

(1) the initial values of the logistic map, a_0 and b_0, and the parameters μ_a and μ_b;

(2) the initial values of Chebyshev's map, z_0 and q_0, and the parameters w_z and w_q;

(3) DNA coding and complementary rules and random integers r_1, r_2, and r_3.

The sensitivities to the initial values and parameters of the logistic map are both considered to be 10^{-16} [24]. If we set the precision decimal value of the keys from 10^{-1} to 10^{-16}, the ratio of the different elements between the two arrays is larger than 0.85. However, when the key difference is 10^{-17}, it equals zero. Therefore, we can define the key space of the initial values of the logistic map: $S_{a_0} = S_{b_0} = 10^{16}$. For the variation of the parameters $\mu_a, \mu_b \in (3.6, 4]$, and $S_{\mu a} = S_{\mu_b} = 0.5 \times 10^{16}$.

In the case of Chebyshev's map, when the change in the initial value is small, $\nabla z_0 = 10^{-16}$, the decrypted image is still indistinguishable [25]. However, when $\nabla z_0 = 10^{-15}$, the decipher result is uncertain. For example, when we encrypt Lena's image with $z_0 = 0.6382911122234563$, it can be successfully decrypted by $z_0 = 0.6382911122234563$; however, when $z_0 = 0.6382911122234564$ is used, the encrypted image cannot be successfully decrypted.

We encrypted Lena's image with two similar initial values ($\nabla z_0 = 10^{-15}$) and obtained the results shown in Figure 3. From the differences observed in Figure 3(c), we can state that the encryption results are completely different. A large number of experimental results indicate that the key spaces for the initial values are $S_{z_0} = S_{q_0} = 10^{15}$. Similarly, the variation of the parameters w_z and w_q in the chaotic region is between 2×10^{-15} and 6×10^{-15}, so that $S_{w_z} = S_{wq} \approx 4 \times 10^{15}$.

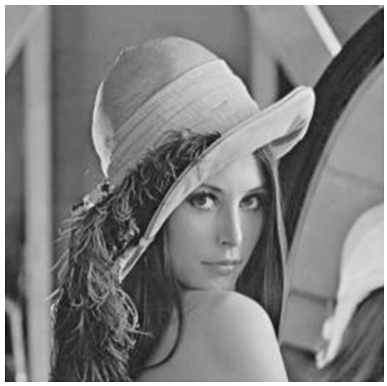
There are only eight kinds of coding DNA that meet the complementary rule, and there are altogether six kinds of legal complementary rules. We used coding DNA rules twice and DNA complementary rules once. Therefore, the key space of the random integers is $S_{r_1} = S_{r_3} = 8$, and $S_{r_2} = 6$. The total key space is

$$S = 8 \times 8 \times 6 \times S_{a_0} \times S_{b_0} \times S_{\mu a} \times S_{\mu_b} \times S_{z_0} \times S_{q_0} \times S_{w_z} \times S_{wq} \approx 1.536 \times 10^{127}, \tag{13}$$

which is much larger than 2^{100}; therefore, the encryption algorithm has a sufficiently large key space to repel all kinds of brute-force attacks.

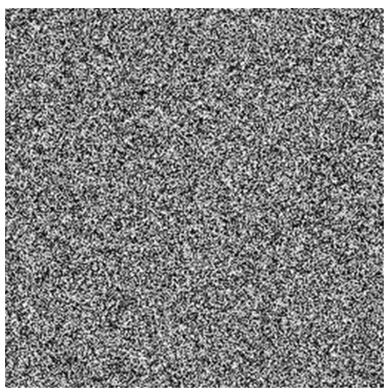
5.2. Resistance to Statistical Attacks

5.2.1. Gray Histogram Analysis. Following statistical analysis of the original and encrypted images, we constructed grayscale histogram analysis of Lena and Shrek and their



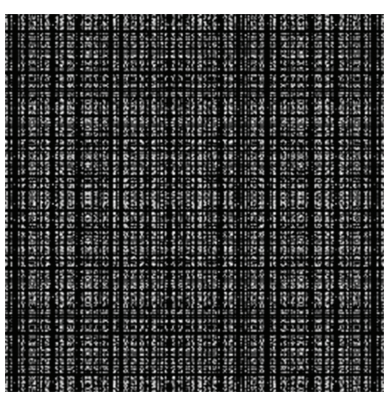
(a) Lena

(b) Permuted rows and columns

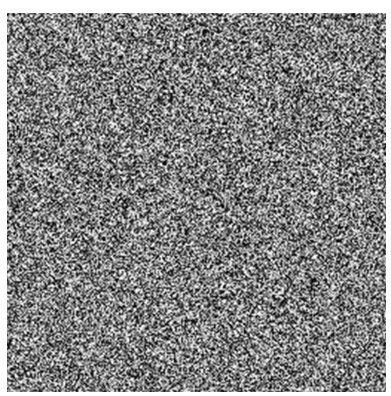


(c) Encrypted image

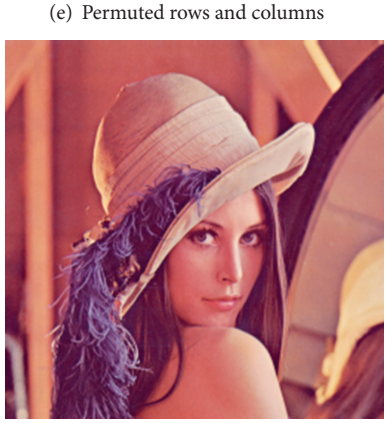
(d) Shrek



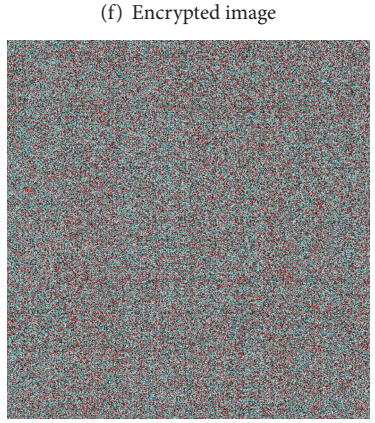
(e) Permuted rows and columns



(f) Encrypted image

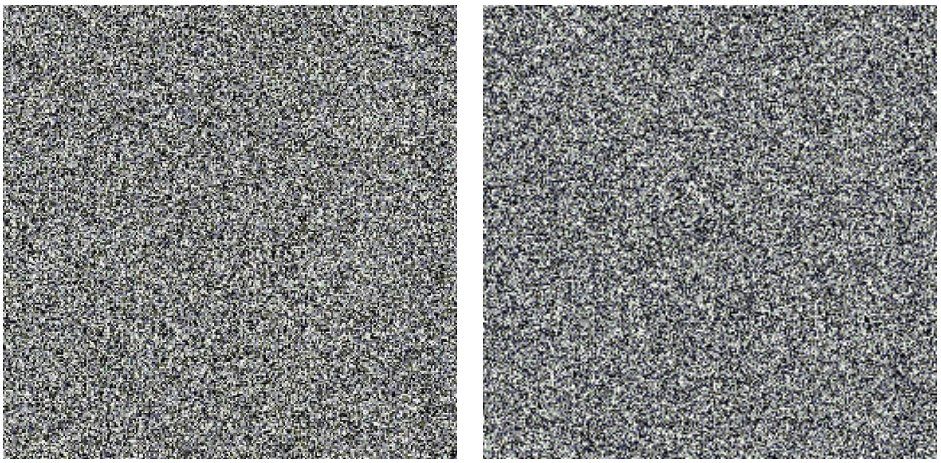


(g) 3D color Lena

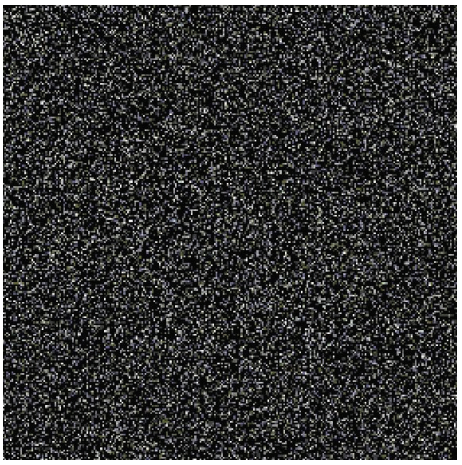


(h) Encrypted Lena

Figure 2: The original and the encrypted images.



(a) $Z_0 = 0.638291112223456$ (b) $Z_0 = 0.638291112223457$



(c) The difference between (a) and (b)

Figure 3: Encryption of Lena's image using similar initial values and their differences.

encrypted images (Figure 4). Comparing the histograms, it is evident that the pixel grayscale values of the original images are concentrated on some values, while the histograms of the encrypted images are relatively uniform, which makes statistical attacks difficult.

5.2.2. Correlation Coefficient Analysis. The correlation coefficient is the evaluation criterion used to find the degree of linear correlation between two random variables. The range of our correlation coefficient r is $[-1, 1]$; $r > 0$ indicates positive correlation and $r < 0$ indicates negative correlation. $|r|$ represents the degree of correlation between the variables, with $r = \pm 1$ indicating perfect correlation and $r = 0$ indicating uncorrelated variables [26]. In general, for $|r| > 0.8$, we assume a strong linear correlation. We calculated the correlation coefficient between the original Lena image and its encrypted image. The result was 0.0128, which is much less than 0.8, thus proving that the correlation between the original and encrypted images is very low. We randomly selected 2,500 pairs of adjacent pixels (in vertical, horizontal, and diagonal directions) from both the original and encrypted images and calculated the correlation coefficient for each pair of adjacent pixels according to (14). Table 2 shows the results of correlation coefficients for two adjacent pixels, which are compared with the results obtained by Zhang et al. [13, 14]. The results indicate that the correlation of two adjacent pixels of the plain image is significant. Therefore, the encryption effect of this algorithm is rather good:

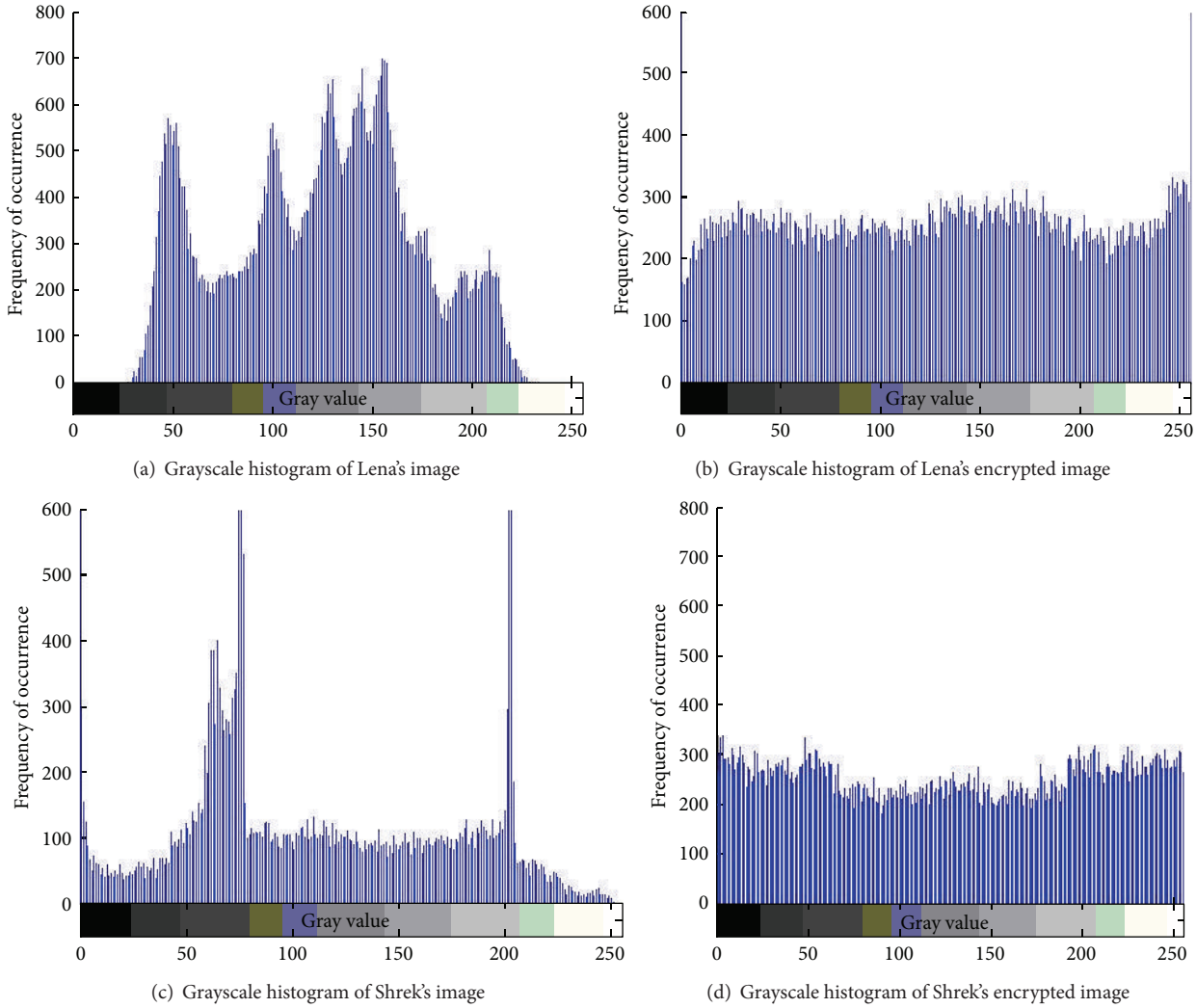
$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{14}$$

where

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)),$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2. \tag{15}$$



(a) Grayscale histogram of Lena's image

(b) Grayscale histogram of Lena's encrypted image

(c) Grayscale histogram of Shrek's image

(d) Grayscale histogram of Shrek's encrypted image

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

Table 2: Comparison of the correlation coefficients of Lena's images.

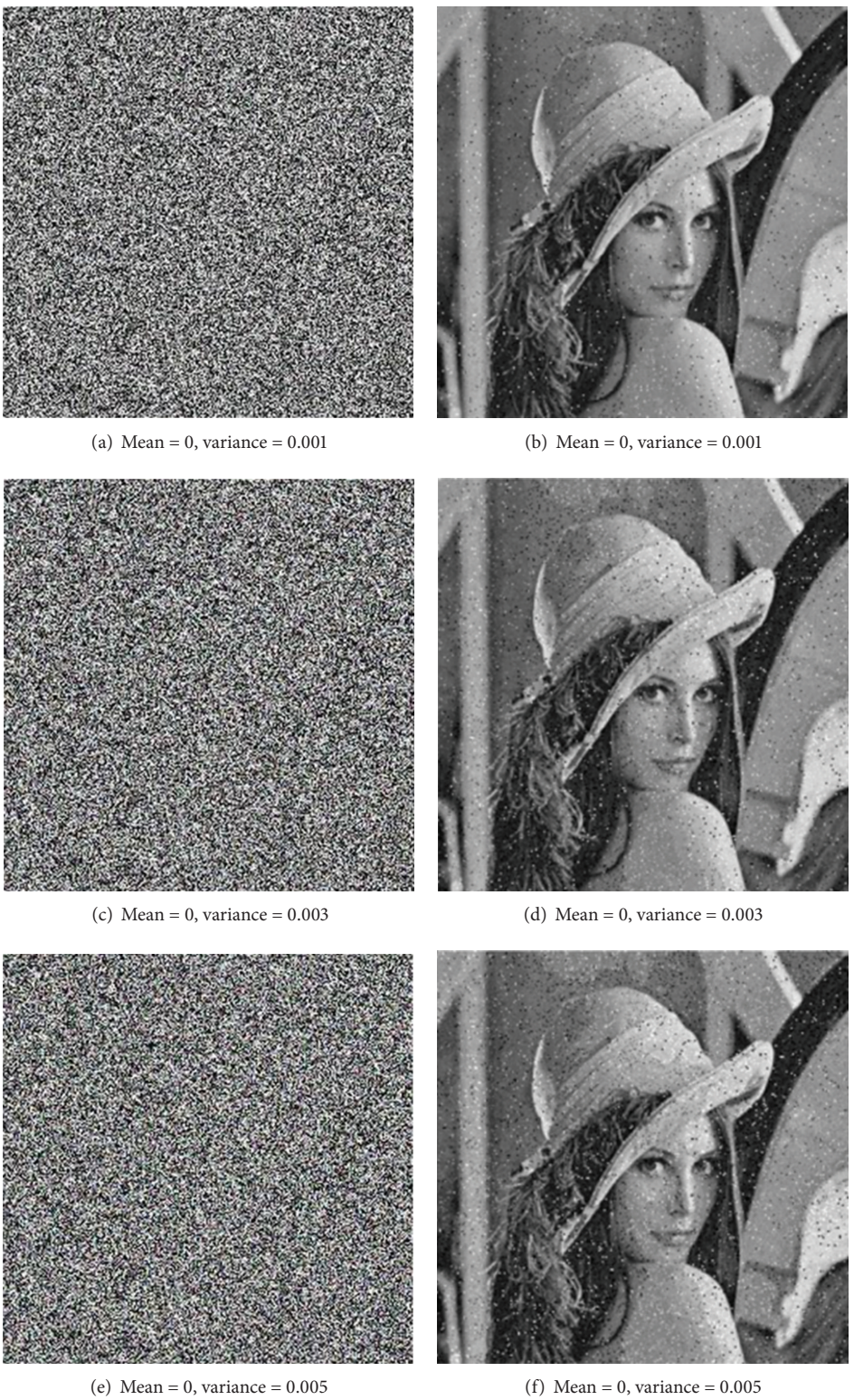
Correlation	Horizontal	Vertical	Diagonal
Original image	0.9765	0.9139	0.9437
Encrypted image	0.0002	0.0024	−0.0032
Zhang et al. [13]	0.0036	0.0023	0.0039
Zhang et al. [14]	0.0046	0.0040	0.0017

5.3. Information Entropy Analysis. Information entropy is the average information from which the redundant part has been excluded. Information entropy is the most important feature of randomness. Let m be the information source; the formula for calculating information entropy is as follows [13]:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log \frac{1}{p(m_i)}, \tag{16}$$

where $p(m_i)$ represents the probability of m. Assume that there are 2^8 information source states and that they appear with the same probability; then, according to (16), we obtain the ideal $H(m) = 8$, which indicates that the information is random. Hence, the information entropy of the encrypted image should be close to eight, and the closer it gets to eight, the harder the cryptosystem leaves information available [14]. We used (16) to calculate the information entropy of the encrypted image of Lena and Shrek (Table 3). Since the obtained values are all close to the ideal value of eight, the probability of accidental information leakage is minuscule.

5.4. Differential Attack. A general requirement for all image encryption schemes is that the encrypted image be significantly different from its original version. This difference can be measured by means of two criteria: namely, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI). NPCR is the change rate of the encrypted image pixels when the image changes one pixel in the process of encryption. The larger NPCR is, the stronger the resistance is of the algorithm to plaintext attack. UACI is the change rate of the average strength of the original image



(a) Mean = 0, variance = 0.001

(b) Mean = 0, variance = 0.001

(c) Mean = 0, variance = 0.003

(d) Mean = 0, variance = 0.003

(e) Mean = 0, variance = 0.005

(f) Mean = 0, variance = 0.005

Figure 5: Encrypted images with noise and their corresponding decrypted images.

Table 3: Information entropy values.

Image	Lena	Shrek
Original image	7.4224	7.3104
Encrypted image	7.9854	7.9479

Table 4: Correlation, NPCR, and UACI for the encrypted Lena and Shrek.

Image	Correlation	NPCR (%)	UACI (%)
Figures 2(a) and 2(c)	0.0028	99.7017	28.2970
Figures 2(d) and 2(f)	−0.0075	95.9316	26.0718
Zhang et al. [13]	0.0033	99.61	38

and the encrypted image. The larger UACI is, the stronger the resistance is of the algorithm to differential attacks [26].

The formulas used to calculate NPCR and UACI are as follows:

$$\begin{aligned} \text{NPCR} &= \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \\ \text{UACI} &= \frac{1}{W \times H}\left[\sum_{i,j} \frac{\left|C(i,j) - C'(i,j)\right|}{255}\right] \times 100\%, \end{aligned} \tag{17}$$

where W and H represent the width and height of the image, respectively. C and C' denote the encrypted images before and after one pixel of the plain image is changed. For the pixel at position (i, j), if $C(i, j) \neq C'(i, j)$, let $D(i, j) = 1$; else, let $D(i, j) = 0$.

We calculated the correlation coefficients, NPCR, and UACI of the original and encrypted images of Lena and Shrek (Table 4) and subsequently deduced that our algorithm is robust against differential attacks.

5.5. Robustness against Noise. One of the most important problems in real-world communication technology is the robustness of a cryptosystem against noise. Signal-independent noise very often occurs between the transmitter and the receiver when an image is transmitted electronically. The error propagation phenomenon implies that errors in the encrypted image will lead to errors in the decrypted image [23]. A good algorithm is designed to avoid the propagation error in the decrypted image.

Our cryptosystem is robust against noise because we first diffuse the pixels by permuting the rows and columns and then confuse each pixel according to the DNA complementary rule. Since the pixels changed by the noise will not propagate in the decrypted image during the decryption process, our algorithm is very robust against noise.

We prefer to use white Gaussian noise because it provides a reasonable assumption for the unavoidable randomness of the real physical channel, and the random numbers of this type of noise are uniformly distributed [23].

Figure 5 shows Lena's encrypted images affected by white Gaussian noise with various variances and the corresponding decrypted images. Table 5 summarizes the mean value of the correlation coefficients, NPCR, and UACI of Lena's noisy decrypted and original images; although NPCR > 99% and UACI > 28%, visually, the noisy decrypted images maintain the overall information contained in the original images and their correlations are still high.

Table 5: Correlation coefficient, NPCR, and UACI between original and decrypted images of Lena in the presence of noise.

Image	Correlation	NPCR (%)	UACI (%)
Figures 5(b) and 2(a)	0.9499	99.2988	28.4779
Figures 5(d) and 2(a)	0.9287	99.6154	28.5392
Figures 5(f) and 2(a)	0.9096	99.6627	28.7051

6. Conclusion

In this paper, we proposed a novel confusion/diffusion algorithm for image encryption. First, we exchanged the pixel positions of rows and columns of the digital image according to a chaotic index based on the logistic chaotic map to confuse the image pixels. Then, we encoded each of the pixels that had been confused into four nucleotides and obtained a one-dimensional nucleotide sequence after a series of iterative computations based on Chebyshev's chaotic map. Next, we transformed each nucleotide into its corresponding base pair a random number of time(s) according to the complementary rule. Finally, we converted the two-dimensional matrix obtained into an encrypted image. Our experimental results and security analyses show that the scheme can achieve not only good encryption results, but also a sufficiently large key space to be able to repel common attacks. Therefore, the scheme is reliable enough to be applied in image encryption.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the Fundamental Research Funds for the Central Universities (DL13CB04) and 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*, 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 and 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] 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.

[16] 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.

[17] 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.

[18] M. Shan, J. Chang, Z. Zhong, and B. Hao, "Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps," *Optics Communications*, vol. 285, no. 21-22, pp. 4227–4234, 2012.

[19] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Computers and Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, 2012.

[20] A. A. Abd El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, no. 11, pp. 2986–3000, 2013.

[21] M. François, T. Grosges, D. Barchiesi, and R. Erra, "A new image encryption scheme based on a chaotic function," *Signal Processing: Image Communication*, vol. 27, no. 3, pp. 249–259, 2012.

[22] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

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

[24] 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.

[25] I. Hussain, T. Shah, and M. A. Gondal, "Application of S-box and chaotic map for image encryption," *Mathematical and Computer Modelling*, vol. 57, no. 9-10, pp. 2576–2579, 2013.

[26] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.