Hindawi Publishing Corporation
Discrete Dynamics in Nature and Society
Volume 2016, Article ID 5408529, 9 pages
http://dx.doi.org/10.1155/2016/5408529

Research Article

An Image Encryption Scheme Based on DNA Computing and Cellular Automata

Shihua Zhou, Bin Wang, Xuedong Zheng, and Changjun Zhou

Key Laboratory of Advanced Design and Intelligent Computing, Dalian University, Ministry of Education, Dalian 116622, China

Correspondence should be addressed to Shihua Zhou; shihuajo@gmail.com

Received 7 June 2016; Revised 15 August 2016; Accepted 22 August 2016

Academic Editor: Charalampos Skokos

Networks have developed very quickly, allowing the speedy transfer of image information through Internet. However, the openness of these networks poses a serious threat to the security of image information. The field of image encryption has drawn attention for this reason. In this paper, the concepts of 1-dimensional DNA cellular automata and T-DNA cellular automata are defined, and the concept of reversible T-DNA cellular automata is introduced. An efficient approach to encryption involving reversible T-DNA cellular automata as an encryption tool and natural DNA sequences as the main keys is here proposed. The results of a simulation experiment, performance analysis, and comparison to other encryption algorithms showed this algorithm to be capable of resisting brute force attacks, statistical attacks, and differential attacks. It also enlarged the key space enormously. It meets the criteria for one-time pad and resolves the problem that one-time pad is difficult to save.

1. Introduction

As image information has become widely transmitted via Internet, the security of that image information has become more and more important [1, 2]. By using image encryption algorithms, the sender encrypts the plaintext into the ciphertext. Only the authorized receiver could decrypt the ciphertext with the secret key(s) to obtain the plaintext [3, 4]. The image encryption methods mainly include seven types, namely, mathematical concept-based image encryption techniques, secret segmentation and secret sharing-based image encryption techniques, compression methodology-based image encryption techniques, modern cryptography mechanism-based image encryption technique, the transform domain-based image encryption techniques, chaos-based image encryption techniques, and DNA cryptography-based image encryption techniques. Mathematical concept-based image encryption techniques are to apply the mathematical problems to design the encryption algorithms [5]. Secret segmentation is that the information is separated into a lot of pieces, and every piece does not have the individual meanings [6, 7]. The main idea of compression methodology-based image encryption techniques is that the compressed image is encrypted [8]. Modern cryptography mechanism-based image encryption techniques are to consider the entire 2D image data as a 1D textual bitstream and then to apply any conventional cipher that has been validated in modern cryptography such as DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), and AES (Advanced Encryption Standard) to encrypt [9]. The main idea of the transform domain-based image encryption is that the digital image is operated in the transform domain. Then the pretreated information is encrypted by using other techniques especially chaos [10, 11]. The pretreatment techniques include fractional Fourier transform (FRT), Discrete Wavelet Transform (DWT), and so on. A large number of image encryption algorithms based on chaos have been proposed. Of these chaos-based algorithms, image encryption algorithms are one of the most important. Unfortunately, many of these approaches have been shown to be insecure [12–15]. DNA-cryptography-based encryption is also an area of furious activity. The security mainly depends on the restrictions of biotechnology, which have nothing to do with computing power [16–22].

In the traditional image encryption methods, mathematical formulas or mathematical model is used through limited iterative calculation so as to achieve the purpose of encryption. Decryption is the inverse of the encryption process. These methods only own computational security. In other words, when the attacker has unlimited computing power, these cryptosystems can be cracked theoretically. With computer technology becoming more updated and the continuous development of cryptanalysis, many traditional encryption methods which were considered to be safe in the past have become no longer strong. Only one-time pad is still safe. Though one-time pad is the most safe encryption method at present, because it is very difficult to save a huge one-time pad, so the use of the existing one-time pad is limited to a great extent. At present, DNA cryptography has made some achievements, but DNA-cryptography-based image encryption is still immature and there are a lot of problems that require solutions. For example, encoding process is complicated, and biological operation error is bigger, and the experimental cost is expensive. In DNA experiment, the error is accumulated in the product way, so the success rate of each step is must be very high. Otherwise, the results may differ with the actual message. However, the biological level does not completely meet the requirements of high success rate. The laboratory with the excellent equipment is needed to complete a series of experiments, so the cost of experiment is very high. Therefore, based on some biological characteristics of DNA computing, it has become the most feasible way that the existing biological operation simulation system is used to execute pseudo operation of DNA computing in order to realize the information encryption. In this paper, we focus on a new approach to image encryption based on reversible T-DNA cellular automata. This method is the combination of DNA computing and cellular automata. In this way, natural DNA sequences can serve as excellent one-time pads. Therefore, not only does this encryption method inherit the high security of one-time pad, but also the operation is simple and the implementation is easy. The concept of 1-dimensional DNA cellular automata is defined, and the concept of T-DNA cellular automata is introduced. Reversible T-DNA cellular automata, DNA key matrix, and the flow of the encryption algorithm are also discussed. The results of relevant experiments and of algorithm performance analysis are shown.

2. DNA Cellular Automata

2.1. 1-Dimensional DNA Cellular Automata. Cellular automata (CA) make up a dynamic system in which space and time are discrete [23]. The cells, which are arranged in the form of a regular lattice structure, have a finite number of states. These states are updated synchronously according to a specified local rule of interaction. In this paper, a 1-dimensional DNA cellular automaton is defined. It consists of a line of cells. A DNA sequence contains four nucleic acid bases, A (adenine), C (cytosine), G (guanine), and T (thymine). A and T complement each other, and C and G complement each other. A given node s here serves as one of four state values, $s \in S = \{A, C, G, T\}$, and the neighborhood radius is r. The nodes closest to node s are those to its left and right. In that way, node s has a local neighborhood of $2r$ cells, and $f : s^{2r+1} \to s$ is the transfer function at discrete time. The state of s at time $t + 1$ is determined by the states of the cells within its neighborhood at time t, and let

$$s_i^{t+1} = f\left(s_{i-r}^t, \ldots, s_{i-1}^t, s_i^t, s_{i+1}^t, \ldots, s_{i+r}^t\right), \tag{1}$$

where s_i^{t+1} represents the state of the ith cell at discrete time $t + 1$.

Consider a 1-dimensional, $r = 1$ DNA cellular automaton. At discrete time t, the state of the ith cell is s_i^t, whose two neighbors are in the following states: s_{i-1}^t and s_{i+1}^t. The evolution of the cellular automata is expressed

$$s_i^{t+1} = f\left(s_{i-1}^t, s_i^t, s_{i+1}^t\right). \tag{2}$$

2.2. T-DNA Cellular Automata. T-DNA cellular automaton (T-DNA CA) is a particular type of DNA cellular automata. It is described in detail here. The specified node s and its three nearest neighbors (left, right, and bottom) form a T-shaped neighborhood. The state of the given node s at time $t + 1$ will be determined from the states of the nodes within itself. According to a specified rule, the state values are updated synchronously at discrete intervals for all cells. With a T-DNA cellular automaton, each cell can take any of the four bases {A, C, G, T}. When the radius $r = 1$, the T-DNA cellular automaton is called an elementary T-DNA cellular automaton (ET-DNA CA). In that case, the closet nodes to the node s are those to its left, right, and bottom. At discrete time t, the state of the location (i, j) of the cell is $s_{i,j}^t$, and its three closest nodes are in the following states: $s_{i,j-1}^t$, $s_{i,j+1}^t$, and $s_{i+1,j}^t$. The evolution of T-DNA cellular automata is expressed

$$s_{i,j}^{t+1} = f\left(s_{i,j-1}^t, s_{i,j}^t, s_{i,j+1}^t, s_{i+1,j}^t\right). \tag{3}$$

3. A New Image Encryption Scheme

3.1. RT-DNA Cellular Automata. Reversible cellular automata (RCA) [24], known as invertible cellular automata, are cellular automata that preserve information completely. RCA are among the most closely studied types of cellular automata. Many studies have been performed on this subject since the early 1960s. In this section, the concept of reversible T-DNA cellular automata (RT-DNA CA) is introduced, and the means by which they can be used to encrypt and decrypt the image information are discussed. Based on the concept of EDNA CA and the concept of T-DNA CA, we give a special design method of T-DNA CA so that it can be appropriate for image encryption. The rules of EDNA CA and a $(r = 0)$ DNA CA were here used to structure a special T-DNA CA by DNA XOR operation. This type of the above cellular automata is called a ST-DNA cellular automaton (ST-DNA CA). f is the transfer function of EDNA CA at discrete time, and F

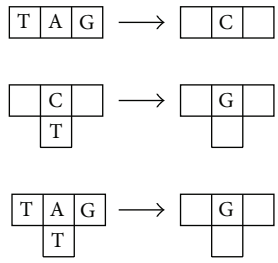


Figure 1: A simple example of the new T-DNA CA.

is the transfer function of ST-DNA CA at discrete time. The evolution is expressed

$$\begin{aligned} s_{i,j}^{t+1} &= f\left(s_{i,j-1}^{t}, s_{i,j}^{t}, s_{i,j+1}^{t}\right) \oplus s_{i+1,j}^{t} \\ &= F\left(s_{i,j-1}^{t}, s_{i,j}^{t}, s_{i,j+1}^{t}, s_{i+1,j}^{t}\right). \end{aligned} \tag{4}$$

A simple example is shown in Figure 1. In order to meet the specific requirements of image encryption, the ST-DNA CA given above must be improved. The newly produced cell was used instead of the original cell. The transfer function F at discrete time of the improved ST-DNA CA is

$$\begin{aligned} s_{i,j}^{t+1} &= f\left(s_{i,j-1}^{t+1}, s_{i,j}^{t}, s_{i,j=1}^{t}\right) \oplus s_{i+1,j}^{t} \\ &= F\left(s_{i,j-1}^{t+1}, s_{i,j}^{t}, s_{i,j+1}^{t}, s_{i+1,j}^{t}\right). \end{aligned} \tag{5}$$

The other ($r = 0$) DNA CA is then used (s_2 is the node of this DNA CA, $s_2 \in S_2 = \{\mathrm{A}, \mathrm{C}, \mathrm{G}, \mathrm{T}\}$) to improve the above ST-DNA CA further so as to produce the avalanche effect of encryption processes, and let

$$\begin{aligned} s_{1(i,j)}^{t+1} &= f\left(s_{1(i,j-1)}^{t+1}, s_{1(i,j)}^{t}, s_{1(i,j+1)}^{t}\right) \oplus s_{2(i,j)} \\ &= F\left(s_{1(i,j-1)}^{t+1}, s_{1(i,j)}^{t}, s_{1(i,j+1)}^{t}, s_{2(i,j)}\right). \end{aligned} \tag{6}$$

When the above ST-DNA CA is a reversible cellular automaton, here called a RT-DNA cellular automaton (RT-DNA CA). In the reverse process, each cell is replaced in by its predecessor cell backward. It can be written as

$$\begin{aligned} s_{1(i,j)}^{t} &= f^{-1}\left(s_{1(i,j-1)}^{t+1}, s_{1(i,j)}^{t+1}, s_{1(i,j+1)}^{t}\right) \oplus s_{2(i,j)} \\ &= F^{-1}\left(s_{1(i,j-1)}^{t+1}, s_{1(i,j)}^{t+1}, s_{1(i,j+1)}^{t}, s_{2(i,j)}\right). \end{aligned} \tag{7}$$

The original EDNA CA can be used to describe the original image, the ($r = 0$) DNA CA expresses the key, and the encryption and decryption processes are performed using the rule of RT-DNA CA. In this algorithm, DNA sequences are used instead of pixel gray values. For each pixel, the range of gray values was 0–255, specifically 00000000–11111111. Here, four bases were used to express each gray value, in which 00, 01, 10, and 11 were replaced by A, C, G, and T. For example, the binary string of a pixel gray value of 54 is 00110110, and the corresponding DNA sequence is ATCG. A simple example is shown in Figures 2 and 3, in which Figure 2 shows the encryption processes using (6), and Figure 3 shows the decryption processes using (7). The original pixel value is 210, and the original EDNA CA is TCAG. The given ($r = 0$) DNA CA is CAGC. After encryption, the gray value becomes 233.

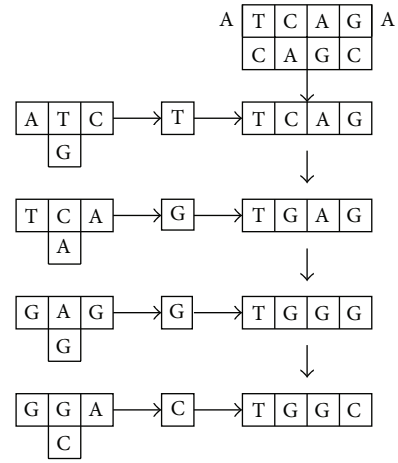


Figure 2: Encryption processes by RT-DNA CA.

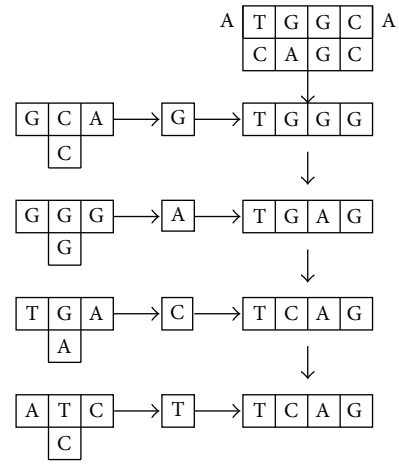


Figure 3: Decryption processes by RT-DNA CA.

3.2. DNA Sequence Operation

3.2.1. DNA XOR Operation. A new DNA XOR operation is here defined. It can achieve exclusive XOR operation between two DNA sequences. Table 1 shows the rules underlying DNA XOR operation. For example, A and T are processed with C, respectively, producing C and G. C and G are satisfied with the Watson-Crick complement regulation.

3.2.2. DNA Multiplication Operation. A DNA multiplication operation that can work on two sequences is here defined. Table 2 shows the rule of DNA multiplication operation. As shown in Table 2, any pair of complementary bases by DNA multiplication operation with any base is also complementary. For example, A and T are processed with C, producing G and C. G and C are satisfied with the Watson-Crick complement regulation.

3.2.3. DNA Matrix Multiplication Operation. In this paper, a new rule of DNA matrix multiplication operation is

Table 1: XOR operation of DNA sequence.

⊕	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 2: Multiplication operation of DNA sequence.

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

used. Two DNA sequences $I_1 = \{d_{11}, d_{12}, \ldots, d_{1l_{I_1}}\}$ and $I_2 = \{d_{21}, d_{22}, \ldots, d_{2l_{I_2}}\}$ are given. Their lengths are l_{I_1} and l_{I_2}. I_1 and I_2 are reconstructed as two matrices $D_1 = [d_{11}, d_{12}, \ldots, d_{1l_{I_1}}]^{-1}$ and $D_2 = [d_{21}, d_{22}, \ldots, d_{2l_{I_2}}]$. Performing DNA multiplication operation is similar to that of general matrix multiplication for D_1 and D_2. This produces the matrix D whose size is $l_{I_1} \times l_{I_2}$. The formula is written as

$$D = D_1 \times D_2 = \begin{bmatrix} d_{11} \\ d_{12} \\ \vdots \\ d_{1l_{I_1}} \end{bmatrix} \times \left[d_{21}, d_{22}, \ldots, d_{2l_{I_2}} \right] = \begin{bmatrix} d_{11}d_{21} & d_{11}d_{22} & \cdots & d_{11}d_{2l_{I_2}} \\ d_{12}d_{21} & d_{12}d_{22} & \cdots & d_{12}d_{2l_{I_2}} \\ \vdots & \vdots & \vdots & \vdots \\ d_{1l_{I_1}}d_{21} & d_{1l_{I_1}}d_{22} & \cdots & d_{1l_{I_1}}d_{2l_{I_2}} \end{bmatrix}. \tag{8}$$

The inner elements $(d_1 d_2)$ in the matrix D are calculated according to the rule of DNA multiplication operation, as shown in Table 2. For example, $D_1 = [\mathrm{ACGT}]^{-1}$ and $D_2 = [\mathrm{CTAG}]$ are set; hence their multiplication is written as

$$D_1 \times D_2 = \begin{bmatrix} \mathrm{AC} & \mathrm{AT} & \mathrm{AA} & \mathrm{AG} \\ \mathrm{CC} & \mathrm{CT} & \mathrm{CA} & \mathrm{CG} \\ \mathrm{GC} & \mathrm{GT} & \mathrm{GA} & \mathrm{GG} \\ \mathrm{TC} & \mathrm{TT} & \mathrm{TA} & \mathrm{TG} \end{bmatrix} = \begin{bmatrix} \mathrm{A} & \mathrm{G} & \mathrm{T} & \mathrm{C} \\ \mathrm{T} & \mathrm{C} & \mathrm{G} & \mathrm{A} \\ \mathrm{G} & \mathrm{A} & \mathrm{C} & \mathrm{T} \\ \mathrm{C} & \mathrm{T} & \mathrm{A} & \mathrm{G} \end{bmatrix}. \tag{9}$$

3.3. Modified DNA Matrix. Here, we designed modified DNA matrix. The gray image $A_{m\times n}$ is $m \times n$ in size. a_{ij} is the gray value of the image pixel, where $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$.

Step 1. SUM and x_{sum} are calculated. SUM is the sum of all pixel values of the image, and let

$$\mathrm{SUM} = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}.$$

$$x_{\mathrm{sum}} = 10000 \times \frac{\mathrm{SUM}}{(m \times n \times 255)} - \left\lfloor 10000 \times \frac{\mathrm{SUM}}{(m \times n \times 255)} \right\rfloor \tag{10}$$

Step 2. A modified value x_{DNA} was designed

$$x_{\mathrm{DNA}} = \frac{\sum_{i=1}^{l} (i \times \omega_i)}{\sum_{i=1}^{l} (3 \times i)}, \tag{11}$$

where ω is weight (the weights of A, C, G, and T are 0, 1, 2, and 3, resp.) and l is the length of the DNA sequence. One DNA sequence is transformed into a decimal.

Step 3. The original value x_0 of chaos is calculated, and let

$$x_0 = \mathrm{mod}\left(\left(x_{\mathrm{SUM}} + x_{\mathrm{DNA}} \right), 1 \right). \tag{12}$$

Step 4. The chaotic sequence z is produced using Logistic Map:

$$x_{i+1} = \mu x_i \left(1 - x_i\right), \tag{13}$$

according to the original value x_0 and the given μ, whose length is $m \times n \times 4$.

Step 5. A new sequence d_T is produced by

$$f(x) = \begin{cases} \mathrm{A} & 0 < z(i,j) \le 0.25 \\ \mathrm{C} & 0.25 < z(i,j) \le 0.5 \\ \mathrm{G} & 0.5 < z(i,j) \le 0.75 \\ \mathrm{T} & 0.75 < z(i,j) < 1. \end{cases} \tag{14}$$

Step 6. d_T is converted to one DNA matrix D_T, whose size is $m \times (n \times 4)$.

3.4. Algorithm Design. In this paper, the original image was encrypted in the light of the definition of RT-DNA cellular automata using a DNA key matrix. Boundary conditions select periodic boundary conditions. There are two types of image encryption techniques, pixel permutation, and pixel diffusion. The encryption process includes XOR operation, which can cause pixel diffusion. At the same time, the preceding nodes affect the subsequent nodes, and the state of node can move backwards. Because periodic boundary conditions are adopted, the node in the rearmost position can act on the node in the first position. After several iterations, pixel permutation is achieved. Figure 4 shows a flow chart of this algorithm. The encryption approach is as follows.

Step 1. Input the original image A_0 whose size is $m \times n$, where m and n are number of rows and columns in the image, respectively.

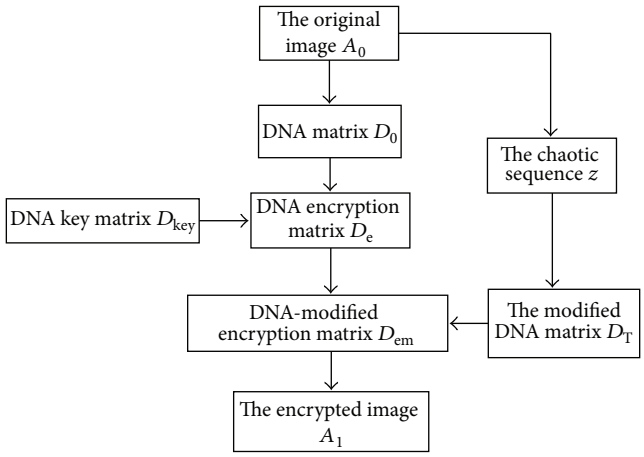


Figure 4: Flow chart.

Step 2. Convert the image to a binary matrix, and then perform DNA encoding on the binary matrix to produce a DNA matrix D_0, $m \times (n \times 4)$ in size.

Step 3. Gain DNA key matrix D_{key}. Two natural DNA sequences, d_1 and d_2, serve as the main keys. Then, the sequence d_1^1 and d_2^1 is produced through enlargement of the sequences d_1 and d_2, whose lengths are m and $n \times 4$, respectively. Then the DNA key matrix D_{key} is produced according to DNA matrix multiplication operation.

Step 4. Generate a DNA encryption matrix D_e. D_0 and the above DNA key matrix D_{key} are calculated according to the new RT-DNA cellular automaton rule shown.

Step 5. Generate the chaotic sequence z. According to the pixel values of the image and DNA sequence, the original value x_0 of the Logistic Map can be calculated. Then, the chaotic sequence z can be generated using the original value x_0 and the given μ, whose length is $m \times n \times 4$.

Step 6. Generate the modified DNA matrix D_T. The threshold function $f(x)$ can be used to produce a new sequence d_T. Its length is $m \times n \times 4$. Then d_T can be converted to one DNA template, D_T, whose size is $m \times (n \times 4)$.

Step 7. Generate a DNA-modified encryption matrix D_{em}. D_e and the DNA matrix D_T are calculated using a DNA XOR operation, and DNA-modified encryption matrix D_{em} is generated.

Step 8. Gain the encrypted image A_1. Perform the inverse processes of DNA encoding for the DNA encryption matrix D_{em}, and then gain the gray value matrix $I(m, n)$. The encrypted image A_1 is gained.

The processes of the decryption algorithm are the reverse of those involved in encryption. The recipient receives the encrypted image A_1 through the insecure channel and receives the secret keys through the secure channel from the senders. Recipients use keys to decrypt the encrypted image in light of the reverse operation of the encryption algorithm.

4. Experimental Results

In this paper, the results of a simulation were analyzed. They confirmed that the validity and effectiveness of the presented approach are demonstrated. For the original gray Lena image that is gained from http://www.cs.cmu.edu/~chuck/lennapg/ 256 × 256 in size, Matlab was used to simulate the present algorithm under the established conditions: the keys were 3053, 4, 57, 4321, 11, 50, 3.95, and 3. Two natural DNA sequences were used. The first one is a Gene ID of 3053 and its length is 57 from the 4th base. Another is a Gene ID of 4321 and its length is 50 from the 11th base. The given μ is 3.95, and the encryption processes were performed 3 times.

The experimental results are shown in Figure 5. Figure 5(a) shows the original image, and Figure 5(b) is the encrypted image. When the recipient receives the true keys, the encrypted image can be encrypted using the decryption algorithm, and the decrypted image is shown in Figure 5(c). The experimental results show that the new encryption approach is feasible and satisfactory.

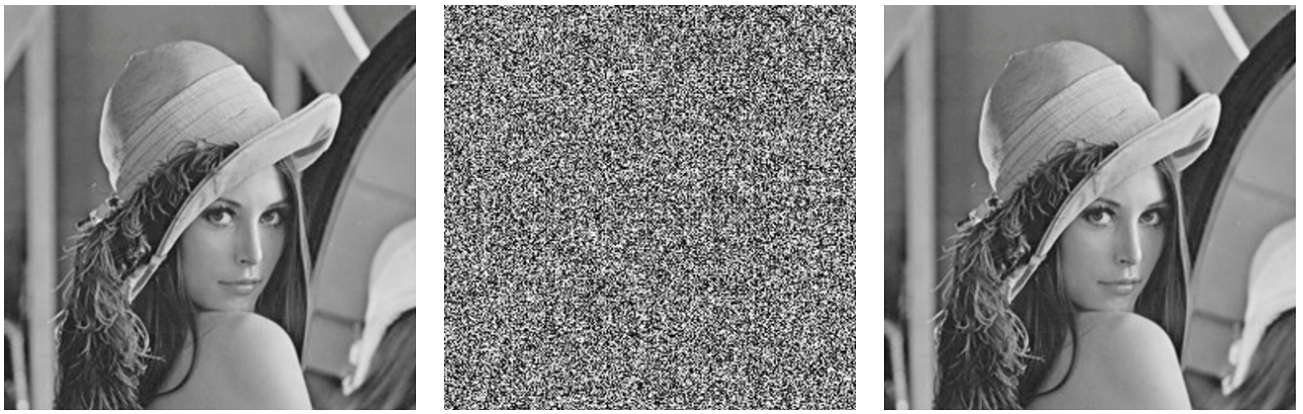
5. Algorithm Performance Analysis

5.1. Key Space Analysis. According to the hypothesis proposed by Kerckhoff, it must be assumed that the attacker knows all relevant information except for the secret key. Consequently, the key space must be large enough to repel a brute force attack. In nature, DNA sequences can vary considerably in both primary structure and length. Even in the same DNA sequence, the length and primary structure can seem to differ if a different start position is selected. In this way, natural DNA sequences can serve as excellent one-time pads. Recent developments in genetic engineering have increased contents of gene banks to tremendous proportions. In this approach to encryption, natural DNA sequences served as primary secret keys. The key space of the present algorithm is $4^{m+n\times4}$, where m and n are the number of rows and columns in the image, respectively. For a gray image 256 × 256 in size, the key space is $4^{256+256\times4} = 2^{2560}$. A comparison to other encryption algorithms is shown in Table 3. This table shows the largest key space of the algorithms in previous studies to be 10^{157}. The key space of the present algorithm is 2^{2560}, suggesting that it would be able to resist brute force attacks more easily. This meets the criteria for a one-time pad. Key management problems are not an issue. Only the Gene ID, starting location, and length of the DNA sequences need to be transmitted. The recipient can retrieve the DNA sequence itself from GenBank.

5.2. Key Sensitivity Analysis. The algorithm was tested with various decryption keys for further analysis of key sensitivity. For example, the decryption keys are 3053, 4, 57, 4320, 11, 50, 3.95, and 3. Figure 6(a) shows the original image, and Figure 6(b) shows encrypted images. Figure 6(c) shows image decrypted using the wrong keys. This image is different

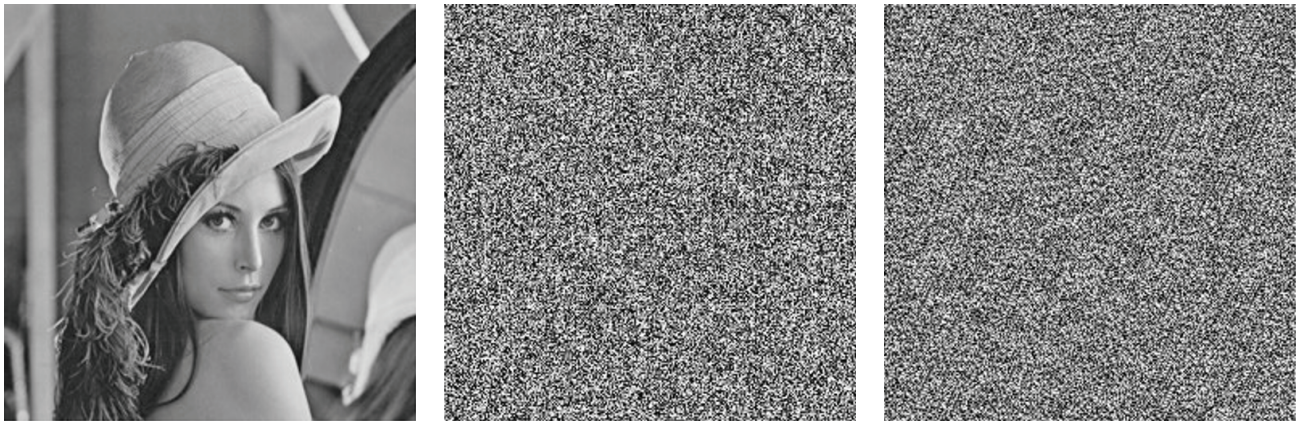
Table 3: Comparison of key spaces.

Algorithm	Reference [2]	Reference [7]	Reference [12]	Reference [13]	Reference [14]	Ours
Key space	$2^{16} \cdot n$	2^{174}	10^{56}	10^{156}	10^{157}	2^{2560}



(a) (b) (c)

Figure 5: Experimental results for the image.



(a) (b) (c)

Figure 6: Experimental results of the wrong Key.

considerably from the original image, providing almost no information about the original image.

5.3. Correlation Coefficient Analysis. In this section, the correlation between two adjacent pixels of the encrypted image was evaluated statistically. First, 3000 pairs of adjacent pixels were randomly selected in the horizontal, vertical, and diagonal directions respectively.

Comparison with other encryption algorithms is shown in Table 4. This table shows that the present algorithm is as effective as the others.

5.4. Differential Attack. Differential attacks take place when attackers make slight changes to the original image. The proposed algorithm was here used to encrypt the original image before and after one pixel being changed. This was performed through comparison of two encrypted images to show the relationship between the original and encrypted images. Here, the encrypted image is called test 1, and the encrypted image after changing the one pixel gray value from test 1 is called test 2. Researchers usually use NPCR (number

Table 4: Comparison with other encryption algorithms.

Algorithm	Horizontal	Vertical	Diagonal
Reference [2]	N/A	N/A	N/A
Reference [7]	−0.146	−0.0028	−0.0240
Reference [12]	0.024178	−0.0194	0.0243
Reference [13]	$-8.1928e-0.04$	0.0016	0.0115
Reference [14]	0.0005	−0.0020	−0.0008
Ours	0.0105	0.0058	0.0073

Table 5: NPCR test for the different image encryption algorithms.

	Experimental value	0.05-level	0.01-level	0.001-level
Reference [2]	N/A	Fail	Fail	Fail
Reference [7]	N/A	Fail	Fail	Fail
Reference [12]	93.6768%	Fail	Fail	Fail
Reference [13]	99.8093%	Pass	Pass	Pass
Reference [14]	99.72%	Pass	Pass	Pass
Ours	99.5619%	Fail	Pass	Pass

Table 6: UACI test for the different image encryption algorithms.

	Experimental value	0.05-level	0.01-level	0.001-level
Reference [2]	N/A	Fail	Fail	Fail
Reference [7]	N/A	Fail	Fail	Fail
Reference [12]	33.3464%	Pass	Pass	Pass
Reference [13]	45.6606%	Fail	Fail	Fail
Reference [14]	32.82%	Fail	Fail	Fail
Ours	33.3315%	Fail	Pass	Pass

Table 7: Comparison with the simulation algorithms.

	Key space	Key sensitivity	Statistical attack	Differential attack
Reference [2]	Small	Yes	Yes	No
Reference [7]	Small	Yes	Yes	No
Reference [12]	Small	Yes	Yes	Weak
Reference [13]	Small	Yes	Yes	Weak
Reference [14]	Small	Yes	Yes	Weak
Ours	Large	Yes	Yes	Strong

of pixels change rate) and UACI (unified average changing intensity) as criteria for examination of the ability of an algorithm to resist differential attack.

In one previous study, authors established a mathematical model of ideally encrypted images and derived expectations and variances of NPCR and UACI [25]. In the present paper, these theoretical values were used to analyze our NPCR and UACI. The results of the present algorithm were compared to those produced by five other algorithms according to criteria established in a previous study [25] (Tables 5 and 6). Table 5 shows a NPCR test of different image encryption algorithms, and Table 6 shows a UACI test. There were 6 criteria across 3 levels. The other algorithms failed at last in 3 criteria, and the first and second algorithms failed all of them. For the present algorithm, only one criterion did not meet the theoretical values, and it is fairly close to the theoretical value. This comparison demonstrates that the present algorithm can resist differential attack very effectively.

5.5. Comparison with Others' Work. A large number of image encryption algorithms have been proposed. Chaos-based image encryption research is a very important field. A lot of chaos-based image encryption schemes have been proposed. Unfortunately, many of these schemes have been found to be insecure, especially against known and chosen-plaintext attacks. Some CA-based algorithms have also been presented. However, the disadvantages are very obvious. For example, an excess of information must be transferred through secure channels. Researchers have shown that traditional image encryption schemes other than those involving one-time pad involve only computational security. DNA cryptography-based image encryption has become a hot research field. The main security basis depends on the limits of biotechnology, which have nothing to do with computing power. For example, Clelland et al. [16] proposed an approach based on microdots. In this approach, the researchers produced artificial DNA strands containing secret messages. However, the current method of DNA cryptography-based image encryption is still in the immature stage. The main difficulties involved in DNA cryptography-based image encryption are the absence of effective secure theory and the simple and realizable method. The results of the encryption only depend on the physical means of transmission.

Tables 7 and 8 show a comparison of results produced by present and other algorithms. Table 7 shows comparison with simulation algorithms. Five different encryption algorithms have been evaluated in previous studies [2, 7, 12–14]. The first algorithm involves the general cellular automata technique. The second involves the elliptical curve ElGamal encryption. A spatiotemporal chaotic system is used in the third. The fourth one and the last one use chaos to encrypt the image. The five previous algorithms and the present algorithm

Table 8: Comparison with the biotic experimental algorithms.

	Text	Image	Bioexperiment	Internet transfer
Reference [16]	Yes	Yes	Yes	No
Reference [17]	Yes	No	Yes	No
Reference [18]	Yes	No	Yes	No
Reference [19]	Yes	No	Yes	No
Reference [20]	Yes	No	Yes	No
Reference [21]	Yes	No	Yes	No
Reference [22]	Yes	No	No	Yes
Ours	Yes	Yes	No	Yes

are all sensitive to slight changes of the keys. This allows them to resist statistical attacks effectively. However, only can the third, fourth, fifth, and presented algorithms resist differential attacks. The largest key space in any of the previous algorithms was 10^{157}, but the present algorithm has a key space of 2^{2560}. The encrypted sequences generated by keys in algorithms showed some connection between elements. In other words, the back element is produced by the front element and one or more functions, such as chaos maps. Attackers may find the entire encrypted sequence by analyzing some of the elements. However, the main keys of the present algorithm are natural DNA sequences, and any bases in the key sequence cannot be affected by other bases. This meets the property of one-time pads. In this way, the present algorithm not only has advantages over other algorithms, but also enlarges key space enormously. This may be used to save one-time pads.

Table 8 shows a comparison of DNA cryptography-based algorithms. Seven encryption algorithms based on DNA cryptography have been evaluated in previous studies [16–22]. The first algorithm [16] uses base redundancy. DNA microdots and PCR were used in the second algorithm [17]. The third and fourth algorithms [18, 19] rely on DNA microarrays. The fifth one [20] uses the DNA binary sequence rule. The sixth one [21] uses DNA self-assembly technique. The last algorithm [22] encrypted the data using a new DNA encoding rule. The first six different encryption algorithms have been used in biotic experiments. These six algorithms can all be used to encrypt text information, but they are fit to encrypt image information except for the fourth one. Although the fourth encryption algorithm can encrypt binary image better, it cannot encrypt gray image and color image. Because of the encrypted boundedness of this kind of algorithm, the complicated bioexperimental operation and the high cost, its development has been limited considerably. The results of encryption must be transferred physically. For this reason, researchers have shifted their attention to computer simulations. They use computers to simulate bioexperiments and to use DNA sequences for encryption. The last algorithm presents a new DNA encoding approach that uses randomized assignments of unique error correcting DNA Hamming code words for single character in the extended ASCII set. This algorithm does not rely on biotic experiments and can easily encrypt text information. However, it is complicated to use this algorithm to encrypt the image. In the our paper, the newly defined concept of RT-DNA cellular automata served as an encryption tool and the natural DNA sequences served as the main keys. The present algorithm not only encrypts text and image information effectively but also does not require any complicated procedure or large expenses. The results can be transferred via the Internet.

6. Conclusion

The concept of RT-DNA cellular automata can be used to complete the encryption processes. The concepts of 1-dimensional DNA CA and T-DNA CA are defined here for the first time. RT-DNA CA is here used to encrypt the image. Experimental results showed this approach to be simple and feasible. Performance analysis showed that this approach meets security requirements and can resist exhaustive attacks very effectively.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (nos. 61672121, 61572093, 61425002, 61402066, 61402067, 61370005, and 31370778), Program for Changjiang Scholars and Innovative Research Team in University (no. IRT_15R07), the Program for Liaoning Innovative Research Team in University (no. LT2015002), the Basic Research Program of the Key Lab in Liaoning Province Educational Department (nos. LZ2014049, LZ2015004), Natural Science Foundation of Liaoning Province (no. 2014020132), Scientific Research Fund of Liaoning Provincial Education (nos. L2015015, L2014499), and the Program for Liaoning Key Lab of Intelligent Information Processing and Network Technology in University.

References

[1] S. Zhou, Q. Zhang, X. Wei, and C. Zhou, "A summarization on image encryption," *IETE Technical Review*, vol. 27, no. 6, pp. 503–510, 2010.

[2] J. Jin, "Image encryption method based on elementary cellular automata," in *Proceedings of the IEEE Southeastcon 2009*, pp. 345–349, Atlanta, Ga, USA, March 2009.

[3] X. Li, C. Li, and I.-K. Lee, "Chaotic image encryption using pseudo-random masks and pixel mapping," *Signal Processing*, vol. 125, pp. 48–63, 2016.

[4] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[5] N. A. Abbas, "Image encryption based on independent component analysis and arnold's cat map," *Egyptian Informatics Journal*, vol. 17, no. 1, pp. 139–146, 2016.

[6] M. Mudia and P. Chavan, "Fuzzy logic based image encryption for confidential data transfer using (2,2) secret sharing scheme," *Procedia Computer Science*, vol. 78, pp. 632–639, 2016.

[7] L. Li, A. EL-Latif, and X. Niu, "Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images," *Signal Processing*, vol. 92, no. 4, pp. 1069–1078, 2012.

[8] R.-J. Chen and S.-J. Horng, "Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 413–426, 2010.

[9] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A modified AES based algorithm for image encryption," *World Academy of Science, Engineering and Technology*, vol. 3, pp. 526–531, 2007.

[10] M. Kumar and A. Vaish, "Encryption of color images using MSVD in DCST domain," *Optics and Lasers in Engineering*, vol. 88, pp. 51–59, 2017.

[11] J. B. Lima and L. F. G. Novaes, "Image encryption based on the fractional Fourier transform over finite fields," *Signal Processing*, vol. 94, no. 1, pp. 521–530, 2014.

[12] L. Teng and X. Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive," *Optics Communications*, vol. 285, no. 20, pp. 4048–4054, 2012.

[13] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Optics Communications*, vol. 284, no. 22, pp. 5290–5298, 2011.

[14] A. Kumar and M. K. Ghose, "Extended substitution-diffusion based image cipher using chaotic standard map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 1, pp. 372–382, 2011.

[15] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[16] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots," *Nature*, vol. 399, no. 6736, pp. 533–534, 1999.

[17] M. Arita and Y. Ohashi, "Secret signatures inside genomic DNA," *Biotechnology Progress*, vol. 20, no. 5, pp. 1605–1607, 2004.

[18] M. Lu, X. Lai, G. Xiao, and L. Qin, "Symmetric encryption method based on DNA technique," *Science in China E*, vol. 37, no. 2, pp. 175–182, 2007 (Chinese).

[19] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography," in *Aspects of Molecular Computing*, vol. 2950 of *Lecture Notes in Computer Science*, pp. 167–188, Springer, 2004.

[20] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with DNA binary strands," *BioSystems*, vol. 57, no. 1, pp. 13–22, 2000.

[21] K. Halvorsen and W. P. Wong, "Binary DNA nanostructures for data encryption," *PLoS ONE*, vol. 7, no. 9, Article ID e44212, 2012.

[22] D. Tulpan, C. Regoui, G. Durand, L. Belliveau, and S. Léger, "HyDEn: a hybrid steganocryptographic approach for data encryption using randomized error-correcting DNA codes," *BioMed Research International*, vol. 2013, Article ID 634832, 11 pages, 2013.

[23] S. Nandi, B. K. Kar, and P. Pal Chaudhuri, "Theory and applications of cellular automata in cryptography," *IEEE Transactions on Computers*, vol. 43, no. 12, pp. 1346–1357, 1994.

[24] J. Kari, "Reversible cellular automata," *Developments in Language Theory*, vol. 3572, pp. 2–23, 2005.

[25] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications*, pp. 31–38, 2011.