Optical Engineering

OpticalEngineering.SPIEDigitalLibrary.org

Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules

Shuliang Sun

SPIE.

Shuliang Sun, "Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules," *Opt. Eng.* **56**(11), 116117 (2017), doi: 10.1117/1.OE.56.11.116117.

Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules

Shuliang Sun[a,b,*]
[a]Fuqing Branch of Fujian Normal University, School of Electronics and Information Engineering, Fuqing, China
[b]Fuqing Branch of Fujian Normal University, Innovative Information Industry Research Center, Fuqing, China

Abstract. An image encryption technique has been proposed using deoxyribonucleic acid (DNA) operations and chaotic map in this scheme. First, initial conditions of row encryption and column encryption are calculated. Then, a two-dimensional sine iterative chaotic map with infinite collapse (ICMIC) modulation map (2D-SIMM) is adopted to produce chaotic sequences. Extended exclusive OR (XOR) is executed to enhance security. A mask matrix is produced by 2D-SIMM. It performs XOR operation with the DNA-encoded matrix. Finally, the revised DNA-encoded matrix is performed two-by-two DNA complementary rules and executed DNA decoding to obtain the cipher image. Experiment results prove that the proposed scheme is secure enough and can resist various attacks. [DOI: 10.1117/1.OE.56.11.116117]

Keywords: two-by-two deoxyribonucleic acid complementary rule; expanded exclusive OR; two-dimensional sine ICMIC modulation map.

Paper 171145 received Jul. 21, 2017; accepted for publication Nov. 13, 2017; published online Nov. 30, 2017.

1 Introduction

Recently, many image encryption methods have been proposed. The diffusion and confusion operations that are proposed by Shannon[1] in cryptography are also used in image encryption. Traditional encryption methods are improper for image encryption such as low efficiency, enormous data, high correlation, and so on.[2] Chen et al.[3] presented a real-time cryptosystem. The confusion and diffusion operations of this scheme were performed based on a lookup table. Chen et al.[4] also put forward an image encryption algorithm based on gray code. It was performed with high efficiency. The chaotic map is highly sensitive to initial values and system parameters, unpredictable, pseudorandom, and ergodic.[5] It is very suitable for an image encryption system. Liu et al.[6] proposed a double image encryption method based on random pixel exchanging and phase encoding in gyrator domains. Mao et al.[7] presented a fast image encryption method, which was based on three-dimensional chaotic baker maps. Sivakumar and Venkatesan[8] proposed an image encryption scheme. Knight's travel path and true random number were adopted in this method. Wang et al.[9] presented an efficient image encryption scheme using a two-step phase-shifting interference method, in fractional Fourier transform and random mixed encoding. Wang and Luan[10] proposed an image encryption scheme using reversible cellular automata and chaos.

Since deoxyribonucleic acid (DNA) computing supports high parallelism, it is also superior in massive storage and extremely low power consumption. Many DNA-based methods have been proposed nowadays.[11–15] Zhen et al.[12] presented an image encryption scheme based on chaotic sequence, DNA encoding, and entropy. Rehman et al.[13] proposed a method that was based on chaos and DNA complementary rules for gray images. The most significant and least significant parts of each block were encoded with different methods. Wang et al.[16] proposed an image encryption technique based on DNA sequence and coupled map lattice. The scheme could resist different attacks and enhance the system's security. Wang et al.[17] also designed an image encryption method based on a two-dimensional (2-D) logistic map and DNA sequence. DNA addition, DNA subtraction, and DNA complementary rules were used to obtain the ciphered image. Belazi et al.[18] designed an equivalent mathematical model of the cryptosystem and algebraic analysis was given. By finding equivalent keys, key space was reduced. The authors also proposed a recovering scheme with lower complexity than the actual decryption method. In Ref. 19, a 2-D logistic map was employed for row circular permutation and column circular permutation. Initial values and system parameters of the chaotic system were calculated first. Abd-El-Hafiz et al.[20] proposed two measures for the evaluation permutation skills. Two parameters were proposed in the program.

The rest of this paper is arranged as follows. Section 2 briefly introduces the two-dimensional sine iterative chaotic map with infinite collapse (ICMIC) modulation map (2D-SIMM), random number generation, DNA operations, and improved expanded exclusive OR (XOR) operation. Section 3 describes the proposed scheme. Section 4 depicts the simulation results. Section 5 presents security analysis and the conclusion is described in Sec. 6.

2 Preliminary Work

2.1 *Two-Dimensional Sine ICMIC Modulation Map*

2D-SIMM[21] is defined as

$$\begin{cases} x_{i+1} = a \sin(\pi y_i) \sin(b/x_i) \\ y_{i+1} = a \sin(\pi x_{i+1}) \sin(b/y_i) \end{cases}, \quad (1)$$

where a and b are the positive system parameters. While $a = 1$ and $b = 5$, the system of 2D-SIMM is a hyper chaotic map. Compared with the 2-D sine logistic modulation

*Address all correspondence to: Shuliang Sun, E-mail: tjussl_07@126.com

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

map (2D-SLMM)[22] and 2-D logistic map,[17] 2D-SIMM has better ergodicity, larger key space, more complex dynamical behaviors, and phase space trajectory.[21] More secure chaotic sequences could be produced with the system. 2D-SIMM is employed in this paper to generate chaotic sequences.

2.2 *Random Number Generation*

The sequences produced by 2D-SIMM are decimal real numbers. The fractional part of a real number is changed into equivalent binary format. The former 16 bits of binary value are separated into two halves each with 8 bits.[8] They are executed XOR operation to generate a random number finally.

The process can be described as follows. Suppose the value generated by 2D-SIMM is 0.63636. The binary bit streams of the fractional part are 10100010111010000111.....

The former 16 bits are 1010001011101000. The first half is $(T_{15-8}) = (10100010)2$, and the other half is $(T_{7-0}) = (11101000)2$. The generated random number $(R) = T_{15-8}$ XOR $T_{7-0} = (01001010)2$.

2.3 *Deoxyribonucleic Acid Operations*

DNA is two twisted strands, which are composed of four bases: adenine (A), cytosine (C), thymine (T), and guanine (G).[13] (A) and (G), respectively, bond with complement (T) and (C), and vice versa. 00, 01, 10, and 11 are represented as A, C, G, and T, respectively. Each pixel is transformed into a DNA sequence with length 4 in. 8-bit gray image. The rule for DNA XOR is shown in Table 1.

The DNA complementary rule must satisfy that[17]

$$\begin{cases} x \neq D(x) \neq D[D(x)] \neq D\{D[D(x)]\} \\ x = D(D\{D[D(x)]\}) \end{cases}, \tag{2}$$

where $D(x)$ is different from x in at least 1-bit position.

There are six DNA complementary rules as follows:

1. G → T, T → A, A → C, C → G;
2. G → T, T → C, C → A, A → G;
3. G → C, C → A, A → T, T → G;
4. G → C, C → T, T → A, A → G;
5. G → A, A → T, T → C, C → G; and
6. G → A, A → C, C → T, T → G.

A complementary rule[23] is defined, which processes the alphabet in doubles instead of one by one. Assume that (xx) is the token and $D(xx)$ defines its complement.

Table 2 A legal two-by-two complementary rule.

Token	Complement	Token	Complement
AA	CG	CG	TC
TC	GC	GC	CT
CT	TT	TT	AG
AG	TA	TA	GA
GA	CA	CA	AT
AT	CC	CC	GG
GG	TG	TG	GT
GT	AC	AC	AA

Here, the same property must apply as follows:

$$\begin{cases} xx \neq D(xx) \neq D[D(xx)] \neq D\{D[D(xx)]\} \neq \ldots \neq D^{15}(xx) \\ xx = D^{16}(xx) \end{cases}. \tag{3}$$

Notice that the double complement of xx is $D[D(xx)]$. $D\{D[D(xx)]\}$ is its triple complement and $D^{15}(xx)$ is its 15-fold complementary. The number of two-by-two complementary rules is 15! (1307674368000). It is far more than traditional complementary rules that total 3! (6) legal rules. The method could expand key space for a cryptographic system efficiently. A legal complementary rule is shown in Table 2.

2.4 *Improved Expanded XOR Operation*

The improved expanded XOR operation[24] is applied to enhance the security and to increase the complexity of information. For two inputs $x = \sum_{i=0}^{7} x_i \cdot 2^i$ and $r = \sum_{i=0}^{10} r_i \cdot 2^i$, the Extended XOR (eXOR) operation can be defined as

$$\mathrm{eXOR}(x, r) = \sum_{i=0}^{7} \mathrm{not}(x_i \oplus r_i \oplus r_{i+3}) \cdot 2^i, \tag{4}$$

where $\mathrm{not}(x)$ flips a single bit x, and the "$x \oplus y$" represents the XOR operation. It has the following performance:

If $\mathrm{eXOR}(x, r) = t$, then $\mathrm{eXOR}(t, r) = x$.

This property can be proved by Table 3.

Table 3 The results of not $(x_i \oplus r_i \oplus r_{i+3})$.

	$r_i r_{i+3}$			
x_i	00	01	10	11
0	1	0	0	1
1	0	1	1	0

3 Image Encryption and Decryption Scheme

3.1 *Secret Key and Random Number Generation*

In this scheme, gray level images with the size of $M \times N$ are applied to demonstrate the proposed scheme. The initial values x_0 and y_0 could be calculated as follows:

$$x_0^1 = \left(x_{01}^0 + \frac{N_0}{1000}\right) \bmod 1, \quad y_0^1 = (y_{01}^0 + x_0^1) \bmod 1, \tag{5}$$

$$x_0^2 = (x_{02}^0 + y_0^1) \bmod 1, \quad y_0^2 = (y_{02}^0 + x_0^2) \bmod 1, \tag{6}$$

where x_{01}^0, x_{02}^0, y_{01}^0, y_{02}^0, and N_0 represent the initial secret keys. (x_0^1, y_0^1) denotes the initial condition of row encryption, and (x_0^2, y_0^2) denotes the initial condition of column encryption. "x mod y" refers to the module operation.

3.2 *Matrix-Level Encryption*

3.2.1 *Row encryption*

The steps of row encryption are displayed as follows:

Step 1. $i = 1$. The initial values (x_0^1, y_0^1) are obtained by Eq. (5). Iterate 2D-SIMM N_0 times and the sequences are discarded in order to avoid the transient effect.

Step 2. Continue to iterate 2D-SIMM again and then obtain the new values (x, y).

Step 3. The fractional parts of the values (x, y) are converted into binary streams (S, T).

Step 4. The 22 most significant bits of S are employed to build random numbers k_1, and the 16 most significant bits of T are adopted to build random numbers k_2.

$S_{21-11} \leftarrow$ first half 11 bits,

$S_{10-0} \leftarrow$ second half 11 bits, and

$k_1 \leftarrow S_{21-11}$ XOR S_{10-0}.

$T_{15-8} \leftarrow$ first half 8 bits,

$T_{7-0} \leftarrow$ second half 8 bits, and

$k_2 \leftarrow T_{15-8}$ XOR T_{7-0}.

$$k_1 = \bmod(k_1, 2047) + 1, \tag{7}$$

$$k_2 = \bmod(k_2, N - 1) + 1, \tag{8}$$

where k_1, k_2 are the integers, and $k_1 \in [1, 2047]$, $k_2 \in [1, N-1]$.

Step 5. For i'th row pixels $P(i, \ldots)$, do $P(i, \ldots) = \text{eXOR}[P(i, \ldots), k_1]$.

Step 6. A k_2-bit right cyclic shift is performed on $P(i, \ldots)$.

Step 7. $i = i + 1$ and update (x, y) by

$$\begin{cases} x = x + s_1 - \lfloor x + s_1 \rfloor \\ y = y + s_1 - \lfloor y + s_1 \rfloor \end{cases}, \tag{9}$$

where s_1 is the mean of $P(i, \ldots)$.

Step 8. Do steps 1 to 7 again until $i > M$.

3.2.2 *Column encryption*

The steps of column encryption are shown as follows:

Step 1. $j = 1$. The initial values (x_0^2, y_0^2) are produced by Eq. (6). Iterate 2D-SIMM N_0 times and the sequences are discarded for avoiding transient effect.

Step 2. Iterate 2D-SIMM once again and get new (x, y).

Step 3. The fractional part of the values (x, y) is converted into binary streams (U, V).

Step 4. The 22 most significant bits of U are employed to build random numbers k_3, and the 16 most significant bits of V are employed to build random numbers k_4.

$U_{21-11} \leftarrow$ first half 11 bits,

$U_{10-0} \leftarrow$ second half 11 bits, and

$k_3 \leftarrow U_{21-11}$ XOR S_{10-0}.

$V_{15-8} \leftarrow$ first half 8 bits,

$V_{7-0} \leftarrow$ second half 8 bits, and

$k_4 \leftarrow U_{15-8}$ XOR S_{7-0}.

$$k_3 = \bmod(k_3, 2047) + 1, \tag{10}$$

$$k_4 = \bmod(k_4, M - 1) + 1, \tag{11}$$

where k_3, k_4 are the integers, and $k_3 \in [1, 2047]$, $k_4 \in [1, M-1]$.

Step 5. For j'th column pixels $P(\cdot, j)$, do $P(\cdot, j) = \text{eXOR}[P(\cdot, j), k_3]$.

Step 6. Connect $P(\cdot, j)$ into a circle. Shift the pixels to up k_4 steps.

Step 7. $j = j + 1$ and update (x, y) by

$$\begin{cases} x = x + s_2 - \lfloor x + s_2 \rfloor \\ y = y + s_2 - \lfloor y + s_2 \rfloor \end{cases}, \tag{12}$$

where s_2 is the mean of $P(\cdot, j)$.

Step 8. Do steps 1 to 7 in a loop until $j > N$.

New pixel matrix P is obtained finally.

3.3 *DNA-Level Encryption*

DNA encryption is depicted as follows:

Step 1. DNA encoding is performed on the new matrix P, and DNA-encoded matrix P_b is obtained with size $M \times 4N$.

Step 2. A chaotic sequence $C = (c_1, c_2, \ldots, c_{MN})$ is generated under initial condition x_0^1 and y_0^2 using Eq. (1). Here, $c_i = x_i (i = 1,2, \ldots, MN)$.

Step 3. Convert c_i $(1 \le i \le MN)$ into corresponding binary format. The former 8 bits are encoded using DNA encoding rule. The length of sequence C_1 is $4MN$.

Step 4. Rearrange the sequence C_1 to form a matrix Q with size $M \times 4N$.

Step 5. The two matrices Q and P_b are executed DNA XOR operation to generate matrix H,

(a) (b) (c) (d) (e)

Fig. 1 Plain images: (a) Lena, (b) Terrace, (c) peppers, (d) Jokul, and (e) Baboon.

$$H(1) = Q(1) \oplus P_b(1) \oplus \mathrm{mod}(N_0, 256),$$
$$H(t) = Q(t) \oplus P_b(t) \oplus H(t-1), \quad (13)$$

$t = 2,3,\ldots,4MN$.

Step 6. Iterate 2D-SIMM once again and get the new (x', y')

$$z = \mathrm{mod}(\lfloor x' \times 10^{14} \rfloor, 15!) + 1, \quad (14)$$

z is the number of the two-by-two complementary rule that has been chosen for image encryption and $z \in [1,15!]$.

Step 7. Iterate 2D-SIMM N_0 times and the sequences are discarded with the initial values x_0^2 and y_0^1.

Step 8. Iterate 2D-SIMM f_0 $[f_0 = \max(M, 2N)]$ times again. Then, two chaotic sequences $E = (x_1, x_2, \ldots, x_M)$ and $F = (y_1, y_2, \ldots, y_{2N})$ are generated.

Step 9. Transform E and F into matrices $K_1(M,1)$ and $K_2(1,2N)$. Multiply K_1 and K_2 to obtain matrix K with size $M \times 2N$

$$L(i,j) = \mathrm{mod}[\lfloor K(i,j) \times 10^{10} \rfloor, 15] + 1, \quad (15)$$

$i \in [1,M]$, $j \in [1,2N]$, and $L(i,j) \in 1,15$.

Step 10. Use the z'th two-by-two DNA complementary rule to operate on matrix H.

```
for i = 1: M
  for j = 1: 2N
    if L(i, j) is equal to w and w is integer,
    Then, change H(i, 2j − 1) and H(i, 2j) to be
      D^w[H(i, 2j − 1)H(i, 2j)]
  end
end.
```

Here, $w \in 1$, 15, and $D^w(xx)$ means its w'th complement.

Step 11. Convert DNA cipher matrix H into decimal number.

Step 12. Cipher image is obtained finally.

3.4 *Image Decryption*

The decryption algorithm is the reverse process of the encryption algorithm. It could be described briefly as follows. First, DNA decryption is applied. Then, column decryption and row decryption are performed. Finally, the plain image is obtained.

4 Simulation Results

The experiments of the proposed algorithm are simulated on the MATLAB 2010b platform. In this paper, Lena, Baboon, peppers, Terrace, and Jokul are used as original images. The size of the plain image is 256×256, as shown in Fig. 1. The initial keys are set (x_{01}^0, x_{02}^0, y_{01}^0, y_{02}^0, and N_0) = (0.3462, 0.5484, 0.7425, 0.8562, and 150).

The experimental results are demonstrated in Fig. 2. Figures 2(a)–2(c) are plain images, cipher images, and decrypted images.

The decrypted image is lossless and the same as the plain image with the proposed scheme.

Two schemes of Ref. 16 and 21 are employed for contrasts of performance evaluations. Encrypted images with different methods are shown in Fig. 3.

5 Security Analysis

An excellent encryption algorithm could resist many kinds of attacks, such as a statistical attack, brute-force attack, differential attack, and plaintext attack, and so on.

5.1 *Key Space and Sensitivity Analysis*

An excellent image encryption algorithm should be very sensitive to secret keys, and key space should be large enough to resist the brute-force attack. In the proposed scheme, the secret keys are x_{01}^0, x_{02}^0, y_{01}^0, y_{02}^0, and N_0. The number of two-by-two DNA complementary rules is a factorial of 15 (15!). If the precision of the system is 10^{-16}, then the key space of the proposed scheme is $10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 15! \approx 1.3 \times 10^{76}$. It will be large enough to withstand an exhaustive attack.

In the paper, secret keys are set (x_{01}^0, x_{02}^0, y_{01}^0, y_{02}^0, and N_0) = (0.3462, 0.5484, 0.7425, 0.8562, and 150). If a tiny alteration (10^{-6}) is brought in one of the initial values, the others remain the same. The decrypted images are depicted in Fig. 4. The difference between improper decrypted images [Figs. 4(b)–4(f)] and the plain image is almost 99.7%. So, the proposed scheme is very sensitive to the system key.

5.2 *Histogram Analysis*

An excellent encryption scheme should provide the flat histogram of the encrypted image. The histograms of a plain image and its encrypted image are shown in Fig. 5. It indicates that the numbers of every pixel value of the encrypted image are nearly even. It demonstrates that a statistical attack is invalid to the proposed algorithm. Histograms of plain and cipher images are displayed in Figs. 5(a) and 5(b).

Fig. 2 Cipher and decrypted images (Baboon, Terrace, and Lena): (a) plain image, (b) cipher image, and (c) decrypted image.

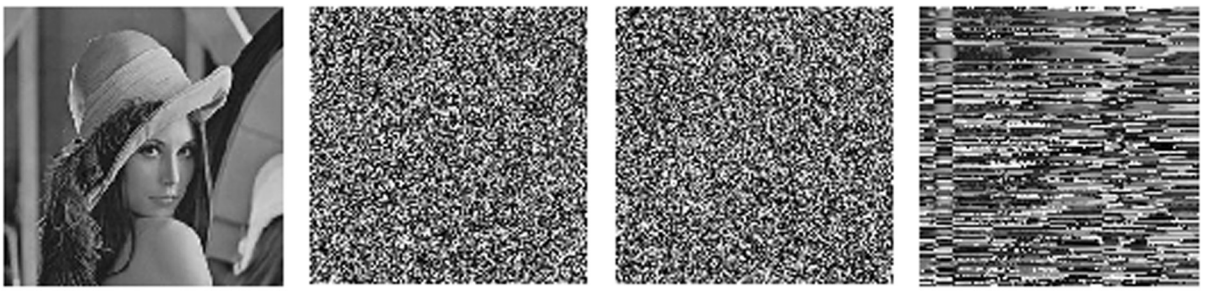

Fig. 3 Plain image and cipher image with different methods: (a) plain image, (b) Liu's scheme,[21] (c) proposed scheme, and (d) Wang's scheme.[16]

5.3 *Correlation Analysis*

The correlation coefficient r_{xy} between two adjacent pixels x and y are defined as

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)D(y)}}, \tag{16}$$

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

7225 pairs of adjacent pixels from the plain image and encrypted image are chosen in the horizontal, vertical, and diagonal directions. Figure 6 shows the correlation of two adjacent pixels in the Lena image and its cipher image. It can be shown that correlation is very high in the plain image but correlation is extremely low in the cipher image.

Table 4 shows the values of correlation coefficients of two adjacent pixels in Fig. 6. The results in the proposed scheme are compared with the results in Refs. 16, 21, 22, and 25. The results reveal that the proposed algorithm is rather good.

5.4 *Information Entropy*

Information entropy is one of the most important features of randomness. If m is the information source, then information entropy is calculated as follows:

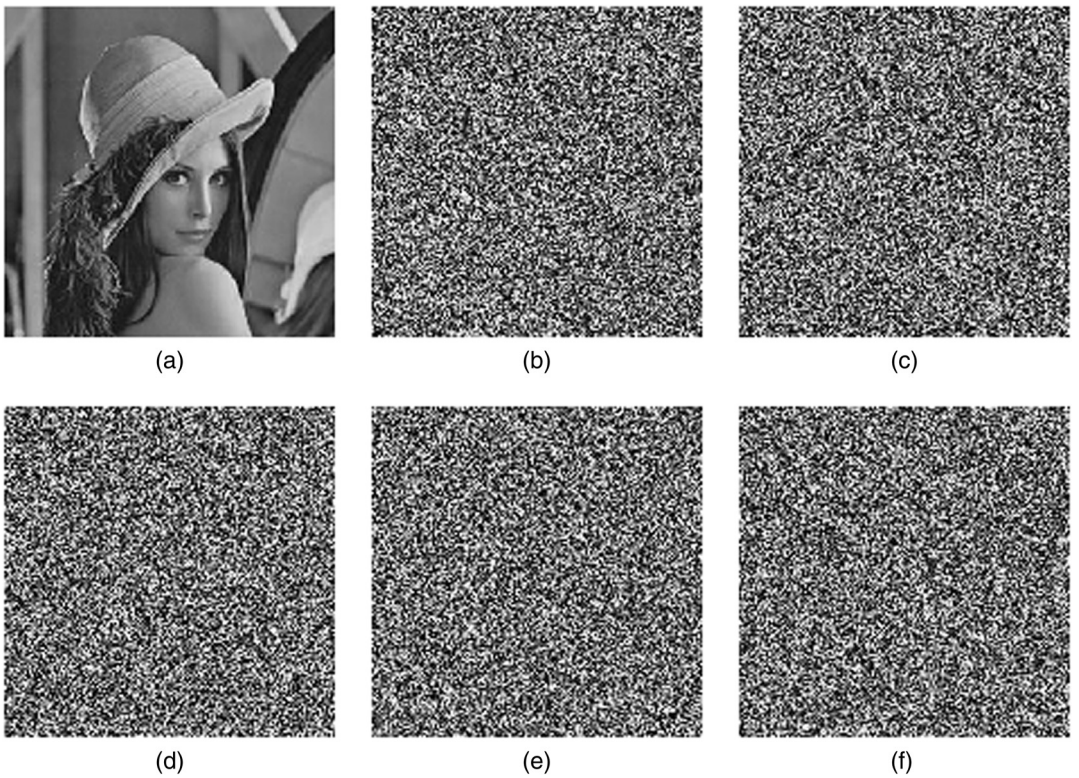

Fig. 4 Decrypted images with different secret keys: (a) decrypted image using the right key, (b) decrypted image with $x_{01}^0 + 10^{-6}$, (c) decrypted image with $x_{02}^0 + 10^{-6}$, (d) decrypted image with $y_{01}^0 + 10^{-6}$, (e) decrypted image with $y_{02}^0 + 10^{-6}$, and (f) decrypted image with $N_0 + 1$.

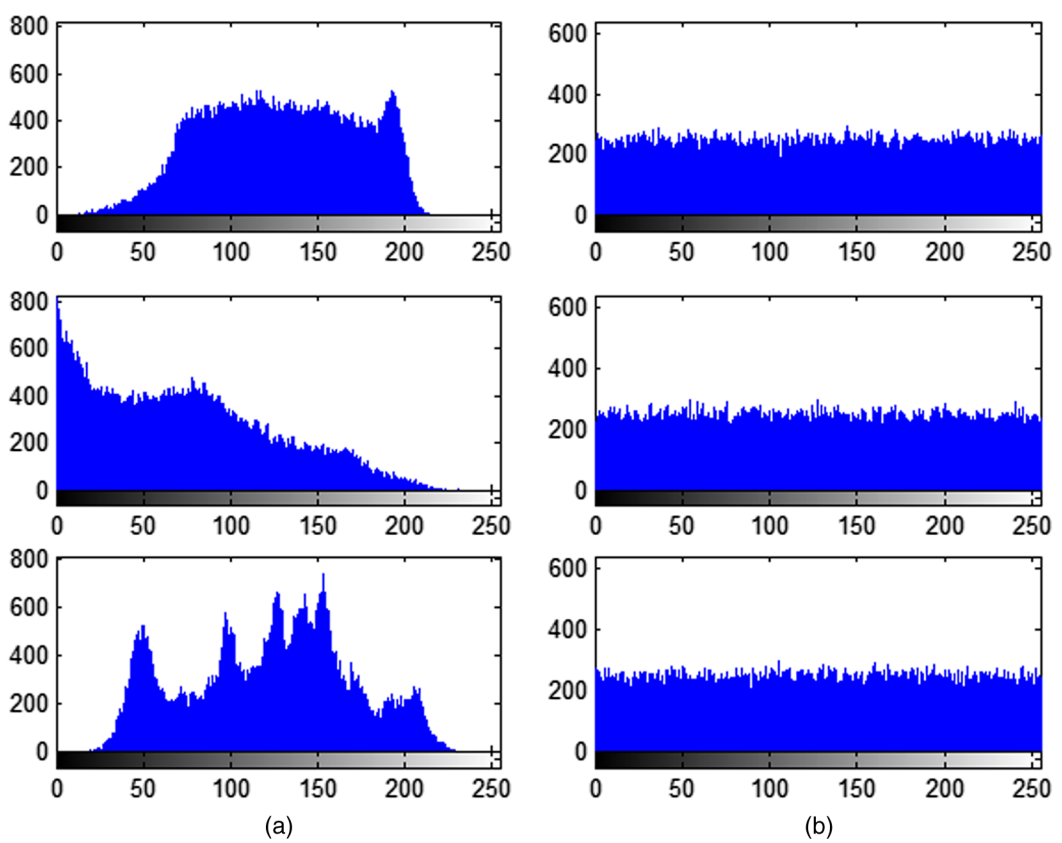

Fig. 5 Histograms of plain and cipher images (Baboon, Terrace, and Lena): (a) histogram of plain image and (b) histogram of encrypted image.

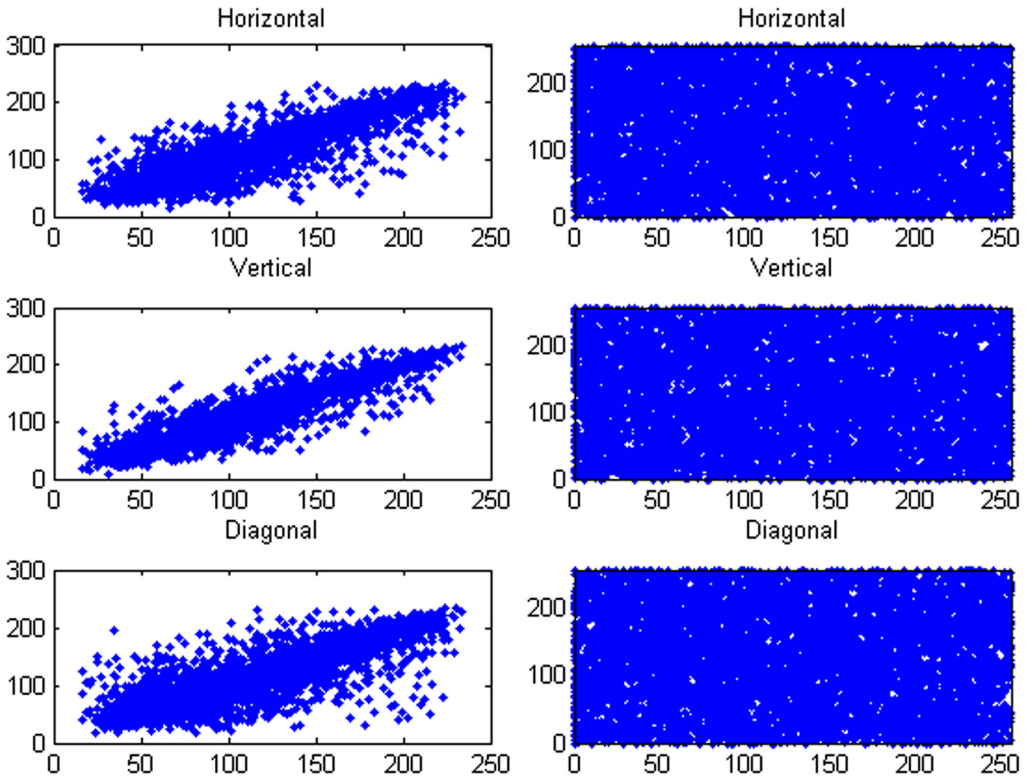

Fig. 6 Correlation analysis in three directions of plain image and cipher image: upper frame with horizontal distribution, center with vertical distribution, and lower with diagonal distribution.

Table 4 Analysis of correlation coefficients.

Algorithm	Horizontal	Vertical	Diagonal
Plain image	0.9425	0.9701	0.9248
Proposed	0.0013	0.0021	−0.0024
Ref. 16	−0.0028	0.0032	0.0052
Ref. 21	0.0033	−0.0028	−0.0039
Ref. 22	0.0048	−0.0037	0.0034
Ref. 25	−0.0062	0.0076	−0.0053

$$H(m) = -\sum_{i=1}^{L} p(m_i)\log_2 p(m_i), \tag{17}$$

where $p(m_i)$ denotes the probability of symbol m_i and L is the total number of m_i. The maximum information entropy is 8. The information entropy of cipher images is listed in Table 5.

5.5 *Differential Attack*

Number of pixels change rate (NPCR) and unified average changing intensity (UACI) are two parameters that are most widely adopted to measure the sensitivity to the plain image.[21] NPCR and UACI are used to test the system to resist differential attacks. NPCR and UACI are calculated as

Table 5 Information entropy of cipher image.

Image	Lena	Terrace	Peppers	Jokul	Baboon
$H(m)$	7.9971	7.9972	7.9973	7.9969	7.9974

$$\mathrm{NPCR} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\%, \tag{18}$$

$$\mathrm{UACI} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{19}$$

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{else} \end{cases}.$$

NPCR = 99.61% and UACI = 33.32%. The experiments demonstrate that the proposed scheme could effectively resist a plaintext attack and differential attack.

5.6 *Noise Attack*

During processing, transmission or an attack from an intruder, the encrypted image will be inevitable to confront with noise. The robust image encryption scheme should withstand a slight noise attack. Figure 7 shows the decrypted Lena with different kinds of noises and intensities.

As shown in Fig. 7, the decrypted image can be recovered even the encrypted image with noise.

Fig. 7 Results of antinoise. Decrypted image of Lena with (a) salt and pepper, 0.02; (b) salt and pepper, 0.05; (c) salt and pepper, 0.1; (d) Gaussian, 0.02; (e) Gaussian, 0.05; and (f) Gaussian, 0.1.

5.7 *Known-Plaintext and Chosen-Plaintext Attacks*

In the proposed scheme, the iteration condition of 2D-SIMM will be changed by the encrypted pixel value. Even if an invader uses all black or white images as the chosen plain image, the proposed scheme could resist attacks. That is because row encryption, column encryption, and DNA-level encryption will be different if the plain image is changed. Therefore, the proposed scheme could resist known-plaintext and chosen-plaintext attacks.

6 Conclusion

In this paper, an image encryption scheme is proposed based on two-by-two DNA complementary rules and 2D-SIMM. First, the plain image is performed confusion and permutation operations. Then, DNA-level encryption is executed. The extended XOR operation is applied to help the image encryption scheme to resist plaintext attacks. The experimental results prove that the scheme could afford a differential attack, brute-force attack, statistical attack, and plaintext attack. The security of the system is very high. The proposed method is suitable for practical application.

Disclosures

I declare that there is no conflict of interest in the manuscript.

Acknowledgments

This research was financially supported by the National Natural Science Foundation of China (Grant No. 61272469), the Natural Science Foundation of Fujian Province (Grant No. 2016J05153), and the Outstanding Youth Scientific Research Training Program of Fujian Province (2017).

References

1. E. Shannon, "Communication theory of secrecy systems," *Bell Labs. Tech. J.* **28**(4), 656–715 (1949).
2. Z. Liu and S. Liu, "Double image encryption based on iterative fractional Fourier transform," *Opt. Commun.* **275**, 324–329 (2007).
3. J. Chen et al., "An efficient image encryption scheme using lookup table–based confusion and diffusion," *Nonlinear Dyn.* **81**(3), 1151–1166 (2015).
4. J. Chen et al., "An efficient image encryption scheme using gray code based permutation approach," *Opt. Laser. Eng.* **67**, 191–204 (2015).
5. H. Liu et al., "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.* **12**(5), 1457–1466 (2012).
6. Z. Liu et al., "Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains," *Opt. Laser. Technol.* **47**(1), 152–158 (2013).
7. Y. Mao et al., "A novel fast image encryption scheme based on 3D chaotic baker maps," *Int. J. Bifurcat. Chaos* **14**(10), 3613–3624 (2011).
8. T. Sivakumar and R. Venkatesan, "A new image encryption method based on Knight's travel path and true random number," *J. Inf. Sci. Eng.* **32**(1), 133–152 (2016).
9. Q. Wang et al., "Double image encryption using phase-shifting interferometry and random mixed encoding method in fractional Fourier transform domain," *Opt. Eng.* **52**(8), 084101 (2013).
10. X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Commun. Nonlinear Sci.* **18**(11), 3075–3085 (2013).
11. H. Mousa et al., "Data hiding based on contrast mapping using DNA medium," *Int. Arab J. Inf. Technol.* **8**(2), 147–154 (2011).
12. P. Zhen et al., "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimed. Tools Appl.* **75**(11), 6303–6318 (2016).
13. A. U. Rehman et al., "Selective encryption for gray images based on chaos and DNA complementary rules," *Multimed. Tools Appl.* **74**(13), 4655–4677 (2015).
14. J. Zhang et al., "Image encryption algorithm based on DNA encoding and chaotic maps," *Math. Probl. Eng.* **2014**, 1–10 (2014).
15. S. Sun, "A novel secure image steganography using improved logistic map and DNA techniques," *J. Internet Technol.* **18**(3), 647–652 (2017).
16. X. Wang et al., "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Laser. Eng.* **73**, 53–61 (2015).
17. X. Wang et al., "A novel image encryption scheme based on 2-D logistic map and DNA sequence operations," *Nonlinear Dyn.* **82**(3), 1269–1280 (2015).
18. A. Belazi et al., "Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map," *Nonlinear Dyn.* **76**(4), 1989–2004 (2014).

19. X. Chai et al., "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Laser. Eng.* **88**, 197–213 (2017).
20. S. K. Abd-El-Hafiz et al., "Novel permutation measures for image encryption algorithms," *Opt. Laser. Eng.* **85**, 72–83 (2016).
21. W. Liu et al., "A fast image encryption algorithm based on chaotic map," *Opt. Laser. Eng.* **84**, 26–36 (2016).
22. Z. Hua et al., "2D sine logistic modulation map for image encryption," *Inform. Sci.* **297**(C), 80–94 (2016).
23. A. Khalifa and A. Atito, "High-capacity DNA-based steganography," in *Informatics and Systems*, pp. 76–80, IEEE, Cairo, Egypt (2012).
24. X. Wang and H. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.* **342**, 51–60 (2015).
25. X. Wang et al., "A fast image algorithm based on rows and columns switch," *Nonlinear Dyn.* **79**(2), 1141–1149 (2015).

Shuliang Sun received his BS degree from Hangzhou Dianzi University in 2003, his MS degree from Guangxi University in 2006, and his PhD from Tongji University in 2011. He is a teacher at the School of Electronics and Information Engineering, Fuqing Branch of Fujian Normal University, China. His research interests include optical pattern recognition, optical image processing, and optical communication.