CNN-based Color Image Encryption Algorithm using DNA Sequence Operations

Jingshuai Wang [1,2] , Fei Long [1], Weihua Ou[3]*
1 School of Electrical Engineering, Guizhou Institute of Technology, Guiyang, China
2 College of Big Data and Information Engineering, Guizhou University, Guiyang, China
3 School of Big Data and Computer Science, Guizhou Normal University, Guiyang, China
Email: feilong@git.edu.cn, ouweihuahust@gmail.com

***Abstract*—The encryption algorithm of color images based on chaos theory has attracted lots of attentions in recent years. Nevertheless, due to the defects of the low dimensional chaotic system in single structure and small key space size, the security of cryptosystem is not sufficient enough. In this paper, we proposed a novel encryption algorithm for color images based on Deoxyribonucleic acid (DNA) sequence operations and cellular neural network (CNN) to dispose of these defects. The proposed cryptosystem of this paper takes on the features of large key space and complex structure. Firstly, the plain color image is split into three matrices (R, G, B) which are transformed into DNA matrices by the DNA encoding rules, respectively. Secondly, the elements' positions of the three DNA sequence matrices are scrambled via the chaotic sequences generated by CNN. Thirdly, the three DNA matrices are summed according to the certain rules and complemented by the complementary rules, and then the cipher-image is obtained by the DNA decoding rules via the DNA matrices. Simulation results and security analysis show that the encryption effect of this paper is not only better than traditional encryption algorithms but also has excellent ability to hold back familiar attacks.**

Keywords—Color image encryption; cellular neural network; DNA operation; security analysis;

I. INTRODUCTION

With the rapid development of communications and computer networks, more and more digital multimedia content, such as image, sound and video, are being carried out via the medium of internet. However, digital multimedia information exists a great deal of hidden dangers in the storage, and the information may be stolen, tampered, these issues are recognized as the key to the development of public information systems. So we should pay attention to the protection of the transmission process. As one of the most effective means to ensure the security of information, image encryption technology has widely used in the digital multimedia information transmission process of internet [1, 2]. Some traditional encryption techniques do not have enough security for the inherent properties of images in the large amount of data and high correlation between pixels [3, 4]. In recent years, image encryption algorithms based on chaotic system have great potentials because of the excellent features of the chaos system: the sensitivity to the initial conditions and control parameters, aperiodicity, pseudo-random [5-10]. Because of the DNA computing excellent properties, such as high storage density, high massive and ultra-low energy consumption, the DNA-based image encryption has attracted more researchers' attention [11-15].

Due to the irregularity and pseudo-randomness of chaos, the chaotic sequences produced by chaotic systems are unpredictable and complicated. Some scholars used the chaotic sequences obtained by the low dimensional chaotic system to encrypt the image in early stage. A new 1D chaotic system for image encryption is proposed by Zhou [16]. Zhong [17] proposed an image encryption algorithm based on 2D Logistic-Sine chaotic map. However, these sequences generated by low dimensional chaotic systems cannot withstand brute force attacks because of their own weakness of the small key space and low security. Hyper-chaotic systems possess larger key space and more complicated dynamic characteristics, so hyper-chaotic system make up the defects of low dimensional chaotic system and more suitable for image encryption. Zamani [18] introduced a novel image encryption scheme based on hyper chaotic systems and fuzzy cellular automata. A new image encryption algorithm based on hyper chaotic system is pointed out which has higher security [19]. Huang [20] researched on the application of image encryption technology based on 7 dimensional CNN hyper chaos and the results showed that the hyper chaos are better than low dimensional chaotic systems.

With the development of DNA computing, DNA cryptography has became a new field of cryptography, and DNA is used as the carrier of information in the field of image encryption. However, these biological experiments can only be achieved in a fully equipped laboratory, and require a high cost. Recently, the high storage density, high parallelism, and ultra-low power consumption of DNA calculations are used in image encryption experiments [21-24]. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic map is introduced[25]. Liu et al. presented image encryption using DNA complementary rule and chaotic maps [26]. Xiuli Chai pointed out a novel chaos-based image encryption algorithm using DNA sequence operations [27]. In order to improve the security of cryptography, a class of color image encryption was proposed based on hybrid hyper-chaotic system and cellular automata [28]. Liu [29] argued that it has some disadvantages with the change of plaintext, security keys and low sensitivity so that

978-1-5386-3016-7/17/$31.00 ©2017 IEEE

the attack on the choice of plaintext is low. Although, many articles have adopted the image encryption method based on DNA operation, and obtained the ideal effect of encryption, the inherent characteristics of the DNA operating have yet to play to the extreme, remains to be further excavated by researchers.

According to the analysis above, this paper proposes a color image encryption algorithm based on DNA sequence operation and cellular neural network. It not only overcomes the shortcomings of low dimensional chaotic system's small key space and low security, but also makes full use of the high storage density, high parallelism and ultra-low energy consumption of DNA computing.

The paper is organized as follows: Section 2 introduces Cellular neural network and presents a four-order cellular neural network and DNA computing. The proposed image encryption and decryption algorithm are presented in Section 3. Section 4 is simulation and security analysis. Finally, we give the conclusions in Section 5.

II. Preparation Knowledge

A. *Cellular Neural Network*

Cellular neural network is first proposed by Chua and Yang in 1988, the basic unit of CNN called cells, each cell is a nonlinear first order circuit which is composed of a linear resistor, a linear capacitor and a voltage controlled current source.

For convenience, we introduce a simplified generalization of CNN cell model in this paper. A four-order CNN dynamic model is described as follows:

$$\begin{cases} \dfrac{dx_j}{dt} = -x_j + a_j y_j + \displaystyle\sum_{k=1,k\neq j}^{4} a_{jk} y_k + \sum_{k=1}^{4} s_{jk} x_k + i_j \\ y_j = 0.5\left(\left|x_j + 1\right| - \left|x_j - 1\right|\right), \quad j = 1,2,3,4 \end{cases} \tag{1}$$

Where x_j and y_j denote the state variables and the cell outputs of the CNN, respectively. a_k, a_{jk}, s_{jk}, a_j are the system parameters. i_j is threshold.

The state equation of cellular neural network model can be described as follows:

$$\begin{cases} \dfrac{dx_1}{dt} = -x_3 - x_4 \\ \dfrac{dx_2}{dt} = 2x_2 + x_3 \\ \dfrac{dx_3}{dt} = 14x_1 - 14x_2 \\ \dfrac{dx_4}{dt} = 200y_4 + 100x_1 - 100x_4 \end{cases} \tag{2}$$

According to the literature [30], we can get different chaotic attractors by setting different initial values and control parameters. Cellular neural networks have real-time, more controllable coefficients, and can produce more complex hyper chaotic behavior, and have a strong sensitivity to initial values and control parameters [31]. The initial value and control parameters of the CNN dynamic model are set as: x_1=0, x_2=0, x_3=0 and x_4=10^{-10}. In order to facilitate the experiment, we will employ the following formula:

$$\begin{cases} x_1(i) = ceil\left(abs\left(\left(x_1(i) \times 10^{10}\right)\right)\right) \bmod 256 \\ x_2(i) = ceil\left(abs\left(\left(x_2(i) \times 10^{10}\right)\right)\right) \bmod 256 \\ x_3(i) = ceil\left(abs\left(\left(x_3(i) \times 10^{10}\right)\right)\right) \bmod 256 \\ x_4(i) = ceil\left(abs\left(\left(x_4(i) \times 10^{10}\right)\right)\right) \bmod 256 \end{cases} \tag{3}$$

B. *DNA sequence operations*

1) DNA encoding and decoding rules

DNA is a kind of elongated macromolecular compound, which is made up of a series of DNA chains. It contains four nucleic acid bases, namely, adenine (A), cytosine (C), guanine (G) and thymine (T). Double-stranded DNA satisfies the principle of Watson-Crick complementary base pairing: A pairs with T, C pairs with G. In the binary, 0 and 1 are complementary, so we extend it, the 00 and the 11 are complementary, and the 01 and 10 are also complementary. When we employ the base A, T, C and G to encode the 00, 01, 10, and 11, according to the mathematical operations, there are 24 kinds of coding rules. But there are only 8 kinds of encoding rules that satisfy the Watson-Crick complement rule, which is shown in Table Ⅰ.

TABLE I. DNA ENCODING RULES

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

2) Hamming distance

In DNA computing, Hamming distance is used to indicate the number of different elements of the corresponding position of two equal length DNA sequences. For the DNA sequences x={x_1, x_2, ⋯x_n} and y={y_1, y_2, ⋯y_n}, defined the Hamming distance $H(x,y)$ and the extended Hamming distance $\hat{H}(x,y)$ as follows, respectively.

$$H(x,y) = \sum_{i=1}^{n} h(x_i, y_i) \tag{4}$$

$$\hat{H}(x,y) = \sum_{i=1}^{n} \hat{h}(x_i, y_i) \tag{5}$$

where

$$h(x_i, y_i) = \begin{cases} 0, x_i = y_i \\ 1, x_i \neq y_i \end{cases} \tag{6}$$

$$\hat{h}(x_i, y_i) = \begin{cases} 0, & x_i = y_i \\ DNAtodec(x_i - y_i), & x_i \neq y_i \end{cases} \tag{7}$$

978-1-5386-3016-7/17/$31.00 ©2017 IEEE

3) DNA complementary rules

The DNA complementary rules must satisfy that, for each base x in the DNA sequence:

$$\begin{cases} x \neq B(x) \neq B(B(x)) \neq B(B(B(x))) \\ x = B(B(B(B(x)))) \end{cases} \tag{8}$$

Abide by the rules of (6), the DNA complementary pairs can be defined, and there are total 6 group legal DNA complementary rules, which are shown as follows:

Rule 1: (AT) (TC) (CG) (GA), Rule 2: (AT) (TG) (GC) (CA)

Rule 3: (AC) (CT) (TG) (GA), Rule 4: (AC) (CG) (GT) (TA)

Rule 5: (AG) (GT) (TC) (CA), Rule 6: (AG) (GC) (CT) (TA)

4) DNA addition and subtraction rules

It is particularly notorious that addition and subtraction operations are regularly utilized in the binary operation. So addition and subtraction operations of DNA sequences are complemented under the rules of the binary operation. There are eight kinds of addition and subtraction operation because we have eight kinds of DNA coding rules.

TABLE II. DNA ADDITION RULES

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

TABLE III. DNA SUBTRACTION RULE

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

III. IMAGE ENCRYPTION AND DECRYPTION ALGORITHM

A. Encryption algorithm

The encryption procedure is composed of two parts: pixel substitution and pixel permutation, which are interleaved in order to transform the plain-image into cipher-image. In this section, the process of CNN-based color image encryption algorithm using DNA sequence operation is shown in Fig.1.

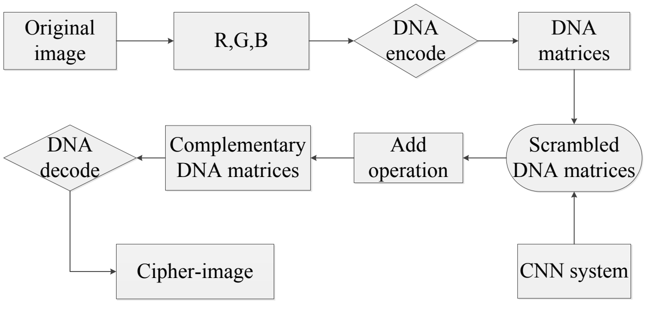

Fig. 1. Steps of encryption algorithm

The encryption steps are as follows:

Step 1: Input color plain image *A*(*m*, *n*, *3*) where *m* and *n* donate the rows and columns of the image size, respectively. And the color image A is divided into three components *R*(*m*, *n*), *G*(*m*, *n*), *B*(*m*, *n*), where *R*(*m*, *n*), *G*(*m*, *n*) and *B*(*m*, *n*) are the pixel values at (*m*, *n*) of three components between 0 and 255, respectively.

Step 2: Transform the decomposed matrixes of *R*(*m*, *n*), *G*(*m*, *n*) and *B*(*m*, *n*) to binary matrixes *R*(*m*, *n*×8), *G*(*m*, *n*×8) and *B*(*m*, *n*×8), then encoded respectively with the DNA encoding rule 1 and get three DNA sequence matrixes *R*(*m*, *n*×4), *G*(*m*, *n*×4) and *B*(*m*, *n*×4).

Step 3: Generate four group chaotic sequence x_1, x_2, x_3, x_4 by using CNN dynamic model in the condition of initial value and the system control parameter are $x_1=0$, $x_2=0$, $x_3=0$ and $x_4=10^{-10}$.

Step 4: The three coding matrices *R*(*m*, *n*×4), *G*(*m*, *n*×4) and *B*(*m*, *n*×4) are subjected to pixel scrambling operations using the four chaotic sequences obtained in the third step according to the following formula:

$$\begin{cases} R(i,j) = R(lx1(i), lx2(j)) \\ G(i,j) = G(lx1(i), lx3(j)) \\ B(i,j) = B(lx3(i), lx4(j)) \end{cases} \tag{9}$$

Where *R*(*i*, *j*), *G*(*i*, *j*), *B*(*i*, *j*) represent the pixel value of the *R*, *G*, *B* components at position (*i*, *j*), respectively.

Step 5: Add operator is used for encryption. Select the rule of addition according to Table Ⅱ and carry out addition operation for DNA sequence matrixes *R*(*m*, *n*×4), *G*(*m*, *n*×4) and *B*(*m*, *n*×4). The rules are following formula:

$$R'(i,j) = R(i,j) + G(i,j) \tag{10}$$

$$G'(i,j) = R(i,j) + G(i,j) + G(i,j) \tag{11}$$

$$B'(i,j) = R(i,j) + G(i,j) + B(i,j) \tag{12}$$

Step 6: Perform the DNA complementary rule on the DNA matrices R'(*m*, *n*×4), G'(*m*, *n*×4) and B'(*m*, *n*×4), respectively, and corresponding complementary DNA matrices are obtained.

Step 7: The DNA sequence matrix R'(*m*, *n*×4), G'(*m*, *n*×4) and B'(*m*, *n*×4) are decoded in accordance with the DNA decoding rules , and finally the re-combination A'(*m*, *n*, *3*) of three channels is obtained which is the final encryption image.

The encryption process is finished.

B. Decryption algorithm

The decryption algorithm is the reverse process of encryption algorithm.

Step 1: Input color cipher-image A'(*m*, *n*, *3*), where m and n donate the rows and columns of the image size, respectively. And convert the cipher-image A'(*m*, *n*, *3*) into three matrixes *R*(*m*, *n*), *G*(*m*, *n*) and *B*(*m*, *n*).

Step 2: Transform the resolved matrixes of *R*(*m*, *n*), *G*(*m*, *n*) and *B*(*m*, *n*) to binary matrixes *R*(*m*, *n*×8), *G*(*m*, *n*×8) and *B*(*m*,

$n\times8$), then carry out the DNA encoding rule to encode the binary matrixes according to Table Ⅰ and three DN sequence matrixes $R(m, n\times4)$, $G(m, n\times4)$, $B(m, n\times4)$ are get.

Step 3: The three matrices $R'(m, n\times4)$, $G'(m, n\times4)$, $B'(m, n\times$ can be obtained by performing an inverse fetch on tl encoding matrixes $R(m, n\times4)$, $G(m, n\times4)$, $B(m, n\times4)$, which ar using the DNA complement rule.

Step 4: Carry out subtraction operation for the three DNA sequence matrices by using the following formula:

$$G(i,j)=G'(i,j)-R'(i,j) \tag{13}$$

$$B(i,j)=B'(i,j)-R'(i,j) \tag{14}$$

$$R(i,j)=R'(i,j)-G(i,j) \tag{15}$$

Step 5: Generate four group chaotic sequences x_1, x_2, x_3, x_4 by using CNN dynamic model in the condition of initial value and the system control parameter are $x_1=0$, $x_2=0$, $x_3=0$ and $x_4=10^{-10}$. The three DNA sequence matrices $R(m, n\times4)$, $G(m, n\times4)$ and $B(m, n\times4)$ are subjected to pixel scrambling operations applying the four chaotic sequence get from CNN according to the follow method:

$$\begin{cases} R(i,j)=R\left(lx1(i),lx2(j)\right) \\ G(i,j)=G\left(lx1(i),lx3(j)\right) \\ B(i,j)=B\left(lx3(i),lx4(j)\right) \end{cases} \tag{16}$$

where $R(i, j)$, $G(i, j)$, $B(i, j)$ represent the pixel value of the R,G,B components at position (i, j), respectively.

Step 6: Convert $R(m, n\times4)$, $G(m, n\times4)$ and $B(m, n\times4)$ into the binary matrices by the DNA decoding rules, respectively. And recombine three channels together, which are separately components of the final decryption image $A(m, n, 3)$.

The decryption process finishes.

I. SIMULATION RESULT AND ANALYSIS

In this section, in order to judge the security of proposed encryption algorithm, several testing experiments about the size of key space, sensitivity of the keys, statistical character and information entropy are executed on color images. The experimental simulations are based on the MATLAB R2014b platform in this paper. 512×512×3 color image "Lena" is used as plaintext images in simulations.

A. Key space analysis

A high-quality encryption system requires not only a large amount of key space size to make any brute force attack ineffective, but also sensitive to all keys. In this algorithm, the initial conditions and control parameters of CNN(x_1, x_2, x_3, x_4) can be used as the secret keys. If the calculation precision is 10^{14}, the key space size of the proposed cryptosystem is $10^{14}\times10^{14}\times10^{14}\times10^{14}=10^{56}$. Besides, the index of the DNA subtraction rules, the index of the DNA encoding rules, the index of the DNA decoding rules and the index of the DNA additions rules can be the private keys. Therefore, the key space size is large enough to resist brute-force attacks.

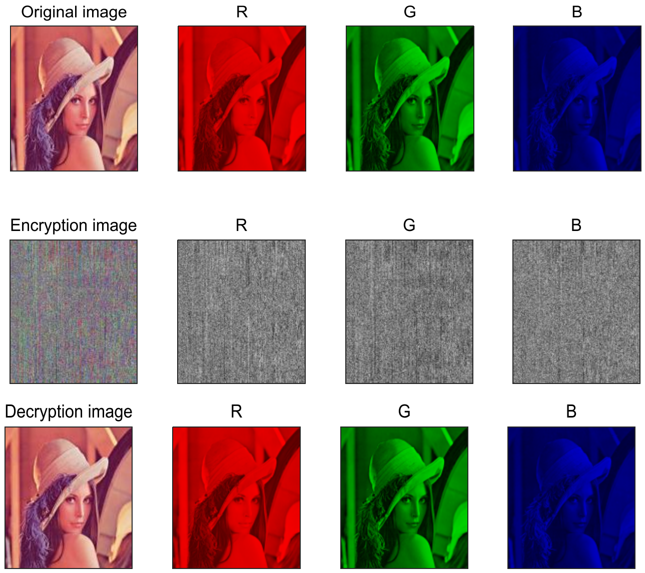

Fig. 2. Original Lena image; Encrypted Lena image; Decrypted Lena image

B. Sensitivity analysis of the keys

Minor changes in plain-image can lead to significant changes in the cipher-images, which is a good feature of the encryption system. The sensitivity test of the keys is used in this paper to verify whether the encryption system can resist differential attack. The number of pixels change rate(NPCR) and the unified average changing intensity(UACI) donate that the number of pixels change rate while one pixel of the plain-image changes and the average intensity of differences between the two images, respectively. NPCR and UACI can be calculated as:

$$NPCR=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times100\% \tag{17}$$

$$UACI=\frac{1}{M\times N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\right]\times100\% \tag{18}$$

where M and N are height and width of the encrypted images C_1 or C_2. $C_1(i, j)$ and $C_2(i, j)$ are gray values at position (i, j) of the images C_1 and C_2, respectively. The binary sequences of the two images of the same size are defined as:

$$D(i,j)=\begin{cases} 0, C_1(i,j)=C_2(i,j) \\ 1, C_1(i,j)\neq C_2(i,j) \end{cases} \tag{19}$$

CNN not only has a lot of controllable parameters, but also has sensitivity to initial values and control variables. In this paper, the sensitivity of the system to the key by slightly changing in the initial conditions and control parameters are demonstrated by experiment.

TABLE IV. COMPARISON OF THE AVERAGE NPCR AND UACI ON THE LENA IMAGE AND PEPPERS IMAGE

Image	NPCR(%)	UACI(%)
Lena	99.45	33.28
	99.57	33.42
	99.53	33.38
Peppers	99.44	33.18
	99.56	33.34
	99.54	33.28

C. *Statistical analysis*

1) Histograms analysis

In order to measure the performance of this encryption algorithm to resist the statistical attack, the distribution of pixel values of original Lena image and encrypted Lena image are shown Fig. 3. By comparing the histogram of the original image and the encrypted image, we find that the histogram distribution of the encrypted graph is uniform, which means that the encrypted image can effectively hide the information about original gray values distribution.

2) Adjacent pixel correlation analysis

As we know that the strong correlation exist between pixels and their adjacent pixels of the digital image, thus, it should be reduced to prevent statistical analysis. In this paper, we randomly select 2000 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original Lena image and encrypted Lena image, respectively. Fig.3 shows the correlation between the original Lena image and the encrypted Lena image in horizontal, vertical and diagonal directions. The results display that the correlation distribution of adjacent pixels of the original image is closely related, while the correlation of adjacent pixels in encrypted image is low than existing ones. The calculation equations are as follows:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{20}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2 \tag{21}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)\left(y_i-E(y)\right) \tag{22}$$

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)\times D(y)}} \tag{23}$$

where x and y are gray values of two adjacent pixels in the image, $cov(x, y)$ is covariance, $D(x)$ and $E(x)$ are variance and mathematical expectation of the variable x, respectively. Fig.3. shows the correlation between the original Lena image and the encrypted Lena image in horizontal, vertical and diagonal directions.

TABLE V. THE CORRELATION COEFFICIENT OF THE ADJACENT PIXELS

Algorithm	Horizontal	Vertical	Diagonal
Original image	0.9737	0.9497	0.9631
Encrypted image	-0.0219	0.0326	-0.0098
Original image[10]	0.9856	0.9682	0.9669
Encrypted image[10]	-0.0318	0.0965	0.0362

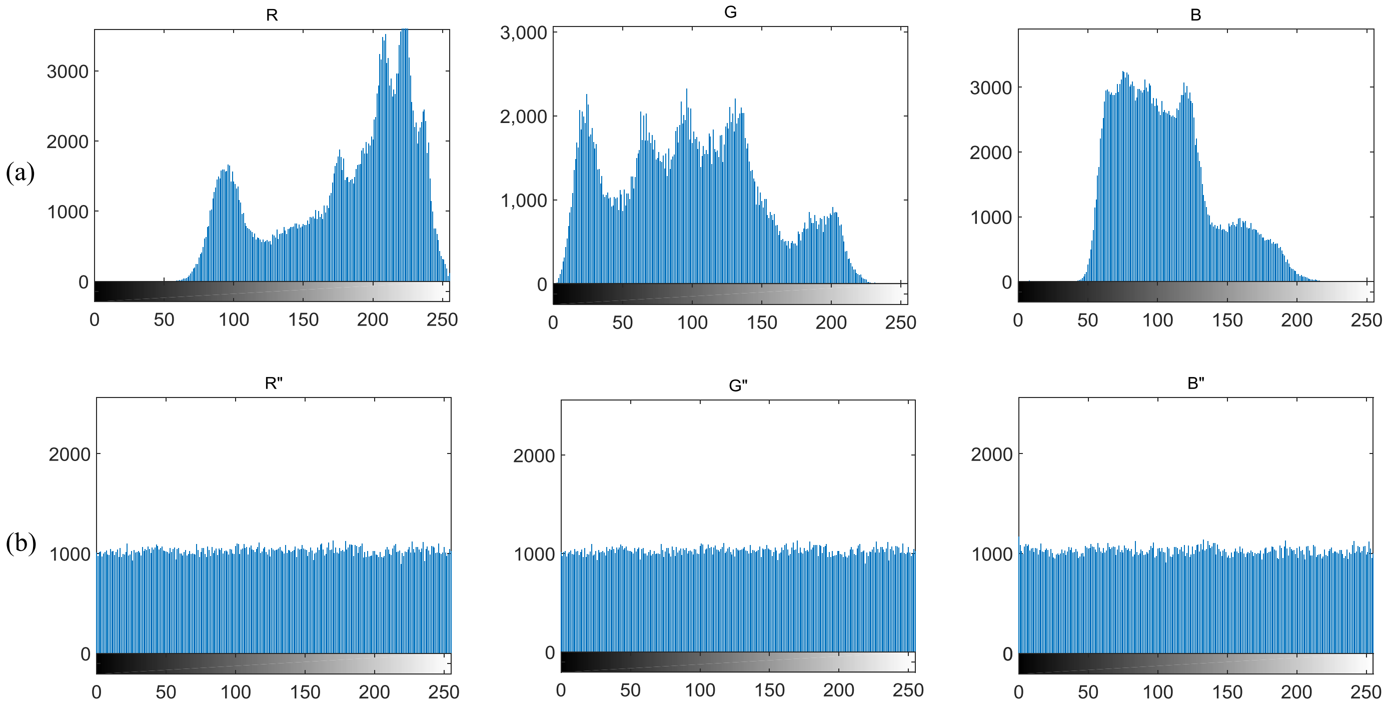

Fig. 3. (a) Histogram of original Lena image; (b) Histogram of encrypted Lena image;

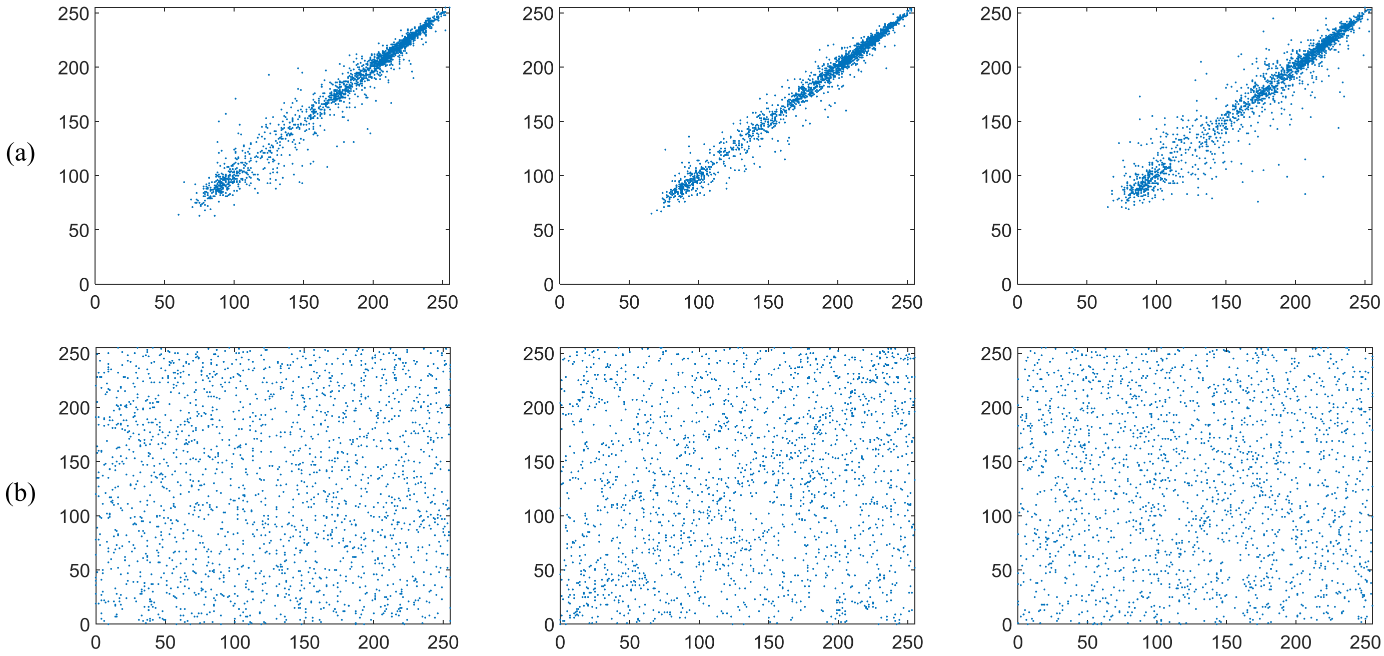

Fig. 4. Adjacent pixel correlations of original Lena image and encrypted Lena image.

(a) is the correlation of original image in R, G, B, respectively; (b) is the correlation of encrypted image in R, G, B, respectively.

D. *Information entropy analysis*

Information entropy is used to measure the randomness of random variables. According to the Shannon theorem, the amount of information for the image is:

$$\begin{cases} H(m) = -\sum_{i=0}^{L-1} P(m_i)\log_2^{P(m_i)} \\ \sum_{i=0}^{L-1} P(m_i) = 1 \end{cases} \tag{24}$$

H is the information entropy of image. Where m_i and $P(m_i)$ represent the gray value and the probability of symbol m_i, respectively.

TABLE VI. THE INFORMATION ENTROPY OF ENCRYPTED IMAGE

Encrypted image	R layer	G layer	B layer
Lena entropies	7.9914	7.9914	7.9902
Flower entropies[20]	7.9897	7.9877	7.9896
Peppers entropies	7.9910	7.9910	7.9911
Flower entropies[20]	7.9894	7.9884	7.9866

When the probability of the gray value of the image is equal, the information entropy of the image is the largest. In other words, the gray values of the image have the most uniform distribution. The results of the Table Ⅴ show the entropies of three channel encryption images are quite close to 8, which means that there exists the lesser probability for this cryptosystem to betray any information of the image. Besides, it is proved that our algorithm is secure against entropy attack since the information entropies of the proposed method are higher than other methods.

II. CONCLUSIONS

In this paper, a color image encryption algorithm using DNA sequence operation and cellular neural networks is proposed. DNA sequences are used to replace the pixel values of the original image and then the elements' position of DNA matrices are scrambled according to the chaotic sequences generated by cellular neural networks. Addition operations and fetch operations are employed to enhance the security of encryption. The experimental results show that the proposed method has strong security against statistical attacks and resist brute-force attacks. All these characteristics prove that the scheme is suitable for color image encryption.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their constructive and insightful comments for further improving the quality of this work. The research work was partially supported by the National Natural Science Foundation of China under Grant (61263005, 61563009), New Century Talents Project of the Ministry of Education under Grant No. NCET-12-0657. And this work was also supported by the National Natural Science Foundation of China (No.61762021,61402122), the Science and Technology Planning Project of Guizhou Province (No.[2017]1130), the 2014 PhD. Recruitment Program of Guizhou Normal University, the Foundation of Guizhou Educational Department (KY[2016]027.

REFERENCES

[1] Y. Zhou, W. Cao and C L P. Chen, “Image encryption using binary bitplane”. Signal Processing, vol. 100, no.7, pp. 197-207, 2014.

[2] W. Zhang, K W. Wong and H. Yu, “A symmetric color image encryption algorithm using the intrinsic features of bit distributions,” Communications in Nonlinear Science & Numerical Simulation, vol. 18, no. 3, pp. 584–600, 2013.

[3] G. Ye. “A block image encryption algorithm based on wave transmission and chaotic systems,” Nonlinear Dynamics, vol. 75, no. 3, pp. 417-427, 2014.

[4] W. Zhang, K W. Wong and H. Yu. “A symmetric color image encryption algorithm using the intrinsic features of bit distributions,” Communications in Nonlinear Science & Numerical Simulation, vol. 18, no. 3, pp. 584–600, 2013.

[5] X Y. Wang, S X. Gu and Y Q. Zhang. “Novel image encryption algorithm based on cycle shift and chaotic system,” Optics & Lasers in Engineering, vol. 68, pp. 126-134, 2015.

[6] W. Zhang, H. Yu and Y L. Zhao. “Image encryption based on three-dimensional bit matrix permutation,” Signal Processing, vol. 118, pp. 36-50, 2016.

[7] J S A E. Fouda, J Y. Effa and S L. Sabat. “A fast chaotic block cipher for image encryption,” Communications in Nonlinear Science & Numerical Simulation, vol. 19. no. 3, pp. 578-588, 2014.

[8] X. Zhang, X. Fan and J. Wang. “A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution,” Multimedia Tools and Applications, vol. 75, no. 4, pp. 1745-1763, 2016.

[9] A A A. El-Latif, L. Li and T. Zhang. “Digital Image Encryption Scheme Based on Multiple Chaotic Systems,” Sensing and Imaging, vol. 13, no. 2, pp. 67-88, 2012.

[10] Dan Zhang, Xinge You, Patrick Shen-Pei Wang, Svetlana N. Yanushkevich, Yuan Yan Tang: Facial Biometrics Using Nontensor Product Wavelet and 2D Discriminant Techniques. IJPRAI vol. 23, no. 3, pp. 521-543 , 2009

[11] X Y. Wang, Y Q. Zhang and X M. Bao. “A novel chaotic image encryption scheme using DNA sequence operations,” Optics & Lasers in Engineering, vol. 73, pp. 53-61, 2015.

[12] R. Enayatifar, H J. Sadaei and A H. Abdullah, “A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata,” Optics & Lasers in Engineering, vol. 71, pp. 33-41, 2015.

[13] R. Guesmi, M A B. Farah and A. Kachouri. “A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2,” Nonlinear Dynamics, vol. 83, no. 3, pp. 1-14, 2016.

[14] Zhibin Pan, Xinge You, Hong Chen, Dacheng Tao, Baochuan Pang: Generalization performance of magnitude-preserving semi-supervised ranking with graph-based regularization. Inf. Sci. vol. 221, pp. 284-296, 2013.

[15] Jing Huang, Xinge You, Yuan Yan Tang, “Rotation invariant iris feature extraction using Gaussian Markov random fields with non-separable wavelet", Neurocomputing, vol. 73 , no. 4-6, pp. 883-894, 2010.

[16] Y, Zhou, L. Bao and C L P. Chen. “A new 1D chaotic system for image encryption,” Signal Processing, vol. 97, no. 7, pp. 172-182, 2014.

[17] Z. Hua, Y. Zhou, C M. Pun. “Image encryption using 2D Logistic-Sine chaotic map,” pp. 3229-3234, 2014.

[18] S, Zamani, M, Javanmard and N. Jafarzadeh. “A novel image encryption scheme based on hyper chaotic systems and fuzzy cellular automata,” IEEE Electrical Engineering. pp. 1136-1141. 2015.

[19] B. Norouzi, S, Mirzakuchaki. “A fast color image encryption algorithm based on hyper-chaotic systems,” Nonlinear Dynamics, vol. 78, no. 2, pp. 995-1015, 2014.

[20] Q. Huang, G. Li. “Research on the Application of Image Encryption Technology Based on 7 Dimensional CNN Hyper Chaos,” IEEE Computer Society. International Conference on Smart City and Systems Engineering. pp. 531-534, 2016.

[21] S. Zhou, Q. Zhang and X. Wei. “An image encryption algorithm based on DNA self-assembly technology,” IEEE Xplore. IEEE International Conference on Intelligent Computing and Intelligent Systems. pp. 315-319, 2010.

[22] L. Liu, Q. Zhang and X. Wei. “A RGB image encryption algorithm based on DNA encoding and chaos map,” Computers & Electrical Engineering, vol. 38, no. 5, pp. 1240-1248, 2012.

[23] H, Liu, 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.

[24] Q. Zhang, L. Guo and X. Wei. “Image encryption using DNA addition combining with chaotic maps,” Mathematical & Computer Modelling An International Journal, vol. 52(11-12), pp. 2028-2035, 2010.

[25] X. Wu, H. Kan and J. Kurths. “A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps,” Applied Soft Computing, vol. 37(C), pp. 24-39, 2015.

[26] H. Liu, X. Wang and A. Kadir. “Image encryption using DNA complementary rule and chaotic maps,” Applied Soft Computing, vol. 12, no. 5, pp. 1457-1466, 2012.

[27] X. Chai, Y. Chen and L. Broyde. “A novel chaos-based image encryption algorithm using DNA sequence operations,” Optics & Lasers in Engineering, vol. 88, pp. 197-213, 2017.

[28] A Y. Niyat, M H. Moattar and M N. Torshiz. “Color image encryption based on hybrid hyper-chaotic system and cellular automata,” Optics & Lasers in Engineering, vol. 90, pp. 225-237, 2017.

[29] Y. Liu, J. Tang and T. Xie. “Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map,” Optics & Laser Technology, vol. 60, no. 2, pp. 111-115, 2014.

[30] J. Peng, D. Zhang and X. Liao. “A Digital Image Encryption Algorithm Based on Hyper-chaotic Cellular Neural Network,” IOS Press, 2009.

[31] Z. He. “The Dynamic Character of Cellular Neural Network with Applications to Secure Communication,” China: Journal of China Institute of Communications, vol. 20, no. 3, pp. 59-67, 1999.