A Secure and Efficient Image Encryption Algorithm Based on DNA Coding and Spatiotemporal Chaos

Xiaodong Li[1,2], Cailan Zhou[2], Ning Xu[1,2]
(Corresponding author: Ning Xu)

Hubei Key Laboratory of Transportation Internet of Things, China[1]
School of Computer Science and Technology, Wuhan University of Technology[2]
122, Luoshi Rd., Wuhan, Hubei 430070, P.R. China
(Email: xuning@whut.edu.cn)
(Received Mar. 19, 2017; revised and accepted June 25, 2017)

Abstract

In this paper, an image encryption algorithm based on DNA random coding and random operation combined with chaotic map is proposed. In order to produce sequences with more chaotic characteristics, a new spatiotemporal chaotic system is proposed by employing the Tent-Sine system (TSS) in the coupled map lattice (CML). SHA-256 hash of the plain image is used to generate secret keys. The Lorenz Map, Logistic Map and TSS are applied to generate all parameters the proposed algorithm needs. In order to get the high randomness and overcome the limitations of DNA computing rules, encode the every rows of original image and key image with DNA rules respectively, which are randomly selected from eight encoding rules. Then, apply encoded original image to execute DNA operations with encoded key image row by row to obtain the transitional image and the one of the four DNA operations of every row is determined by logistic map; Finally, randomly decode the transitional image to gain the eventual encrypted image. experimental results demonstrate that the proposed algorithm have ability to resist typical attacks.

Keywords: Coupled Map Lattice; DNA Coding; Lorenz Chaotic Map; SHA-256; Tent-Sine System

1 Introduction

With the rapid development of the Internet, the security of the image constantly attract people's attention. in order to protect the image information are not to be disclosed, many image encryption algorithms are proposed and implemented [4, 16, 22]. Because of bulky data capacity, high redundancy and strong correlations among adjacent pixels, typical image encryption algorithms such as RSA [14], DES [10, 40], AES [15, 21] are not competent to encrypt such digital images. Nowadays, many image encryption algorithm have been proposed, such as, image cryptosystem based on chaos [9, 11, 19, 20, 30], DNA computing [6, 33, 34, 35, 38], fractional fourier transform [1, 36], or cellular automata(CA) [7, 18]. Among those, chaos based image cryptosystem have attracted extensive concerns because of a natural and close connection between chaos and cryptography. Such as, sensitive dependence on initial conditions, pseudo-randomness,ergodicity and reproduction are primary features of chaos system, which meets the requirements of encryption. However, digital implementations of chaotic systems will become periodic eventually because of finite precision and temporal discretization can result with the security risks into chaos based cryptosystem. To overcome the short period issue existing in chaos, spatiotemporal chaotic system with longer period has been widely employed in image cryptography [2, 17, 31]. To improve the chaotic property of three maps Logistic, the Logistic-Tent, Logistic-Sine and Tent-Sine systems were developed [39]. In this paper, TSS combined with CML is used to obtain longer period and generate pseudo-random sequences.

Many of the excellent properties of DNA computing have recently been found, for example: large-scale computational parallelism, huge storage space and tiny energy loss. Therefore, the use of DNA complementary rules to encrypt information technology has made great progress. Zhen et al. [37] proposed an image encryption algorithm based on spatiotemporal chaotic system and DNA coding. In this research, logistic and spatiotemporal chaotic system are proposed, the mix DNA coding and eight DNA encode rules will guarantee the efficiency of image confusion and diffusion. Chai et al. [3] proposed an algorithm based on memristive hyperchaotic system, cellular automata (CA) and DNA sequence. In the research, a dynamic DNA encoding scheme is proposed. Two DNA rule matrices for encoding the plain image and

two-dimensional (2D) CA are generated from chaotic sequences, and they are decided by the plain image, hence we can obtain different DNA encoding rules for different plain image. Wang et al. [26] proposed a novel image encryption algorithm based on DNA computing and chaotic map. In this research, a kind of spatiotemporal chaos map, such as coupled map lattice is exploited to confuse the plain image. After encoded the confused image, permute its rows and columns to obtain the encoded cipher image. Hu et al. [8] proposed a novel image encryption scheme which used hyper dimensional chaotic systems and cycle operation for DNA sequence. In this research, the pseudo-random sequence is controlled by a chens hyper-chaos system, a cycle operation for DNA sequences is used to diffuse the pixel values of the image. After carrying out exclusive-OR operation for decoded matrices, and then the cipher image is generated.

However, the current DNA encoding image encryption algorithm still exist problems [13] including: DNA encoding rules are limited, and the limited DNA computation rules, key sensitivity is low, etc. In view of these problems in the proposed encryption algorithm, the algorithm proposed in this paper will combine the DNA computing with the DNA coding rules, Using the excellent characteristics of chaotic map such as randomness to randomly determine the DNA encode rules and DNA operations. We proposed a new DNA XNOR operation that can increase the choice of DNA computing space. SHA-256 hash of the plain image is used to generate secret keys, as long as the original image has a slight change, SHA-256 hash value will make a huge difference, which enhances the sensitivity of the cryptosystem.

The cryptosystem utilizes a 256 bit external secret key K,which is generated by exploited SHA-256 function to original image. We use K to generate the initial values of TSS system and one-dimensional logistic map. Hence the secret keys are extremely related to plain image. the cryptosystem can resist brute force attack, chosen-plaintext attack and chosen-ciphertext attack. TSS is applied to generate key image of the size of M*N*4, then use randomly encoded key image to conduct random DNA operations with encoded three matrices R, G and B components row by row to obtain three encoded DNA transitional images,and DNA operation and DNA encode rules are randomly decided by one-dimensional logistic map. The Lorenz system [12, 24] is used to generate three sequences. These sequences are used to permute three encoded DNA transitional images.

The main contributions of the proposed encryption algorithm are as follows:

1) Exploit the chaotic map randomly determine the DNA encode rules and DNA operations,then executing DNA coding and computing row by row to guarantee the image's encoding rules and operations of each row are randomly selected.

2) A new spatiotemporal chaotic system is constructed by employing the Tent-Sine system (TSS) in the coupled map lattice (CML).

The rest of this paper is organized in the following manners: Section 2 introduce the basic theory of the proposed algorithm. The proposed image encryption method is explained in Section 3. In Section 4, experimental results and security analysis are proposed. Finally the conclusions are drawn in Section 5.

2 Basic Theory

2.1 TSS-based CML

Algebraic implementation of any chaos map could be periodic, but the period of discrete dynamic system such as, the CML is adequately long to ensure cryptosystem security [26]. The CML defined as in Equation (1):

$$x_{j+1} = (1-e)F(x_{j+1}(i) + eF(x_j)), \tag{1}$$

where i=1,2,...,n is the time variable, j=1,2,...,l is the spatial variable, l is the lattice length (In the proposed image cryptosystem, l=3. $e \in (0,1)$ expresses the coupling factor, $x_j(i)$ expresses the variate for the jth lattice site at time i. Moreover, the periodic boundary of the CML is $x_1(i) = x_{l+1}(i)$. In order to generate extremely random sequences, TSS is adopted as the map $F(x)$:

$$F(x) = \begin{cases} u(1-x)/2 + (4-u)\sin(\pi x)/4 \bmod 1 & x \geq 0.5 \\ (ux/2 + (4-u)\sin(\pi x)/4) \bmod 1 & x < 0.5 \end{cases} \tag{2}$$

Where $x \in (0,1), u \in (0,4]$.

2.2 1-D Logistic Map

In this proposed algorithm, we use 1-D logistic map [29] to select particular category of DNA operations or DNA encoding rules. 1-D logistic map can be defined as in Equation (3).

$$f(x) = rx(1-x) \ x \in [0,1], \tag{3}$$

where $x \in (0,1), r \in (0,4]$. we can figure that when $r \in (3.9,4]$ the random-like sequence is in 0 and 1.

2.3 Lorenz System

As a continuous three-dimensional chaotic system, Lorenz system is defined by the Equation (4):

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \end{cases} \tag{4}$$

Where a, b, c are system parameters, the system is in a chaotic state, while $a = 10$, $b = 28$, $c = 8/3$. It is essential to disperse the system by the fourth-order Runge-Kutta method for encrypting image.

2.4 DNA Encoding and Computing

DNA is composed of four deoxynucleotides A (adenine), G (guanine), C (cytosine), T (thymine), where G and C are complementary, so are A and T. Generally, 0 and 1 are complement to each other in binary system. Hence, 00, 11, 01, 10 could be encoded into the four bases. There are 24 kinds of DNA encoding methods according to combinatorics, but out of which only 8 coding combinations are effective because of the complementary relationship between the four, as listed in Table 1.

Table 1: Encoding and decoding rules

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

In image cryptosystem, the gray value of a pixel can be expressed as its corresponding binary sequence, and then encoded into a DNA sequence. on the contrary, a DNA sequence can be translated into a pixel value. For instance: The pixel value 196, its binary sequence 11000100 could be encoded into a DNA sequence GCAC adopting DNA encoding Rule 5. And so on 55 is gained by decoding the DNA sequence with Rule 7. Additionally, we apply different operations of DNA sequence to encrypt the image. The details of the addition, subtraction, XOR DNA operations rules are shown in the following tables, Table 2 to Table 4.

Table 2: XOR operation

$\oplus$	A	C	T	G
A	A	C	T	G
T	T	G	A	C
C	C	A	G	T
G	G	T	C	A

Table 3: Addition operation

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

Table 4: Subtraction operation

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

Table 5: XNOR operation

$\odot$	A	C	T	G
A	C	A	G	T
T	T	G	C	A
C	A	C	T	G
G	T	G	A	C

Inspired by the DNA Addition, Subtraction, and Exclusive OR operations, we proposed XNOR DNA operation that is shown in Table 5. From this table, we can detect the the value of each row or column is unique. That is, the outcome of XNOR DNA operation is distinctive. In this paper, we will apply these DNA operations rules to diffuse pixel gray values.

2.5 Hash-256

Hash functions are mainly used to provide the security service of integrity. Hash-256 is a widely used cryptographic hash function, which generates 256 bits hash value typically presented as a 64 digit hexadecimal number literally. Due to its good feature of security, even one-bit change can lead to a significant difference between two images. We divide the 256-bit secret key into 8-bit blocks(ki), so K can also be expressed as follows.

$$K = k_1, k_2, k_3 \cdots, k_{32}$$

The initial values can be derived as follows.

$$\begin{cases} x_1 = x'_1 + \frac{(k_1 \oplus k_2 \oplus k_3 \oplus \cdots \oplus k_{11})}{256} \\ x_2 = x'_2 + \frac{(k_{12} \oplus k_{13} \oplus k_{14} \oplus \cdots \oplus k_{22})}{256} \\ x_3 = x'_3 + \frac{(k_{23} \oplus k_{24} \oplus k_{25} \oplus \cdots \oplus k_{32})}{256} \end{cases} \quad (5)$$

$$x_{avg} = \frac{x_1 + x_2 + x_3}{3}, \quad (6)$$

where x'_1,x'_2 and x'_3 are the initial given values.

3 Proposed Cryptosystem

3.1 Key Image Generation

In the image encryption algorithm, the key image is generated by the following steps:

Step 1: Use Equation(5) to modify the initial conditions x'_1,x'_2 and x'_3.

Step 2: On the condition of the parameters e, u and the modified initial values x_1x_2 and x_3, TSS-based CML is executed for 500 times for avoiding the transient effect. Continue to execute the chaotic map for M+$4N$ times and three pseudo-random sequences CL_1, CL_2, CL_3 are obtained. CL_1, CL_2, CL_3 are converted into six sequences as follows:

$$\begin{cases} s'_1 = CL_1(1:2M) \\ s'_2 = CL_2(1:2M) \\ s'_3 = CL_3(1:2M) \\ s'_4 = CL_1(2M+1:4M+N) \\ s'_5 = CL_2(2M+1:4M+N) \\ s'_6 = CL_3(2M+1:4M+N) \end{cases} \quad (7)$$

$$s_j = floor((s'_j \times 10^6 - fix(s'_j \times 10^6)) \times 10^{10}) \mod 256, \quad (8)$$

where j=1, 2, ..., 6, *floor*(a) returns the nearest integer to a towards minus infinity, *fix*(a) rounds a to the nearest integer towards zero. After executing Equation (7) and Equation (8), the pseudo-random sequence of s_j (j=1, 2, ..., 6) is in 0 and 255.

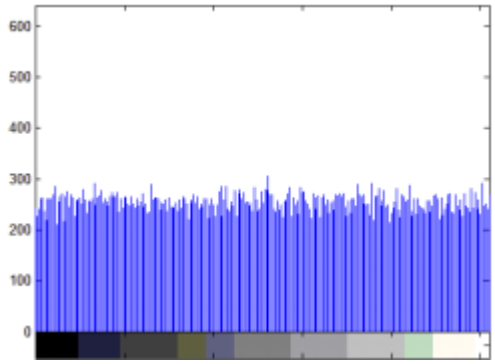


Figure 1: Histogram of the key image

Step 3: The six pseudo-random sequences are handled to generate tow sequences:I_1 of length M and I_2 of length N. Then a key image $KI(M,N)$ is constructed by I_1 and I_2:

$$\begin{aligned} I_1 &= s_1(1:M) \oplus s_2(M+1:2M) \oplus s_3(1:M) \\ I_2 &= s_4(N+1:2N) \oplus s_5(1:N) \oplus s_6(N+1:2N) \end{aligned}$$

$$KI = I_1 \times I_2 = \begin{bmatrix} I_{11} \\ I_{12} \\ \vdots \\ I_{1M} \end{bmatrix} \times \begin{bmatrix} I_{21} & I_{22} & \cdots & I_{2N} \end{bmatrix} = \begin{bmatrix} I_{11}I_{21} & I_{11}I_{22} & \cdots & I_{11}I_{2N} \\ I_{12}I_{21} & I_{12}I_{22} & \cdots & I_{12}I_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ I_{1M}I_{21} & I_{1M}I_{21} & \cdots & I_{1M}I_{2N} \end{bmatrix}$$

Figure 1 shows a sequence of random pixels value which are generated by the proposed method through histogram. The information entropy of the generated key image is 7.9979.

3.2 Encryption Algorithm

In the proposed encryption algorithm, particular DNA encoding rules and DNA operations are randomly decided by 1-D logistic map. Firstly, the SHA-256 is applied on the original image to produce the sequence K and then, the initial values of the TSS-based CML system can be calculated using K. Secondly, R,G and B components of original image and the key image are encoded, applying a randomly selected rule from Table 1, into four DNA sequence matrices. Thirdly, employ encoded key image to conduct random DNA operations with the encoded plain images to obtain a transitional image. Fourthly, the transitional image is permuted by using a Lorenz chaotic sequence. Finally, decode the permuted DNA matrix applying a randomly selected rule from Table 1 to gain the eventual cipher image. The details of the encryption algorithm is presented as follows:

Step 1: The input is a original image $P(M,N,3)$ which M and N express the width and height of the image, respectively.

Step 2: Produce the key sequence K and the initial values x'_1,x'_2 and x'_3 of the Lorenz system and the initial value x_avg of the 1-D Logistic map according to Section 2.5.

Step 3: the plain image is divided into three components, and we obtain three components, R, G and B, and convert the R, G, B to binary matrices R(M,N*8), G(M,N*8) and B(M,N*8), then encode R, G, B by rows with DNA rules that are decided by Equation (2) and Equation (9) and gain three DNA sequence matrices Pr(M,N*4), Pg(M,N*4) and Pb(M,N*4).

$$rule = \lfloor x \times 8 \rfloor + 1. \tag{9}$$

In Equation (9), *rule* is the selected type of DNA rule, which occupies an important position in the encoding stage. The initial value of Equation (2) is provided by Equation (5) and Equation (6). The details about DNA rules are shown in Table 1. Each pixel of a row is coding by particular DNA rule. After all pixels of image are encoded, the size of encoded images are 4*M*N.

Step 4: Generate key image according to Section 3.1, then encode KI by rows with DNA rules that are decided by Equation (2) and Equation (9) and obtain a encoded DNA sequence matrices $KI_e(M,N*4)$.

Step 5: Execute DNA operations between the encoded plain image (Pr, Pg and Pb) and the encoded key image (KI_e) row by row. The particular type of DNA operations is determined by Equation (2) and Equation (10). Details on DNA operations are listed in Table 2 to Table 5.

$$\begin{cases} op = \lfloor x \times 3 \rfloor + 1 \\ pr' = pr \ op \ KI_e \\ pg' = pg \ op \ KI_e \\ pb' = pb \ op \ KI_e \end{cases} \tag{10}$$

Where op is the selected type of DNA operation. Carry out the selected operation row by row After the encoded transitional images are generated, namely Pr', Pg' and Pb', in the process of this period, four kinds of DNA operations (XOR, XNOR +, -) are randomly executed. The size of encoded transitional images are 4*M*N.

Step 6: Generate three chaotic sequences according to the initial value x'_1,x'_2 and x'_3 of the Lorenz system. Executing Equation (4) with the fourth-order Runge-Kutta method for 1000 times to avoid the transient effect, where the step size of the Runge-Kutta method is 0.001. Continue to iterate Lorenz system, three pseudo-random sequences sx, sy and

sz are generated, whose length is $M*N*4$. Then the three sequences are handled by Equation (11).

$$\begin{cases} (lx, fx) = sort(sx) \\ (ly, fy) = sort(sy) \\ (lz, fz) = sort(sz) \end{cases} \quad (11)$$

Where $sort()$ is the sequencing index function, fx is the new sequence after ascending to sx, lx, ly and lz are the index value of fx, fy and fz, respectively.

Step 7: Convert the three binary matrices Pr', Pg' and Pb' to three vectors $Vr(M*N*4)$, $Vg(M*N*4)$ and $Vb(M*N*4)$, respectively. Confuse Vr, Vg and Vb according to:

$$\begin{cases} Vr'(i) = Vr(lx(i)) \\ Vg'(i) = Vg(ly(i)) \\ Vb'(i) = Vb(lz(i)) \end{cases}$$

Step 8: Convert Vr', Vg' and Vb' to three matrices $Re(M, N*4)$, $Ge(M, N*4)$ and $Be(M, N*4)$, respectively. Decode Re, Ge and Be exploiting a selected DNA encoding rule and generate three matrices Rb,Gb and Bb. The decoding rule is according to Equation (9). Randomly DNA decoding and DNA encoding enhance the performance of diffusion process of the proposed algorithm.

Step 9: Finally, merge Rb,Gb and Bb images and that is the ultimate cipher image.The cipher image is with size $M*N$.

3.3 Decryption Algorithm

Decryption algorithm is the inverse process of encryption. receivers should have already obtained the secret keys applied to encrypt the original images. Then we can decode cipher images by following steps:

Step 1: Using randomly selected DNA rules, encode the R, G and B components of the ciphered image. We obtain three matrices Re, Ge and Be, and we convert them to three vectors Vr', Vg' and Vb'. As it is mentioned in Step 3 of the encryption algorithm.

Step 2: Vr', Vg' and Vb' are confused vectors. In order to obtain the non-confused vectors Vr, Vg and Vb, we invert Step 7 which is mentioned in the encryption algorithm as follows:

$$\begin{cases} Vr(i) = Vr'(lx(i)) \\ Vg(i) = Vg'(ly(i)) \\ Vb(i) = Vb'(lz(i)) \end{cases}$$

Where lx,ly and lz are generated as it is mentioned in Step 6 of the encryption algorithm.

Step 3: Convert the three vectors Vr,Vg and Vb to three matrices Pr',Pg' and Pb'.

Step 4: Use encoded key image and encoded cipher image to generate the transitional encoded image. The particular DNA operation is illustrated in Step 5 of Encryption algorithm. After we invert the step 5 of the encryption algorithm to obtain Pr, Pg and Pb, and KI_e is obtained and as it is mentioned in Step 4 of the encryption algorithm.

Step 5: Decode the Pr, Pg and Pb to get the R, G and B components of the plain image. The particular rule is illustrated in Step 3 of the encryption algorithm.

Step 6: Finally, merge R, G and B images and that is the ultimate original image.

4 Simulation Result and Security Analysis

In this paper, we use the standard 256*256*3 color image of "Lena" as the input image. We utilize MATLAB 7.12 to simulate the encryption and decryption operations and set parameters e=0.01, u=1.4356, r=1.4356, x'_1=0.5346x'_2=0.4846, x'_3=0.6969.

4.1 Key Space

A key space larger than 2100 could guarantee high level of security from the crytography of view [27]. In the proposed cryptosystem, the keys are:

1) The given initial values of x'_1,x'_2 and x'_3.

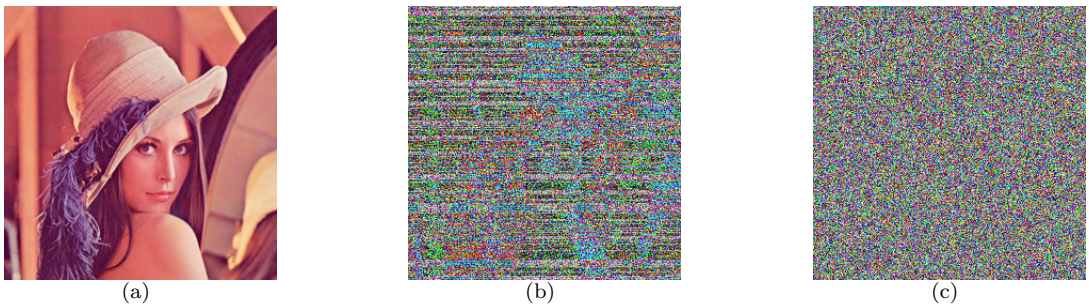
2) The 256-bit long hash value.

3) The parameters of e and u of TSS-based CML and r of the logistic map.

For the initial conditions x'_1,x'_2,x'_3, r, e, and u ,if the precision is 10^{14}, the key space size will be 10^{84}. Further, the key space of the security SHA-256 is 2^{128}, we can get the total key space $S = 2^{128}*10^{84} \approx 3.4*10^{122}$, which is enough to prevent the exhaustive attack. Thus, brute-force attacks on the key are impossible.

4.2 Key Sensitivity

A good encryption algorithm should be sensitive to the secret key; that is, a very tiny different in the secret key will cause a greatly significant change in the output. We conduct a secret key sensitivity test using a key that is just little different from the original key to encrypt Lena image. One of the keys x'_1, u is altered tinily and keep other keys parameters unchanged, then the encrypted image is decrypted by the changed keys. As it can be seen from Figure 2, no effective information is decrypted, which suggests that the proposed cryptosystem could resist the exhaustive attack.



(a) (b) (c)

Figure 2: Key sensitivity tests: decrypted images while (a) right keys, (b) $x'_1 + 10^{-16}$, (c) $u + 10^{-15}$

4.3 The Histogram Analysis

Image histogram is a significant characteristic in image analysis. An ideal cipher image should has a uniform frequency distribution. Figure 3 and Figure 4, illustrate the histograms of the plain and cipher images,it clearly shows that the histograms of the cipher image is uniform and random-like, which suggests that the proposed algorithm does not provide any useful statistic information in the cipher image.

4.4 Information Entropy

The information entropy calculated by Equation (12) is a significant features for measuring the randomness of the cipher image. The gray values distribute more uniformly, the entropy is more close to its ideal value:

$$H(m) = -\sum_{i=0}^{M-1} p(m_i)\log_2 p(m_i), \sum_{i=0}^{M-1} p(m_i) = 1, \quad (12)$$

where m_i (i = 0, 1,$\cdots$, M-1) represents the gray values, $p(m_i)$ (i = 0, 1,$\cdots$, M-1) represents the probability of the symbol s. The entropy should ideally be 8 for a cipher image with 256 gray levels, which indicates that the information is uncertainty. In the paper the average information entropy of the cipher image is 7.9985, close to the ideal value 8. Hence, we conclude that the proposed algorithm has high randomness. The entropy for cipher images using different encryption algorithm are calculated and listed in Table 6, the result of the proposed algorithm in this paper is larger than other algorithms.

Table 6: Results of information entropy

Algorithm	Entropy
Ours	7.9985
[27]	7.9971
[2]	7.9856
[23]	7.9965

4.5 Correlation of Two Adjacent Pixels

To analyze the correlation of the plain image and cipher image, we have randomly selected 5000 pairs of adjacent pixels from plain-image and cipher-image and have calculated the correlation coefficients as follows:

$$\begin{aligned} E &= \frac{1}{N}\sum_{i-1}^{N} x_i \\ D(x) &= \frac{1}{N}\sum_{i-1}^{N} (x_i - E(x))^2 \\ Cov(x,y) &= \frac{1}{N}\sum_{i-1}^{N} (x_i - E(x))(y_i - E(y)) \\ r_{xy} &= \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \end{aligned} \quad (13)$$

The x and y represent gray-level values of two adjacent pixels. The correlation of R, G and B components of plain image and cipher image of Lena is shown in Figure 5. Table 7 shows that the dependence between adjacent pixels of the cipher image is much smaller than of plain-image. These results clearly show that the correlation coefficients of the plain image are close to 1 while those of the cipher image are nearly 0 and the distribution of adjacent pixels is fairly uniform. It indicates that the proposed algorithm has successfully eliminated the correlation of adjacent pixels in the plain image so that neighboring pixels in the cipher image virtually have no correlation. So the proposed algorithm can resist the statistic attacks.

4.6 Differential Attack

The number of pixels change rate (NPCR) and the unified average changing intensity (UACI) for the cipher images are generally applied to evaluate the number of pixels change rate. $C_1(i, j)$ and $C_2(i, j)$ stand for two cipher images which corresponding plain images are only one pixel value difference.

$$\begin{aligned} NPCR &= \frac{\sum_{i=0}^{M-1}\sum_{i=0}^{N-1} D(i,j)}{M \times N} \times 100\% \\ D(i,j) &= \begin{cases} 0, C_1(i,j) = C_2(i,j) \\ 1, C_1(i,j) \neq C_2(i,j) \end{cases} \\ UACI &= \frac{1}{M \times N}\left[\sum_{i=0}^{M-1}\sum_{i=0}^{N-1} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%, \end{aligned} \quad (14)$$

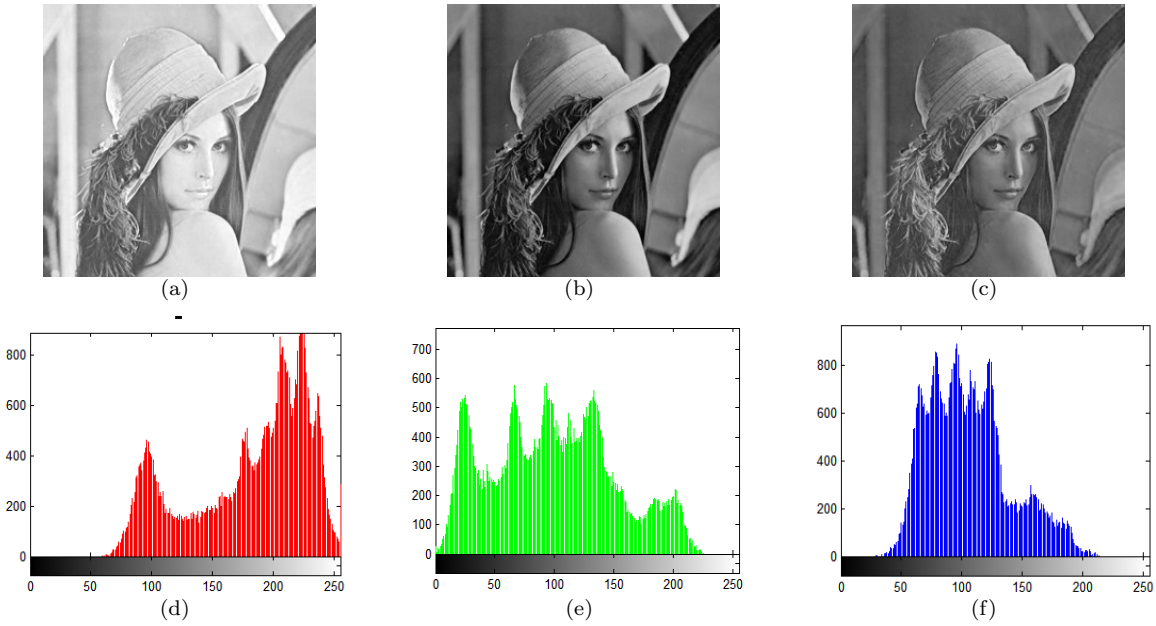


Figure 3: (a) plain image Lena-R, (b) plain image Lena-G, (c) plain image Lena-B, (d) the histogram of the plain image Lena-R, (e) the histogram of the plain image Lena-G, (f) the histogram of the plain image Lena-B

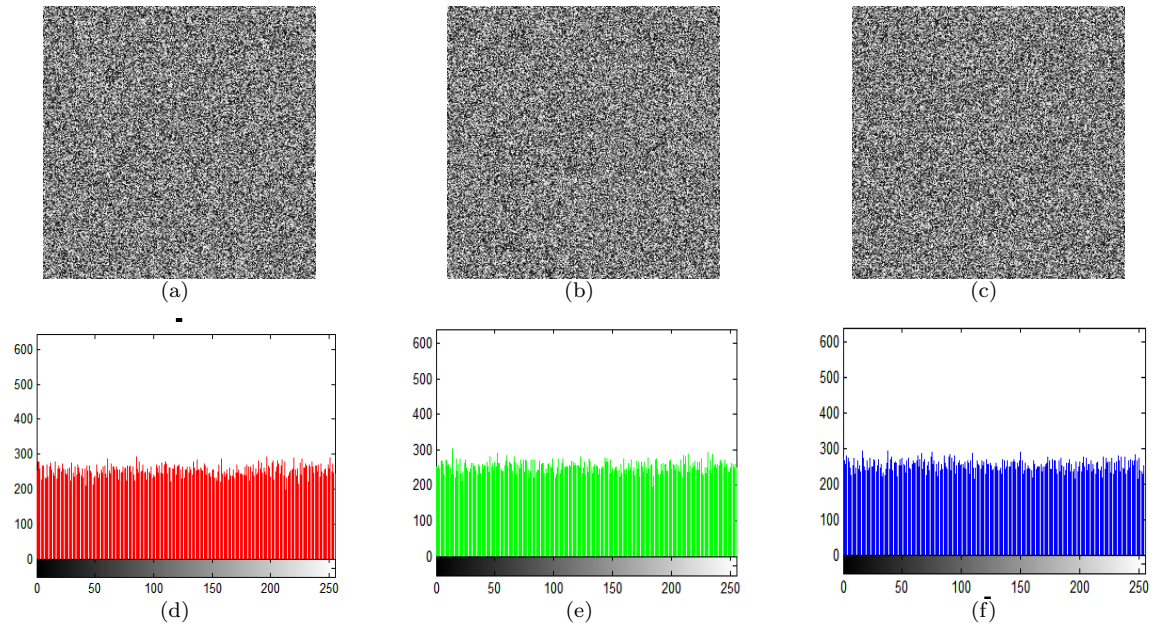


Figure 4: (a) The encrypted image Lena-R, (b) The encrypted image Lena-G, (c) The encrypted image Lena-B, (d) the histogram of the encrypted Lena-R, (d) the histogram of the encrypted Lena-G, (f) the histogram of the encrypted Lena-B.

Table 7: The related correlation coefficient between plain-image and cipher image

Scan direction	Lena					
	Plain image			Cipher image		
	R	G	B	R	G	B
Horizontal	0.9828	0.9725	0.9725	0.0095	0.0183	0.0034
Vertical	0.9689	0.9700	0.9486	-0.0026	0.0001	-0.0035
Diagonal	0.9704	0.9585	0.9585	0.0078	-00039	0.0052

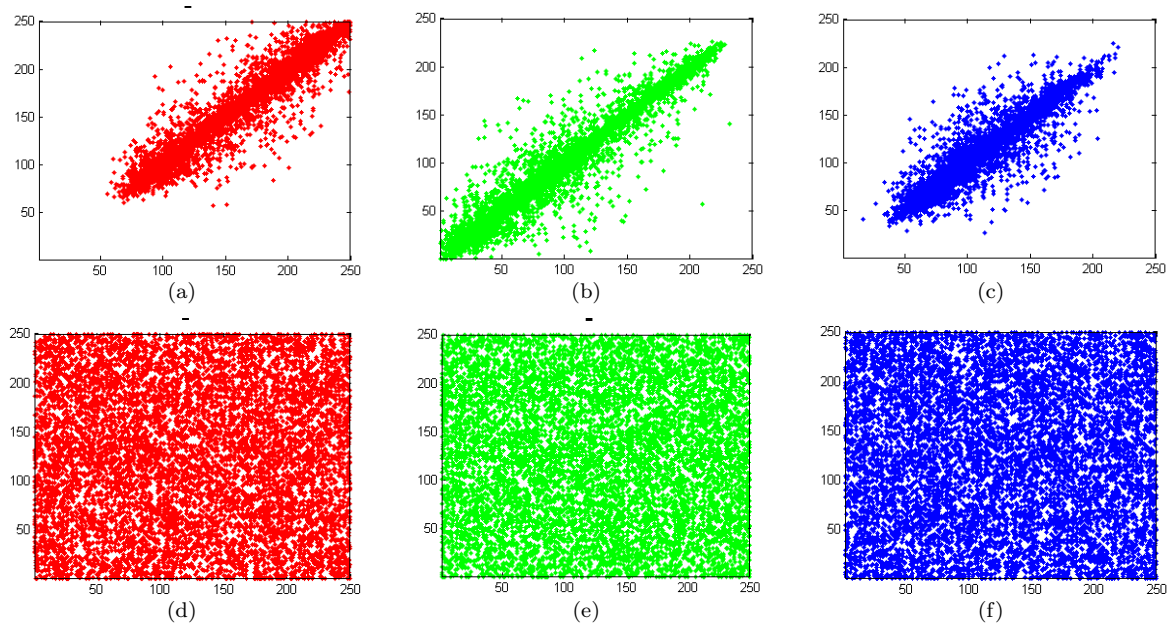


Figure 5: Distribution of two horizontally adjacent pixels in the plain image of Lena in the (a) red, (b) green, (c) blue components. The distribution of two horizontally adjacent pixels in the cipher-image of Lena in the (d) red, (e) green, (f) blue components.

where M and N are the width and height of the cipher image, respectively. In order to evaluate the plain image sensitivity of the proposed algorithm, one pixel randomly selected from the plain image is changed. Two cipher images are generated by encrypting the plain and the modified plain images using the proposed algorithm. The UPCR and UACI between the two cipher images are listed in Table 8 (The experiment is performed over 100 times.). So we can see that the NPCR and UACI are extremely close to the expected values, so the proposed algorithm has the ability to resist the differential attack.

4.7 Data Loss Attack

An ideal cryptosystem should be against data loss attack through transmission and storage. The size of 64*64, 128*128, 256*128 are deleted from the cipher image to evaluate the robustness of the proposed algorithm against the cropping attack, which are shown in Figure 6 (a)-(c). The corresponding decrypted images are shown in Figure 6 (d)-(f) can still be recognizable. So we prove that the proposed algorithm has the ability to resist the data loss attack.

5 Comparison

To demonstrate its superiority, the proposed cryptosystem is compared with the existing image encryption techniques towards some performance indicators, as in Tables 6 and 8. For key space analysis, it is sufficiently large to resist the exhaustive attack. The correlation coefficients of our cryptosystem are more close to 0 than the encryption methods [5, 25, 28, 32], which reveals that the cryptosystem withstands the statistical attack better. The information entropy in this paper is higher compared with those in [2, 23, 39]. Table 8 exhibits that the NPCR, UACI values of the proposed cryptosystem are close to the ideal values, meaning the image cryptosystem with the ability to against the known-plaintext and the chosen-plaintext attacks.

6 Conclusions

In proposed algorithm, a robust image encryption algorithm established on the spatiotemporal chaotic system and DNA operation is proposed. We proposed TSS combined with CML to make up a new spatiotemporal chaos for generating more random sequences. In the DNA operation process, adding the DNA XNOR operation, through this improvement, not only improve the randomness of the encryption,but also enhance the pixels diffusion effect. In order to guarantee the sensitivity of the cryptosystem, the algorithm randomly determine the DNA encode rules and DNA operation which is decided by one-dimensional logistic map. Through the experimental result and security analysis, we find that our algorithm has good encryption effect, larger secret key space and high sensitive to the secret key. Furthermore, the proposed algorithm also can resist most known attacks, such as statistical analysis and exhaustive attacks. All these features show that our algorithm is very suitable for digital image encryption.

Table 8: Results of NPCR and UACI

Image	NPCR			UACI		
	R	G	B	R	G	B
Our (Lena)	99.6395	99.6378	99.6564	33.6875	33.4883	33.4796
Our (Peppers)	99.6404	99.6299	99.6283	33.3998	33.5734	33.5387
[5]	99.60	99.60	99.59	33.52	33.49	33.38
[25]	99.6086	99.6086	99.6086	33.5000	33.5000	33.5000
[32]	99.61	99.61	99.61	33.38	33.38	33.38
[28]	99.5862	99.2172	98.8479	33.4834	33.4639	33.2689

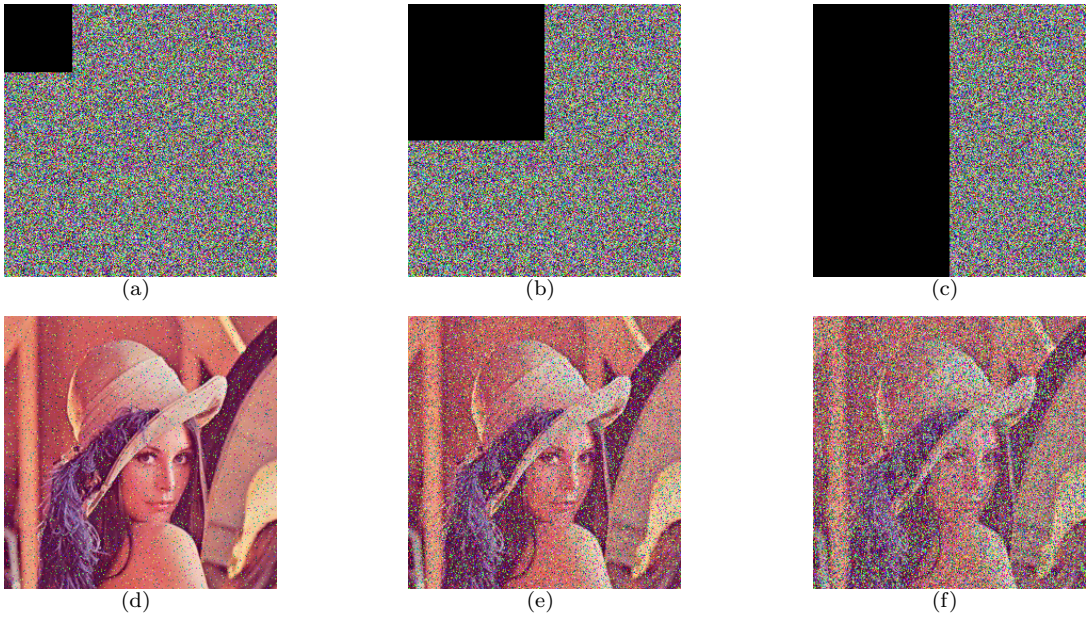


Figure 6: The encrypted Lena with (a) 1/16, (b) 1/4, (c) 1/2 data cropping; corresponding decrypted images (d)-(f) from (a)-(c).

References

[1] S. E. Azoug and S. Bouguezel, "A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional fourier transform," *Optics Communications*, vol. 359, no. 1, pp. 85–94, 2016.

[2] R. Bechikh, H. Hermassi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Breaking an image encryption scheme based on a spatiotemporal chaotic system," *Image Communication*, vol. 39, no. PA, pp. 151–158, 2015.

[3] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Processing Image Communication*, vol. 52, pp. 6–19, 2017.

[4] C. C. Chang, M. S. Hwang, T. S. Chen, "A new encryption algorithm for image cryptosystems", *Journal of Systems and Software*, vol. 58, no. 2, pp. 83–91, Sep. 2001.

[5] P. Devaraj and C. Kavitha, *A Coupled Chaos Based Image Encryption Scheme Using Bit Level Diffusion*, Springer International Publishing, 2015.

[6] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics & Lasers in Engineering*, vol. 56, no. 5, pp. 83–93, 2014.

[7] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "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.

[8] T. Hu, Y. Liu, L. H. Gong, and C. Y. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," *Nonlinear Dynamics*, pp. 1–16, 2016.

[9] I. A. Ismail, M. Amin, and H. Diab, "A digital image encryption algorithm based a composition of two chaotic logistic maps," *International Journal of Network Security*, vol. 11, no. 1, pp. 1–10, 2010.

[10] B. Jin, D. Wang, and G. Xu, "A new method of fast image encryption based on image characteristics

and DES," in *Wireless Communication and Sensor Network: Proceedings of the International Conference on Wireless Communication and Sensor Network (WCSN'15)*, pp. 520–525, 2016.

[11] C. Jin, H. Liu, "A color image encryption scheme based on Arnold scrambling and quantum chaotic," *International Journal of Network Security*, vol. 19, no. 3, pp. 347–357, 2017.

[12] J. Li, Y. Xing, C. Qu, and J. Zhang, "An image encryption method based on tent and lorenz chaotic systems," pp. 582–586, 2015.

[13] Y. Liu, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map," *Optics and Laser Technology*, vol. 60, pp. 111–115, 2013.

[14] G. Lokeshwari, S. Susarla, and S. U. Kumar, "A modified technique for reliable image encryption method using merkle-hellman cryptosystem and RSA algorithm," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 18, no. 3, pp. 293–300, 2015.

[15] K. J. Nandu and R. G. Kumar, "Security enhanced image encryption using password based AES algorithm," *International Journal of Engineering & Technical Research*, vol. V4, no. 6, 2015.

[16] S. V. Sathyanarayana, M. A. Kumar, and K. N. H. Bhat, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points," *International Journal of Network Security*, vol. 12, no. 3, pp. 137–150, 2011.

[17] C. Song and Y. Qiao, "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 17, no. 10, pp. 6954–6968, 2015.

[18] A. Souyah and K. M. Faraoun, "An image encryption scheme combining chaos-memory cellular automata and weighted histogram," *Nonlinear Dynamics*, vol. 86, no. 1, pp. 1–15, 2016.

[19] W. Srichavengsup and W. San-Um, "Data encryption scheme based on rules of cellular automata and chaotic map function for information security," *International Journal of Network Security*, vol. 18, no. 6, pp. 1130–1142, 2016.

[20] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map," *Multimedia Tools & Applications*, vol. 74, no. 15, pp. 1–20, 2015.

[21] S. M. Wadi and N. Zainal, "High definition image encryption algorithm based on AES modification," *Wireless Personal Communications*, vol. 79, no. 2, pp. 811–829, 2014.

[22] O. Wahballa, A. Wahaballa, F. Li, I. Ibn Idris and C. Xu, "Medical image encryption scheme based on Arnold transformation and ID-AK protocol," *International Journal of Network Security*, vol. 19, no. 5, pp. 776–784, 2017.

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

[24] X. Y. Wang, P. Li, Y. Q. Zhang, L. Y. Liu, H. Zhang, and X. Wang, "A novel color image encryption scheme using DNA permutation based on the lorenz system," *Multimedia Tools & Applications*, pp. 1–23, 2017.

[25] X. Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[26] X. Y. Wang, Y. Q. Zhang, and X. M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 73, no. 73, pp. 53–61, 2015.

[27] X. Y. Wang, Y. Q. Zhang, and Y. Y. Zhao, "A novel image encryption scheme based on 2-D logistic map and DNA sequence operations," *Nonlinear Dynamics*, vol. 82, no. 3, pp. 1269–1280, 2015.

[28] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.

[29] G. C. Wu and D. Baleanu, "Discrete fractional logistic map and its chaos," *Nonlinear Dynamics*, vol. 75, no. 1-2, pp. 283–287, 2014.

[30] W. S. Yap, C. W. Phan, W. C. Yau, and S. H. Heng, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map," *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1483–1491, 2015.

[31] M. Zhang and X. Tong, "A new algorithm of image compression and encryption based on spatiotemporal cross chaotic system," *Multimedia Tools & Applications*, vol. 74, no. 24, pp. 11255–11279, 2015.

[32] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical & Computer Modelling*, vol. 52, no. 1112, pp. 2028–2035, 2010.

[33] S. Zhang and T. Gao, "An image encryption scheme based on DNA coding and permutation of hyperimage," *Multimedia Tools & Applications*, vol. 75, no. 24, pp. 17157–17170, 2016.

[34] Y. Zhang, "Cryptanalysis of an image encryption algorithm based on chaotic modulation of arnold dual scrambling and DNA computing," *Advanced Science Focus*, vol. 2, no. 1, pp. 67–82(16), 2014.

[35] Y. Q. Zhang, X. Y. Wang, J. Liu, and Z. L. Chi, "An image encryption scheme based on the mlncml system using DNA sequences," *Optics & Lasers in Engineering*, vol. 82, pp. 95–103, 2016.

[36] T. Zhao, Q. Ran, L. Yuan, Y. Chi, and J. Ma, "Security of image encryption scheme based on multi-parameter fractional fourier transform," *Optics Communications*, vol. 376, pp. 47–51, 2016.

[37] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools & Applications*, vol. 75, no. 11, pp. 6303–6319, 2016.

[38] S. Zhou, B. Wang, X. Zheng, and C. Zhou, "An image encryption scheme based on DNA computing and cellular automata," vol. 2016, no. 2, pp. 1–9, 2016.
[39] 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.
[40] W. Y. Zibideh and M. M. Matalgah, "Modified data encryption standard encryption algorithm with improved error performance and enhanced security in wireless fading channels," *Security & Communication Networks*, vol. 8, no. 4, pp. 565–573, 2015.

Biography

Xiaodong Li is a M.S. candidate at school of Computer science and technology of Wuhan University of Technology. His research interests include: image encryption, information security.

Cailan Zhou received the M.S degrees in Computer science and technology from Wuhan University of Technology, China. She is an associate professor at the Computer science and technology from Wuhan University of Technology, China. Her main research interests include digital image processing,Machine learning and Deep learning, etc.

Ning Xu received his Ph.D. degree in electronic science and technology from the University of Electronic Science and Technology of China in 2003. Later, he was a postdoctoral fellow with Tsinghua University from 2003 to 2005. Currently, he is a professor at the Computer Science Department of Wuhan University of Technology. Dr. Xus research interests include computer-aided design of VLSI circuits and systems, computer architectures, data mining, and highly combinatorial optimization algorithms.