# Chaos-based image encryption using a hybrid cellular automata and a DNA sequence

Abolfazl Yaghouti Niyat
Department of Software Engineering, Islamic Azad University, Mashhad Branch, Mashhad, Iran
ayaghouti@gmail.com

Reza Mohammad Hei Hei
Department of Software Engineering, Islamic Azad University, Mashhad Branch, Mashhad, Iran
r.mohammadi.gh@gmail.com

Majid Vafaei Jahan
Department of Software Engineering, Islamic Azad University, Mashhad Branch, Mashhad, Iran
Vafaeijahan@mshdiau.ac.ir

*Abstract*— **A novel image encryption algorithm based on a hybrid model of deoxyribonucleic acid (DNA), cellular automata (CA) and chaotic system is proposed. CA due to its complex behavior has several applications such as generating random numbers and cryptography. DNA rules, DNA sequence XOR operator and CA rules are used simultaneously to encrypt the plain-image pixels. To determine rule number in DNA sequence and also CA, a 2-dimension logistic map is employed. Experimental results show that the proposed image encryption scheme has a lot of characteristics, including large key space, low correlation of adjacent cipher pixels, and high security, which can effectively protect the security of the encrypted image.**

***Keywords-Chaotic map; Image encryption; Cellular Automata (CA); Deoxyribonucleic acid (DNA); 2 – D Logistic map***

## I. INTRODUCTION

Along with the rapid development of computer and Internet, information security has become an increasingly serious issue. In recent years, cryptosystems based on chaos theory have attracted a great deal of attention [1]. The chaos system possesses of a variety of characteristics, such as high sensitivity to initial conditions, determinacy, ergodicity and so on. Chaotic sequences produced by chaotic maps are often pseudo-random sequences, and their structures are very complex and difficult to be analyzed and predicted [2-6]. The first work applying CA as pseudo-random number generator (PRNG) was done by Wolfram in 1986. His work shows the ability of CA to generate random bits [7]. Cellular automata which are a class of discrete dynamical systems can be implemented in image encryption without much additional hardware or software complexity as a good option in the transmission of large amount of data applications [8]. In recent years, CAs has been already used largely for image cryptography, image processing, authentication and security and so on. Also other methods have been researched for image encryption [9].

With the research of DNA computing, DNA cryptography is born as a new cryptographic field emerged, in which DNA is used as information carrier and the modern biological technology is used as implementation tool [10]. In 1994, Adleman [11] did the first ever experiment on DNA computing, and initiated a new stage in the information age. In subsequent research, the characteristics of DNA computing, massive parallelism, huge storage and ultra-low power consumption had been found. In recent years, the researchers have proposed another kind of image encryption schemes, namely, DNA-based image encryption methods. Liu et al. [12] introduced an image encryption method using DNA complementary rule and two chaotic maps with good stochastic property. Shyam et al.[13] proposed a novel encryption scheme based on DNA computing, they used the nature DNA sequences to encoding the information and encrypted an image by using the XOR logic operation. Zhang et al. [14] proposed DNA-based image encryption where they used definitions of DNA sequence operations to encrypt image pixels and combined hyper-chaotic maps, image fusion operation and DNA sequence XOR operations to implement image encryption.

In this paper, we combine two-dimensional coupled Logistic map, DNA sequence and CA to construct a secure image encryption scheme. Firstly, all the plain-image pixels should be converted to DAN nucleic acids by standard rules which are defined in DNA sequence, then, a one-dimensional, uniform CA with a periodic boundary condition is used to generate a new sequence for encrypting plain-image pixels. In order to choose standard rules in DAN sequence, we uses two-dimensional coupled Logistic map. Combination of CA, DNA and two-dimensional coupled Logistic map make proposed algorithm very strong against common attack in the image encryption method.

The rest of the paper is organized as follows. In Section II, the preliminary is introduced. The proposed image encryption scheme is presented in Section III. In Section IV, some simulation results and the security analysis are given. Finally, In Section V, some conclusions are drawn.

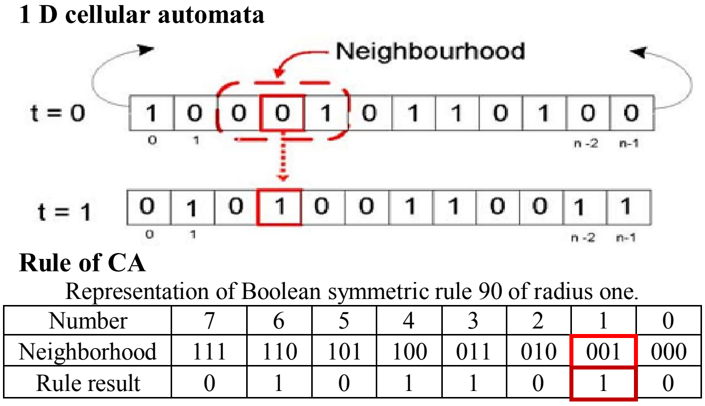
## II. Preliminaries

### A. Cellular automata

A Cellular automata (CA), introduced by von Neumann in 1940s, is a dynamic system in which its time, space and states are all discrete. The CA evolves deterministically in discrete time steps and each cell takes its value from a finite set S, called the State Set. A CA is named Boolean if S ϵ {0,1}[15]. The cells change their states synchronously at discrete time instants. The next state of each cell depends on the current states of the neighbor cells according to a state transition rule. Elementary cellular automata (ECA) are the simplest case, which is a linear array of cells with three neighborhood dependency, and state of each cell is 0 or 1. Let $S_i$ denotes the current state of the i-th cell at time t, and *f* a Boolean state function that specifies the local rule. The next state of $S_i$ at time t+1 is produced as:

$$S_i^{t+1} = f(S_{i-1}^t, S_i^t, S_{i+1}^t) \qquad (1)$$

The set of local rules for the time evolution of one dimensional CA has been coded by Wolfram in [16]. An example of Wolfram's notation for CA rule 90 is given in Fig.1 [17]. The rule number represents the binary number in a decimal way. For example, if *f* (1 1 1) = 0, *f* (1 1 0) = 1, *f* (1 0 1) = 0, *f* (1 0 0) = 1, *f* (0 1 1) = 1, *f* (0 1 0) = 0, *f* (0 0 1) = 1, *f* (0 0 0) = 0, then the binary number 01011010 is 90 in decimal. So, the CA is called Rule 90 CA. Since the neighborhood is composed of 3 cells, for each cell there are two values, 0 and 1. Therefore, 2 × 2 × 2 = $2^3$ possible binary states for the three cells neighboring a given cell, there are a total $2^8$ = 256 cellular automata, each of which can be indexed with an 8-bit binary number [18, 19]. If all CA cells obey the same rule, then the CA is said to be a uniform CA; otherwise, it is a non-uniform CA [20]. In addition, a CA is said to be a CA with periodic boundary condition if the extreme cells are adjacent to each other; otherwise, it is called null-boundary CA [21]. In this paper, we used a uniform one-dimensional CA with periodic boundary and {0, 1} as its states and the state of each cell depends on the state of itself and its neighbors.



| Number | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| Neighborhood | 111 | 110 | 101 | 100 | 011 | 010 | 001 | 000 |
| Rule result | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |

Figure 1. 1D cellular automata with neighborhood=1.

### B. DNA sequence encryption

#### 1) DNA encoding and decoding for image

A DNA sequence contains four nucleic acid bases A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are complementary, G and C are complementary. Because 0 and 1 are complementary in the binary, so 00 and 11 are complementary, 01 and 10 are also complementary. By using four bases A, C, G and T to encode 00, 01, 10 and 11, there are 24 kinds of coding schemes. But there are only eight kinds of coding schemes satisfy the Watson-Crick complement rule, which are shown in Table I [22].

In this paper, we use the DNA code to encode the image. For the 8 bit image, each pixel can be expressed as a DNA sequence whose length is 4 (its binary sequence's length is 8). For example: if there is a pixel with a gray level 157, the binary format is (10011101)2. The DNA code for all 8 rules in Table I is as follows: Rule 1 (CGTG), Rule 2 (GCTC), Rule 3 (CGAG), Rule 4 (GCAC), Rule 5 (ATGT), Rule 6 (TAGA), Rule 7 (ATCT) and Rule 8 (TACA).

### C. XOR algebraic operation for DNA sequences

With the rapid developments of DNA computing, some biology operations and algebraic operations based on DNA sequence are presented by researchers, such as XOR operation. XOR operation for DNA sequences is performed according to traditional XOR in the binary. Corresponding to eight kinds of DNA encoding schemes, there also exist eight kinds of DNA XOR rules. In this paper, we used the XOR operation to fusion the original image. For example, there are two DNA sequences [AGCT] and [CTGA], we adopt one type of XOR operation which is shown in Table II to XOR them and we get a sequence [CCTT] as the result. The XOR operation is reflexive. So, we also can get the sequence [AGCT] by sequence [CATT] XOR sequence [CTGA] under the XOR operation. From Table II, we can see that any one base in every row or column is unique, in other words, the results of XOR operation is one and only [14, 23, 24]. In this paper, we will use this XOR operation rule to scramble the pixel values of the original image.

TABLE I. **Eight kinds of schemes encoding and decoding map rule of DNA sequence.**

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

TABLE II. **One type of XOR operation for DNA sequences.**

| **XOR** | **A** | **G** | **C** | **T** |
|---|---|---|---|---|
| A | A | G | C | T |
| G | G | A | T | C |
| C | C | T | A | G |
| T | T | C | G | A |

### D. Logistic map function

Overall, because of the inherent characteristics of chaotic functions, they are strongly sensitive to the initial parameter values and their related evolution function [25]. This means a slight alteration in input parameter value causes huge changes in the value that is generated by the evolution function. One of the most popular and useful chaotic functions is the logistic map function described in Eq. (2) [26].

$$X_{n+1} = RX_n(1 - X_n) \qquad (2)$$

Where $X_0$ is initial condition, $R$ is the system parameter and $n$ is the number of iterations. The research shows that the map is chaotic for 3.57 < $R$ < 4 and $X_{n+1}$ belong to the interval (0, 1) for all $n$.

### *E. 2D Coupled Logistic Mapping*

The two-dimensional coupled Logistic map [27] is described as follows:

$$x_{n+1} = \mu_1 x_n(1 - x_n) + \mu_1\, y_n^2$$
$$y_{n+1} = \mu_2 y_n(1 - y_n) + y_2(\, x_n^2 + x_n\, y_n) \qquad (3)$$

This system is chaotic when 2.75 < µ1 ≤ 3.4, 2.7 < µ2 ≤ 3.45, 0.15 < γ1 ≤ 0.21 and 0.13 < γ2 ≤ 0.15 and generate chaotic sequences x, y in the interval (0, 1).

## III. Proposed Method

To have a safe and secure encryption algorithm, the value of $X_0$ and $y_0$ in Eq. (3) is taken from a 256-bit key which is created as:

K=$\{k_0, k_1, k_2, \dots, k_{31}\}$

Subject to: $k_i = \{k_{i,0}, k_{i,1}, \dots, k_{i,7}\}$ (4)

Where in $k_{i,j}$, i denotes the character number and j shows the bit number in $k_i$.

There are two usages for secret key to generate x0 and also yo, in 2D Logistic map, where are used to determine two rules number in Table I. These initial values (x0 and y0) are calculated as

$$X_0 = \frac{k_1 \oplus k_2 \oplus \dots \oplus k_{15} + \sum_{i=1}^{15} k_i}{2^{12}} \qquad (5)$$

$$y_0 = \frac{k_{15,0}^{127} + \ k_{15,1}^{128} + \ \dots \ \ + k_{31,0}^{256} + \cdots \ \ + k_{31,7}^{256}}{2^{128}} \qquad (6)$$

Where Ki represents an 8-bit character and ⊕ denotes an exclusive OR. Owing to Eqs. (5) and (6), both x0 and y0 belong to interval [0, 1]. Values x0 and y0 are employed to generate x1 and y1 as the starting points of 2D Logistic map. All generated x and y are used to determine two DNA rules number for encoding plain-image pixels and CA content. These rules number (R) in Table I will be chosen with the help of Eq. (7) and Eq. (8).

DNA_R1= $\lfloor X_n \times 7 \rfloor + 1$ (7)

DNA_R2= $\lfloor y_n \times 7 \rfloor + 1$ (8)

The initial value for CA is drawn as Eq. (9).

CA= $k_{\,i=\mathrm{mod}\,(\,\mathrm{fix}\,(X_0\ \times 2^{31})\,,31)}$ (9)

UPD_R= $\lfloor x_n \times 7 \rfloor + 1$ (10)

TABLE III. **Boolean Expression of Each CA Rule.**

| $R_i$ | Rule number | Boolean function |
|---|---|---|
| 1 | 30 | $S_i^{t+1} = S_{i-1}^t$ xor $[S_i^t$ or $S_{i+1}^t]$ |
| 2 | 90 | $S_i^{t+1} = S_{i-1}^t$ xor $S_{i+1}^t$ |
| 3 | 150 | $S_i^{t+1} = S_{i-1}^t$ xor $S_i^t$ xor $S_{i+1}^t$ |
| 4 | 153 | $S_i^{t+1} = S_i^t$ xnor $S_{i+1}^t$ |
| 5 | 165 | $S_i^{t+1} = S_{i-1}^t$ xnor $S_{i+1}^t$ |
| 6 | 86 | $S_i^{t+1} = [S_{i-1}^t$ nor $S_i^t]$ xor $[\mathrm{not}(S_i^t)]$ |
| 7 | 105 | $S_i^{t+1} = \mathrm{not}[S_{i-1}^t$ xor $S_i^t$ xor $S_{i+1}^t]$ |
| 8 | 101 | $S_i^{t+1} =$<br>$[S_{i-1}^t$ nor $S_{i+1}^t]$or$[(S_i^t$ xor $S_{i+1}^t)$and$S_{i-1}^t\,]$ |

TABLE IV. **CA rules lookup table.**

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 165 | 105 | 86 | 153 | 90 | 101 | 30 | 150 |

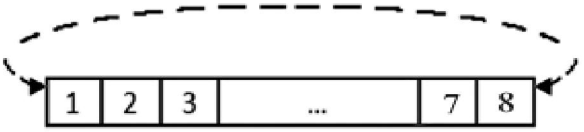


Figure 2. Selection of cells neighborhood.

In our approach, a one-dimensional, uniform 1 × 8 CA with a periodic boundary condition is used to generate random numbers using 8 rules: 153, 30, 90, 165, 86, 105, 101, 150. The Boolean expression of each CA rule is shown in Table III. According to [28], generated numbers by these rules have the best results in different tests such as entropy, chi-square and diehard. Each cell determines its next state based on its current state and simultaneously its left side and right side neighbor's state. Each cell has exactly two fixed neighbors, for example cells i-1 and i+1 are the neighbors of cell i. Moreover, as shown in Fig. 2, neighbors CA(1) are CA(8) and CA(2), and neighbors CA(8) are CA(7) and CA(1).

The following equation is used to encrypt pixels in the plain-image with M row and N column.

$$\acute{C}(i,j) = \begin{cases} p(i,j) \oplus CA(1,\dots,8) & i = 1, j = 1 \\ p(i,j) \oplus CA(1,\dots,8) \oplus \acute{C}\,(i,j-1) & \text{Otherwise} \end{cases} \qquad (11)$$

The mentioned XOR in Eq. (11) is the biological XOR that is taken from Table II. P(i,j) and Ć(i,j) show pixels, in position i and j, in plain-image and cipher-image, respectively. Value of P(i,j) will be changed to binary format, then this value and CA(1, ..., 8) will be converted to DNA sequence format, using rules in Table I, which are determined by DNA_R1 and DNA_R2, respectively. From the set of 256 CA rules we select eight rules: 153, 30, 90, 165, 86, 105, 101, and 150 for image encryption. According to Table IV in each stage is used as CA standard rule number for updating ca (1, ..., 8) in the next stage. UPD-R will be chosen with the help of Eq. (10) for determine rule number in Table IV. In final step of proposed encryption algorithm, Ć(i,j) in each stage will convert to binary format using DNA_R1, which is generated in the same stage, to determine rule number in Table I. In the following of this work, an example is provided in Fig.3 to make the proposed method easy to understand.

Assume that $x_0$=0.33, $y_0$=0.85, $p = \begin{array}{|c|c|}\hline 150 & 237 \\ \hline \end{array}$ , $ca = \begin{array}{|c|c|c|c|c|c|c|c|}\hline 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ \hline \end{array}$

$\mu_1$=2.93, $\mu_2$=3.173, $y_1$=0.197, $y_2$=0.139

P(1,1) = 150 $\xrightarrow{\text{Binary}}$ $(10010110)_2$

$x_0$=0.33, $y_0$= 0.85 $\xrightarrow{\text{Eq.3}}$ $x_1$ =0.7901, $y_1$=0.7057

$x_1$ =0.7901 $\xrightarrow{\text{Eq.7, n = 1}}$ DNA-R1= 6 AND $y_1$=0.7057 $\xrightarrow{\text{Eq.8, n = 1}}$ DNA-R2 = 5

P(1,1) = $(10010110)_2$ $\xrightarrow{\text{DNA-R1= 6}}$ ATTA , ca(1, ..., 8) = $(01011010)_2$ $\xrightarrow{\text{DNA-R2= 5}}$ TTAA

Ĉ(i,j) $\xrightarrow{\text{Eq.11 when i = 1, j = 1}}$ ATTA ⊕ TTAA $\xrightarrow{\text{Table II}}$ TATA $\xrightarrow{\text{DNA-R1= 6}}$ $(01100110)_2$ $\xrightarrow{\text{Decimal}}$ 102

P(1,2) = 237 $\xrightarrow{\text{Binary}}$ $(11101101)_2$

$x_1$ =0.7901, $y_1$=0.7057 $\xrightarrow{\text{Eq.3}}$ $x_2$ =0.5839, $y_2$=0.8748

$x_2$ =0.5839 $\xrightarrow{\text{Eq.7, n = 2}}$ DNA-R1= 5 AND $y_2$= 0.8748 $\xrightarrow{\text{Eq.8, n = 2}}$ DNA-R2 = 7

P(1,2) = $(11101101)_2$ $\xrightarrow{\text{DNA-R1= 5}}$ CACT AND $x_2$ =0.5839 $\xrightarrow{\text{Eq.10, n = 2}}$ UPD-R= 5

ca(1, ..., 8) = $(01011010)_2$ $\xrightarrow{\text{Update CA by UPD-R (rule 90)}}$ $ca = \begin{array}{|c|c|c|c|c|c|c|c|}\hline 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ \hline \end{array}$

ca(1, ..., 8) = $(10011001)_2$ $\xrightarrow{\text{DNA-R2 = 7}}$ CGCG

Ĉ(i,j) $\xrightarrow{\text{Eq.11 when i = 1, j = 2}}$ CACT ⊕ CGCG ⊕ TATA $\xrightarrow{\text{Table II}}$ TGTC $\xrightarrow{\text{DNA-R1= 5}}$ $(01000111)_2$ $\xrightarrow{\text{Decimal}}$ 71

Cipher-image Ĉ = $\begin{array}{|c|c|}\hline 102 & 71 \\ \hline \end{array}$

Figure 3. An example of proposed method step.

## IV. Simulation Result and Analysis

In the current section, the various experiments performed to identify and validate the proposed method's performance are described.

### 1) *Statistical attack*

Histogram and correlation tests are investigated in the coming sub-sections to avoid a statistical attack.

#### a) *Histogram analysis*

The histogram is one of the most statistical characteristics of an image, and represents the frequency of all the gray level values from all over the image. Fig. 4 depicts the histogram of the Pepper image based on the statistical analysis of the plain image and the cipher image. Unlike the uniformity of the cipher image, the histogram of the plain image fluctuated as seen in Fig. 4.

#### b) *Correlation coefficient analysis*

It is well known that the less correlation of two adjacent pixels the stronger ability of resisting statistical attack. In this section, correlation coefficient of two adjacent pixels in original image and encrypted image is studied. In order to test the correlation between two adjacent pixels, we randomly select 4096 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original image and the encrypted image, using the following formulas to calculate the correlation coefficient.

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

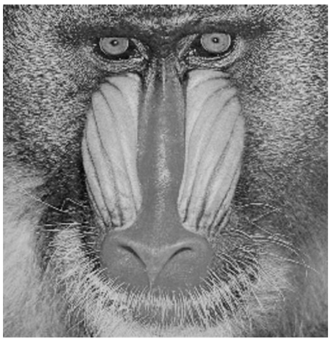
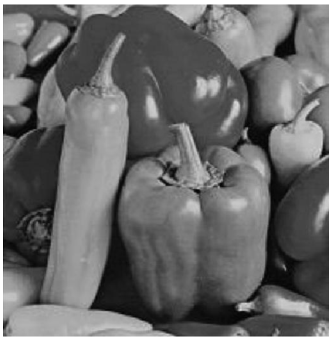
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (12)$$

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

$$r_{xy} = \frac{Cov(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}}$$

Where x and y are the grey value of two adjacent pixels in the image, Cov(x, y) is covariance, D(x) is variance, E(x) is mean. The related result is defined in Table V shows the correlation coefficient of the cipher-images.

TABLE V. **Obtained correlation coefficient in Vertical, Horizontal and Diagonal direction**

| | |  |  |
|---|---|---|---|
| **Vertical** | **-0.0084** | **-0.0091** | **-0.0089** |
| **Horizontal** | **0.0324** | **0.0505** | **0.0213** |
| **Diagonal** | **0.0025** | **0.0017** | **0.0013** |

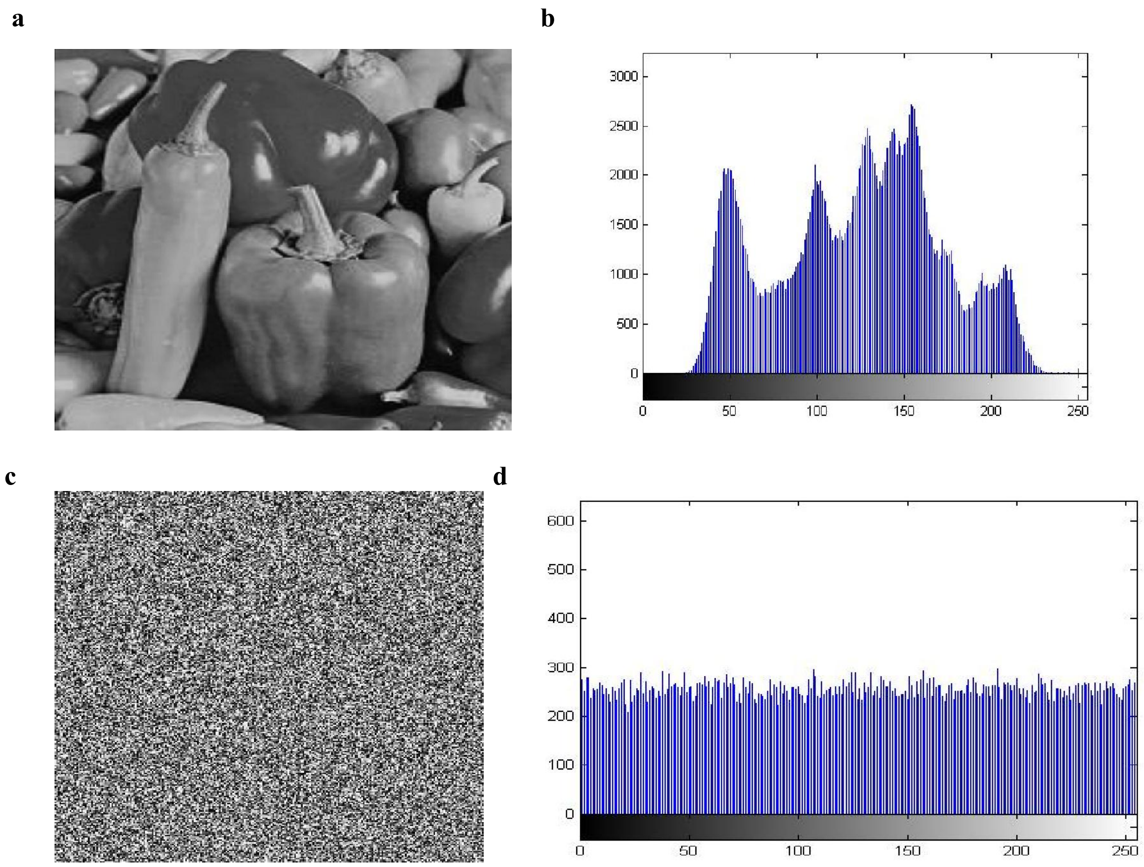


Figure 4. (a) plain-image, (b) histogram of plain-image, (c) cipher-mage, (d) histogram of cipher-image.

TABLE VI. The information entropy of encrypted image.

| Image | Fatima | Baboon | Peppers | Lena |
|---|---|---|---|---|
| H | 7.9968 | 7.9965 | 7.9975 | 7.9978 |

### 2) *Security analysis*

#### a) *Information entropy*

The information entropy is defined to express the degree of uncertainties in the system [29]. We can also use it to express uncertainties of the image information. The information entropy can measure the distribution of grey value in the image, the results show that the greater information entropy the more uniform of the distribution of grey value. The information entropy is defined as follows:

$$\mathrm{H(m)} = -\sum_{\mathrm{i=0}}^{\mathrm{L}} \mathrm{p(m_i)} \log_2 \mathrm{p(m_i)} \tag{13}$$

where $\mathrm{m_i}$ is the ith grey value for L level grey image, $\mathrm{p(m_i)}$ is the emergence probability of $\mathrm{m_i}$, so $\sum_{\mathrm{i=0}}^{\mathrm{L}} \mathrm{p(m_i)} = 1$. For an ideally random image, the value of the information entropy is 8. An effective encryption algorithm should make the information entropy tend to 8. The information entropies of encryption images are shown in Table VI, all of which are very close to 8. It is can be seen that the propose algorithm is very effective.

#### b) *Key space analysis*

The brute-force attack has the ability to attack against existing types of encryption, with different degrees of success. In this type of attack, attackers have cipher-image and secret key as well and they try to check each variant of secret key automatically with a computer program which makes speed of searching for exact key faster. The brute-force attack basically starts with one-digit secret key, and then go to two-digit secret key going on until the end of secret key. In order to resist against brute-force the secret key space should be quite large[26]. To avoid brute-force attacks, the secret key space is $2^{256}$, so the encryption algorithm has a large enough key space to resist all kinds of brute-force attacks.

## V. CONCLUSIONS

In this paper, we proposed a novel image encryption algorithm based on hybrid DNA sequence, CA and two-dimensional Logistic map. DNA rules, DNA sequence XOR operator and CA rules are used simultaneously to encrypt the plain-image pixels. To determine rule number in DNA sequence and also CA, a tow-dimension logistic map is employed. Through the experiment result and security analysis, we find that our algorithm has good encryption effect, larger secret key space. 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 image encryption.

## REFERENCES

[1] Xing-Yuan Wang, Ying-Qian Zhang, Xue-Mei Bao. “A novel chaotic image encryption scheme using DNA sequence operations”, Optics and Lasers in Engineering 73 (2015) 53–61

[2] S.G. Lian, A block cipher based on chaotic neural networks, Neurocomputing 72 (2009) 1296−C1301.

[3] Z.H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, Phys. Lett. A 346 (2005) 153−157.

[4] N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map, Image Vis. Comput. 24 (9) (2006) 926−934.

[5] S.G. Lian, Efficient image or video encryption based on spatiotemporal chaos system, Int. J. Chaos Solitons Fractals (Elsevier) 40 (15) (2009) 2509−2510.

[6] C. Fu, Z.L. Zhu, A chaotic image encryption scheme based on circular bit shift method, in: The 9th International Conference for Young Computer Scientists, 2008, pp. 3057−3061.

[7] Wolfram S. Cryptography with cellular automata. In: Proceedings of the CRYPTO 85 advances in cryptography, vol. 218; 1985. pp. 429e32.

[8] A.A. Abdo, Shiguo Lian, I.A. Ismail, M. Amin, H. Diab. “A cryptosystem based on elementary cellular automata”, Commun Nonlinear Sci Numer Simulat 18 (2013) 136–147

[9] Jun Jin “An image encryption based on elementary cellular automata”, Optics and Lasers in Engineering 50 (2012) 1836–1843

[10] G.Z. Xiao, M.X. Lu, L. Qin, X.J. Lai, New field of cryptography: DNA cryptography,Chin. Sci. Bull. 51 (12) (2006) 14131420.

[11] Adleman, Molecular computation of solutions of combinatiorial problems, Science 266 (1994) 1021_1024.

[12] H. Liu, X. Wang, A. kadir, Image encryption using DNA complementary rule and chaotic maps, Appl. Soft Comput. 12 (5) (2012) 1457–1466.

[13] M. Shyam, N. Kiran, V. Maheswaran, A novel encryption scheme based on DNAcomputing, in: HIPC2007, 2007.

[14] Zhang Q, Guo L, Wei X. “A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system”. Optik—Int J Light Electron Opt 2013;124:3596–600.

[15] Seyed Morteza Hosseini, Hossein Karimi, Majid Vafaei Jahan, Generating pseudo-random numbers by combining two systems with complex behaviors, journal of information security and applications 19 (2014) 149e162.

[16] Wolfram S. Statistical mechanics of cellular automata. Rev Mod Phys 1983;55:60144.

[17] Franciszek Seredynski, Pascal Bouvry, Albert Y. Zomaya, “Cellular automata computations and secret key cryptography”, Parallel Computing 30 (2004) 753–766.

[18] A.A. Abdo, Shiguo Lian, I.A. Ismail, M. Amin, H. Diab, A cryptosystem based on elementary cellular automata, Commun Nonlinear Sci Numer Simulat 18 (2013) 136–147.

[19] Ping Ping, Feng Xu, Zhi-Jian Wang, Image encryption based on non-affine and balanced cellular automata, Signal Processing 105 (2014) 419–429

[20] Kokolakis I, Andreadis I, Tsalids P. Comparison between cellular automata and linear feedback shift registers based pseudorandom number generators. Microprocessors and Microsystems 1997;20:643e58.

[21] Nandi S, Kar BK, Chowdhuri PP. Theory and applications of cellular automata in cryptography. IEEE Trans Comput 1994;43:1346e57.

[22] J.D. Watson, F.H.C. Crick, A structure for deoxyribose nucleic acid, Nature 171(4356) (1953) 737−738.

[23] P. Gaborit, O.D. King, Linear constructions for DNA codes, Theor. Comput. Sci.334 (2005) 99−113.

[24] O.D. King, P. Gaborit, Binary templates for comma-free DNA codes, Discrete Appl. Math. 155 (2007) 831−839.

[25] R Enayatifar, S Faridnia, HH Sadeghi. Using the chaotic map in image steganography. International Conference on Signal Processing Systems; 2009.

[26] Rasul Enayatifar, Abdul Hanan Abdullah, Ismail Fauzi Isnin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence”, Optics and Lasers in Engineering 56 (2014) 83–93

[27] X.Y. Wang, and Q. J Shi, “New Type Crisis, Hysteresisand Fractal in Coupled Logistic Map.” Chinese Journal of Applied Mechanics, pp. 501-506, 2005

[28] Seredynski F, Bouvry P, Zomaya AY. “Cellular automata computations and secret key cryptography”. Parallel Comput 2004;30:753e66.

[29] C.E. Shannon, Communication theory of security systems, Bell Syst. Tech. J. 28 (1949) 656715.