International Journal of Security and Its Applications
Vol.9, No.9 (2015), pp.285-294
http://dx.doi.org/10.14257/ijsia.2015.9.9.25

# A Kind of Encryption Method of QR Code based on ECA State Ring

Yu Guang, Shi Yunbo* and Che Chang

*Measuring and Control Technology and Instrumentations*
*Harbin University of Science and Technology,*
*Harbin, China*
*yuguang@hrbust.edu.cn*

***Abstract***

*In view of the simple keys, time-consuming in encryption and decryption process and the loss of original function characteristics in encrypted image QR two-dimensional code, we adobe a kind of encryption method of QR code based on ECA state ring. In this method, the simple structure, highly parallel of elementary cellular automaton is being used. Operating each pixel point on the quick response code except which can express QR code function information. The simulation results show that the method is faster than two kinds of typical QR code encryption method, and the encrypted image can preserve the original QR code function information, while the safety coefficient is very similar.*

***Keywords***: *RCA state ring; QR code; Encryption; Decryption*

## 1. Introduction

With the emergence of information and the rapid popularization of network technology, the hitherto unknown change has occur in people's daily life, work and learning. Information has become an important strategic resource of modern social development. People attach great importance in information security and information hiding technology. Bar code technology is a new technology which gather coding, identification, data acquisition, processing and printing [1]. Two dimensional code is a bar code which is high reliability, larger information capacity, strong confidential security and a variety of error level. QR code not only has the common advantages of two-dimensional code, but also has 360 degrees of fast reading and express Chinese. With these advantages, the two dimensional code is used widely in many fields such as traffic, printing, medical, financial and mobile communications. One concern is that the train ticket real name of China Railway Customer Service Center makes good use of the advantages of QR codes in recent years. It can deposit the user identity and the information such as number into the QR code. Besides that, concert tickets and part of the Aerospace Corp's boarding passes used QR codes. But the application of the convenient goes with the disclosure of information [2]. In the related report, people use QR decoding software commonly used can read the user ticket, identity and information in trains. This report aroused the concern of the safety performance of QR codes. The law enforcement staff use special software to read on the QR code, complete the related enforcement operations, which can master the government area enterprise compliance with industrial and commercial regulations. The two-dimensional code security and confidentiality need extra attention, in case that the important information was leaked.

This paper design an encryption method with high safety and real-time, which learn from the information encryption method, the digital image encryption theory and cellular automaton. This method can keep the original advantages of QR codes.

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

## 2. The Based Theory of Cellular Automaton

The cellular automaton is a dynamics system which changes in discontinuous time dimension. Specifically, the cellular automaton consists of four main parts [3]. It is cellular space, state, neighborhood and rules. Marked that $A=(L_d, S, N, f)$.Among them:

$A$ express cellular automaton;

$L_d$ express cellular space, $d$ express spatial dimension in it;

$S$ express finite discrete state set of cellular automaton, $S=\{S_0, S_1, \cdots, S_{k-1}\}$, $k$ express the number of state;

$N$ express neighborhood vector, it is constituted by $m$ different vectors in $Z^d$ ,which is $N=(v_1, v_2, \cdots v_m)$, $f$ express local transfer function, which is mapped to $S$ *from* $S^m$.

The change rules of cellular automaton is the equation or function which the cellular automaton evolution process follows. This rule determines each cellular next evolution time state of cellular automaton system. To a specific cellular automaton, when the change rule is determined, its initial conditions will determine. The evolution path of cellular automaton system is determined too.

The local transform function of one-dimensional cellular automaton can be expressed as:

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

$S_i^t$ is expressed the cellular state of moment $t$ in $i$. $r$ express the neighbor radius.

"State ring" is the main part of state transition diagram. Because of the hidden security problems of QR two-dimensional code information storage, we design an encryption and decryption method of QR two-dimensional code based on the elementary cellular automaton loop state [4]. The method used the characteristics of ECA state ring. The length is 8, and the boundary condition is cyclic boundary condition. The state space of ECA is $\{0,1\}$, which can encrypt or decry the non QR code feature pixel of QR two dimensional code in two value image. It is fast encryption speed, good effect and high security.

## 3. Algorithm Design

The QR encryption algorithm based on the state ring of ECA in which encryption and decryption use the same key. So the key is as follows: $rule$ is expressed the rules of ECA, $seed$ is expressed the seed of the random number generator. The pseudo random integer column $T$ is expressed the length of the random number seed.

### 3.1 The Encryption Process Description

The encryption principle block diagram shown in figure 1.The specific encryption process is described as follows:

Step 1: The two value image of QR two-dimensional code is as the plain image. The gray value matrix of two value image convert into one-dimensional array form by columns. The gray value of each successive pixel is as a group. The gray value in each group is expressed as $group(n)$ .The size $N \times N$ QR two-dimensional code which is divided into $(N \times N) \div 8$ groups.

Step 2: According to the structure characteristics of two value image about QR two-dimensional code, we set the symmetric key. The encryption size $N \times N$ two value image of QR code includes: $rule$ is expressed the rules of ECA, $seed$ is expressed the seed of the random number generator [5].The random integer column $T$ is expressed the length of the random number seed. The $N \times N$ size QR two-dimensional code, of which seed is shown as:

 Copyright ⓒ 2015 SERSC

$$seed = N \times N / 8 \tag{2}$$

The pseudo-random integer column is:

$$T = \{t(n) | t(n) \in [1,7]\}, 1 \le n \le seed \tag{3}$$

In the above formula, $t(n)$ express the encryption number of $group(n)$ gray value in the plain image. $8 - t(n)$ is decryption times.

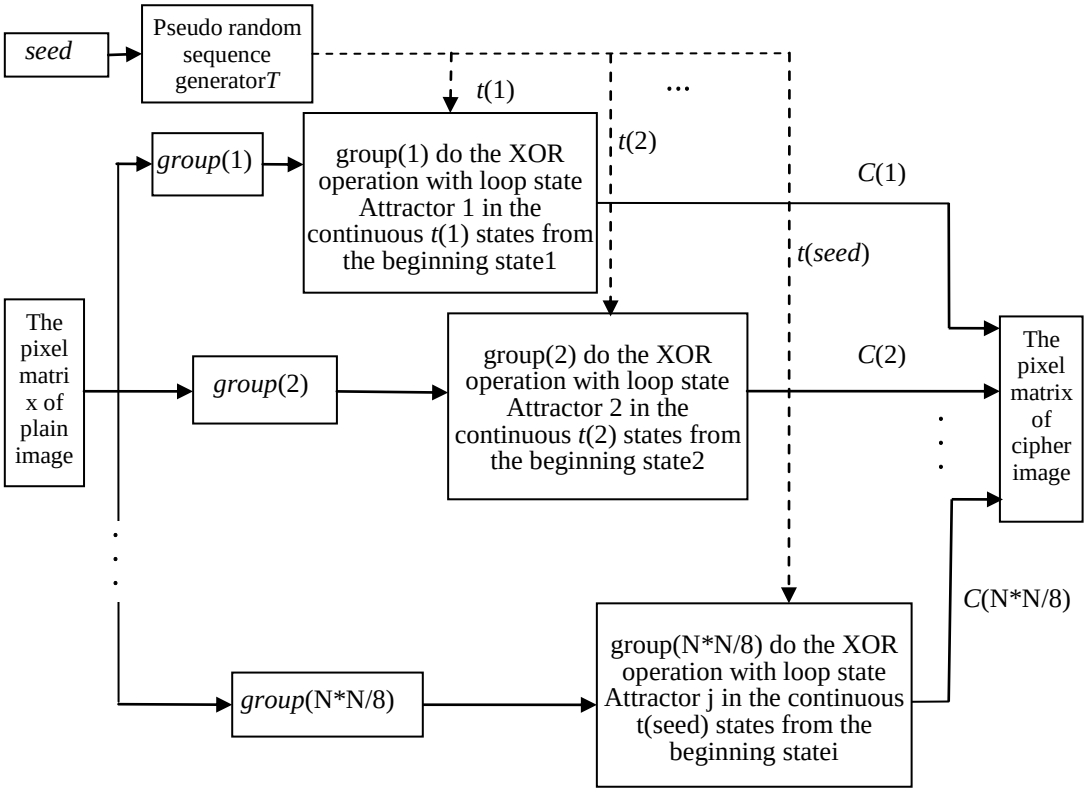



**Figure 1. Schematic Diagram of Encryption Algorithm**

Step 3: In the specified rules, $state(1)$ express each state ring value of state transition diagram about elementary cellular automaton. $group(n)$ express each gray value in QR code plaintext image. $Attractor\ \ j$ express QR code encryption state ring in $rule$ .Determining the initial state $state(i)$ .Of which $i$ , $j$ is shown as:

$$i = \begin{cases} \mathrm{mod}(n,k), n \ne 8 \\ 8, n = 8m \end{cases} \tag{4}$$

$$j = \mathrm{mod}(n,l) \tag{5}$$

In that, $l$ express the number of state ring. $k$ express the states number of a loop state $Attractor$ .

Step 4: Doing the bitwise XOR operation continuously. $Attractor\ \ j$ express the state in each bitwise XOR loop state. The $t(n)$ states is continuous in loop state.

$$C(n) = group(n) \oplus state(i) \oplus \cdots \oplus state(i + t(n) - 1) \tag{6}$$

In that, $state(i)$ express the encryption initial state in $rule$ . $C(n)$ express the $n$ group gray value of ciphertext which is encrypted by QR code two value image.

Step 5: After all data processing, inserting the pixel location of QR two-dimensional code which can express functional information in the appropriate place. The $(N \times N) \div 8$

groups $C(n)$ data is being restructured to $N \times N$ pixel gray matrix of two value image. It can generate the cipher image of QR two-dimensional code, and the encryption is completed.

### 3.2 The Decryption Process Description

Decryption is the inverse of the encryption process. Schematic diagram of the decryption process as is shown in figure 2.The decryption process is described below:

Step 1: In the specified rules, $state(1)$ express the numerical minimum state in each state ring which is in the state transition diagram of elementary cellular automaton. The gray value matrix of cipher image is converted into a one-dimensional array form by column. After removing the pixel which can represent the function information in QR two-dimensional code, every 8 consecutive pixel values in gray matrix of cipher image are lumped together. All are divided into $(N \times N) \div 8$ groups. $C'(n)$ express each gray value $C'(n)$ .In $rule$ , $Attractor\ \ j'$ express decryption state ring, and $state(i')$ express the initial state ring. Of which $i$ , $j$ is shown as:

$$i' = \begin{cases} \mathrm{mod}(\mathrm{mod}(n,k)+t(n),k), \mathrm{mod}(n,k)+\mathrm{t}(n) \neq 8m \\ 8, \mathrm{mod}(n,k)+t(n)=8m \end{cases} \tag{7}$$

$$j' = \mathrm{mod}(n,\mathrm{l}) \tag{8}$$

In that, $k$ express the number of state in loop state $Attractor\ \ j'$ ; $l$ express the number of state ring in $rule$ .

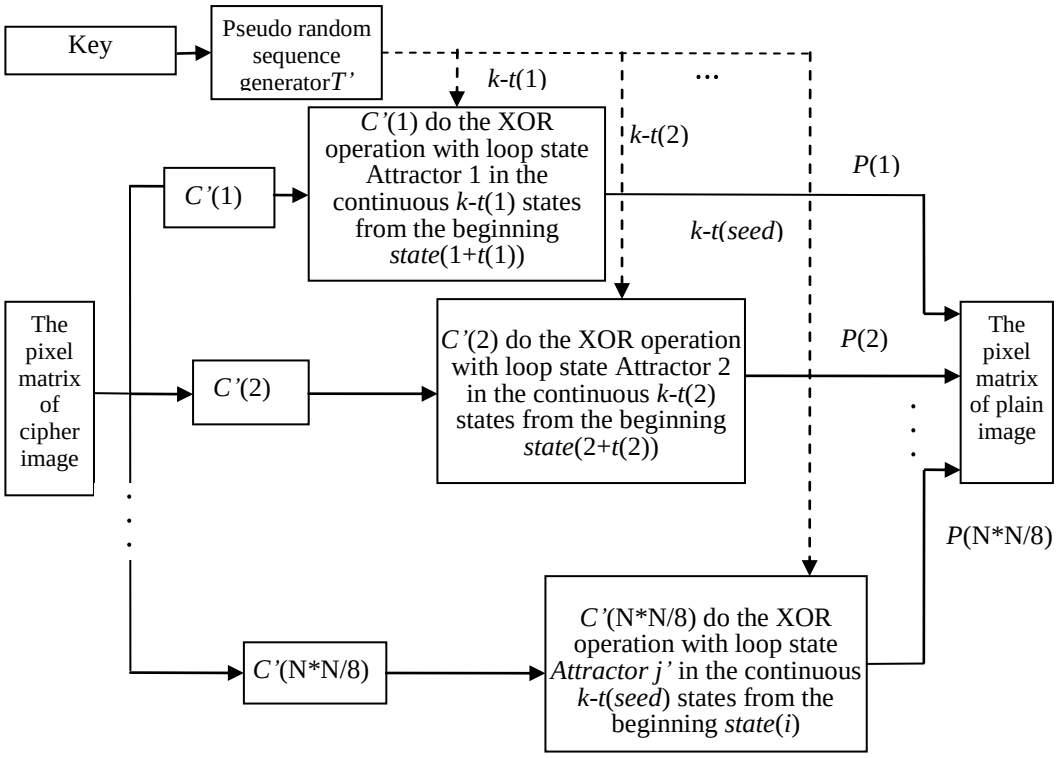



**Figure 2. Schematic Diagram of Decryption Algorithm**

Step 2: According to the received random number $seed$ of the key and random matrix $T$ .We get the decryption random number matrix $T'$ .The elements in the $T'$ is $k - t(n)$ ,which express decryption times.

 Copyright ⓒ 2015 SERSC

Step 3: Each gray value of cipher image in QR code do the $XOR$ arithmetic for $k-t(n)$ times continuously. To be specific, every $C'(n)$ must do the bit by bit $XOR$ arithmetic with the consecutive $k-t(n)$ state in the ECA loop state $Attractor\ \ j'$.The mathematical description of specific decryption is:

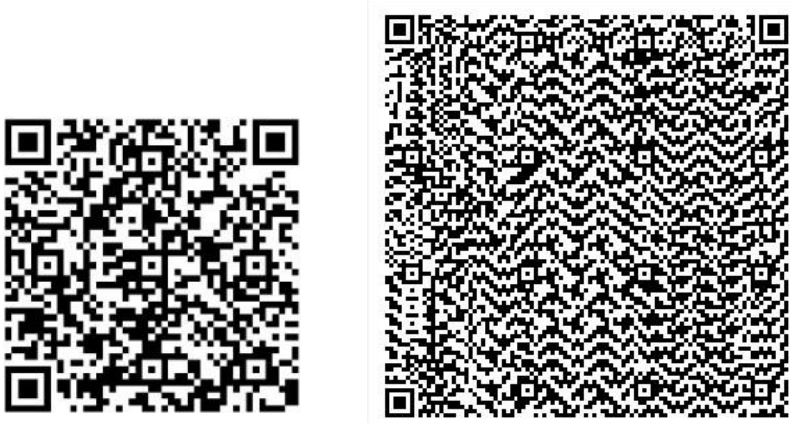
$$P(n)=C'(n)\oplus state(i')\oplus\cdots\oplus state(i'+k-t(n)-1) \tag{9}$$

In the $rule$, $state(i')$ express the beginning state of decryption in $Attractor\ \ j'$ ring. $P(n)$ express the $n$ group gray value which is being decrypted.

Step 4: After all data are being processed, Inserting the pixel which can show the functional information about QR two-dimensional code in the corresponding position. Regrouping the $(N\times N)\div 8$ groups $C(n)$ data into $N\times N$ pixel gray matrix about two value image. It can generate the plain image of QR two-dimensional code, and the decryption is complete.

## 4. Simulation and Analysis

Using versions 7 and versions 20 QR two-dimensional code as the experimental image, which is as shown in figure 3.The length of the cyclic boundary condition is 8.The ECA state loop algorithm of which state space is $\{0,1\}$ and the key is $(53,42,T_{42})$,with DES algorithm and chaotic sequence algorithm encrypt to the original QR two-dimensional code as is shown in figure 3.The cipher image which is obtained by three kinks of encryption method from the QR code two value image of two version, as is shown in figure 4.4(a) is the cipher image which the QR code of version 7 is encrypted by ECA state ring. 4(b) is the cipher image which the QR code of version 7 is encrypted by DES state ring.4(c) is the cipher image which the QR code of version 7 is encrypted by chaotic sequence algorithm state ring.4(d) is the cipher image which the QR code of version 20 is encrypted by ECA state ring.4(e) is the cipher image which the QR code of version 20 is encrypted by DES state ring.4(f) is the cipher image which the QR code of version 20 is encrypted by chaotic sequence algorithm state ring.



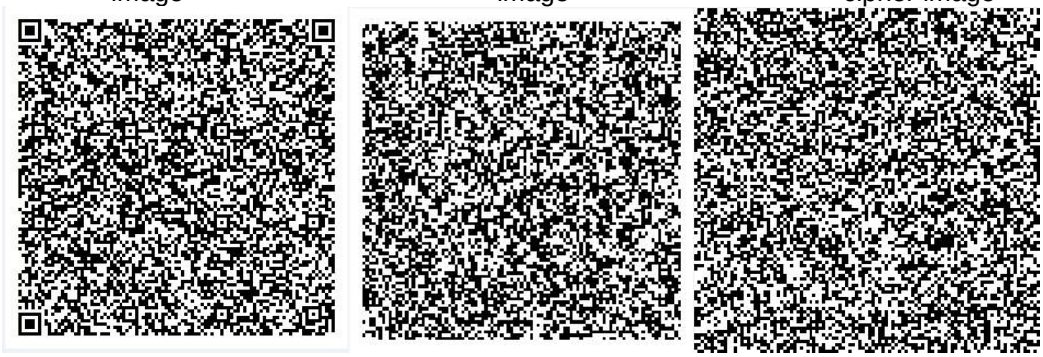
a) The standard QR code of version 7 b) The standard QR code of version 20

**Figure 3. Original QR Code of Version 7 and 20**

From figure 4, only encryption method of ECA loop state can keep the original function information of QR code. The functional characteristics of QR two-dimensional code would be destroyed by encryption in DES algorithm and chaotic sequence algorithm. But it cannot distinguish the good and bad of security encryption and the encryption speed from picture effect. Based on this, analyzing the encryption effect from key sensitivity, correlation of adjacent pixels, gray value scrambling degree, key space and decryption time.

Copyright ⓒ 2015 SERSC

a) ECA state ring cipher image | b) DES algorithm cipher image | c) Logistic algorithm cipher image



d) ECA state ring cipher image | e) DES algorithm cipher image | f) Logistic algorithm cipher image

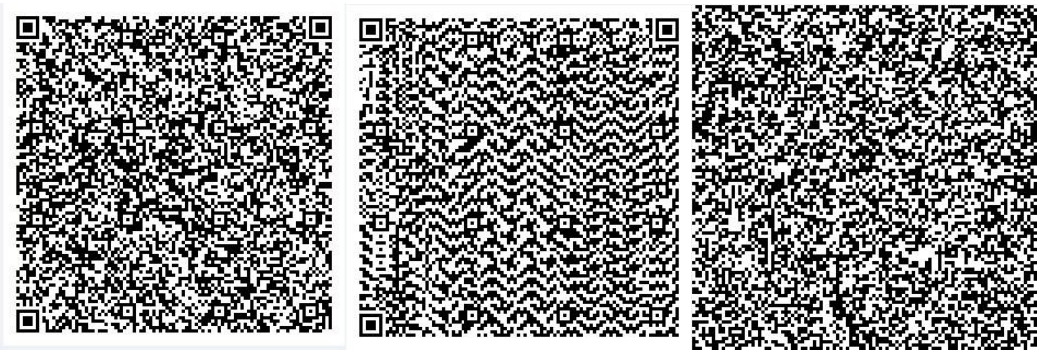
**Figure 4. Comparison of the Three Kinds of Encryption Algorithm**

### 4.1 Key Sensitivity

The cipher image which is encrypted by ECA state ring algorithm in the two value image of version 7 QR two-dimensional code as is shown in figure 5(a).The correct decryption image of this algorithm as is shown in figure 5(b).When the first binary number of $state(1)$ is reversed, the QR two-dimensional code image would deviate tiny in the key. The decryption image is obtained which is shown in figure 5(c).The cipher image which is encrypted by ECA state ring algorithm in the two value image of version 20 QR two-dimensional code as is shown in figure 5(d).The correct decryption image of this algorithm as is shown in figure 5(e).When the first binary number of $state(1)$ is reversed, the QR two-dimensional code image would deviate tiny in the key. The decryption image is obtained which is shown in figure 5(f).

a) ECA state ring cipher image | b) The correct decryption key | c) The error decryption key

 Copyright ⓒ 2015 SERSC



d) ECA state ring cipher image | e) The correct decryption key | f) The error decryption key

**Figure 5. Analysis Figure of Key Sensitivity**

As is shown in figure 5, when the key deviates little, it cannot obtain the correct decryption image by using the encryption method of ECA state ring. The density map is highly sensitive to the key.

### 4.2 The Correlation of Adjacent Pixels

There are only two values in gray value of two value image. The correlation between adjacent pixels is hard to display in the histogram [6]. Therefore, the correlation coefficient of adjacent pixels can be calculated by the following formula:

$$\gamma_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{10}$$

$x$ and $y$ in the above formula express the gray value of adjacent pixels in the image. $\operatorname{cov}(x, y)$ is the covariance of $x$ and $y$ . $D(x)$ and $D(y)$ express the standard deviation of $x$ and $y$ .

In order to test the correlation between the original of ECA state ring encryption algorithm and adjacent pixels of density map, extracting 10 groups of adjacent pixels in cipher image of version 7 QR two-dimensional code randomly. Each group is 100 (horizontal, vertical or diagonal direction).Similarly, extracting 10 groups of adjacent pixels in cipher image of version 20 QR two-dimensional code. Each group is 1000 (horizontal, vertical or diagonal direction).Averaging the 10 groups data of version 7 QR two-dimensional code and of version 20 QR two-dimensional code according to the direction. It can get the correlation coefficient of adjacent pixels in horizontal, vertical and diagonal directions. The correlation coefficient which is calculated by three direction is as shown in table 1.

**Table 1. Adjacent Pixels Correlation Coefficient of Original and Cipher Images**

| Direction | Version 7 QR code | | Version 20 QR code | |
|---|---|---|---|---|
| | Original image | Cipher image | Original image | Cipher image |
| Horizontal correlation | 0.2015 | 0.0759 | 0.1966 | 0.0585 |
| Vertical correlation | 0.2034 | 0.0943 | 0.2062 | 0.0739 |
| Diagonal correlation | 0.1982 | 0.0379 | 0.1985 | 0.0531 |

### 4.3 The Scrambling Degree of Adjacent Pixel Difference

The gray difference calculation formula of a pixel and its neighboring pixels in image is as shown in formula (11).There are only two pixel values of 0 or 1 in two value image,

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

therefore using the form of absolute value to calculate the gray level difference. $G(x,y)$ express the pixel gray value of coordinate $(x,y)$ . $GD$ express the Gray Distance[7].The gray scale average distance between a coordinate gray value and adjacent four coordinate in the image is shown as:

$$GD(x,y)=\frac{\sum_{i,j}|G(x_i,y_j)-G(x'_i,y'_j)|}{4} \tag{11}$$

Calculating the pixel difference between the other coordinate points and adjacent coordinate except for the blank area around. Adding up and taking the average value, it can get the average adjacent pixel difference $E(GD(x,y))$ in the QR code image:

$$E(GD(x,y))=\frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1}GD(x,y)}{(M-2)\times(N-2)} \tag{12}$$

And the scrambling degree of adjacent pixel difference is defined as:

$$GDD(I,I')=\frac{E'(GD(x,y))-E(GD(x,y))}{E'(GD(x,y))+E(GD(x,y))} \tag{13}$$

Parameter $E$ and $E'$ express the average adjacent pixel difference before and after encryption respectively above the formula. $GDD$ is $(-1,1)$ .If $GDD<0$ ,the scrambling degree of original image is better. The odds of that happening is low. If $GDD>0$ ,he scrambling degree of ciphertext image is better. $GDD$ is more close to 1 and more better. Using $GDD$ to measure the encryption algorithm which can reflect the encryption effect of two value image well.

In order to test the adjacent pixel scrambling degree of ECA state ring encryption algorithm, calculating the original image and encrypted image according to the formula (11)、(12) and (13) which is in three kinds of encryption method of version 7 and version 20 QR two-dimensional code. The results are shown in table 2.

**Table 2. Scrambling Degree Evaluation of a Variety of Encryption Schemes**

| Parameters | Version 7 QR code | | | Version 20 QR code | | |
|---|---|---|---|---|---|---|
| | DES encryption | Chaotic encryption | Cellular automata encryption | DES encryption | Chaotic encryption | Cellular automata encryption |
| *E(GD(x,y))* | 0.0047 | 0.0047 | 0.0047 | 0.0014 | 0.0014 | 0.0014 |
| *E'(GD(x,y))* | 0.4247 | 0.4515 | 0.4532 | 0.4527 | 0.4538 | 0.4550 |
| *GDD* | 0.7999 | 0.8809 | 0.8806 | 0.8013 | 0.8903 | 0.9045 |

$E(GD(x,y))$ is the average adjacent pixel difference of original QR code image. This value is fluctuation in the vicinity of 0.001 from table 2.There are large gray similar region(all 1 or all 0)in original QR code image. The change of average adjacent pixel difference is smaller.

$E'(GD(x,y))$ is the average adjacent pixel difference of cipher image. The change of $E'(GD(x,y))$ is bigger than $E(GD(x,y))$ from table 2.Data show that the different gray value pixels in the cipher image are scattered out randomly. The change of $E(GD(x,y))$ in cipher image is bigger than which in original QR code image. The randomness is stronger.

$GDD>0.5$ in three kinds of encryption algorithm shows when the scrambling degree of adjacent pixel difference is big, the encryption work would be served well[8].From $GDD$ in three kinds of encryption methods it could find that the $GDD$ of ECA state ring

 Copyright ⓒ 2015 SERSC

encryption algorithm is bigger than which of DES and chaotic sequence algorithm. So the encryption effect of ECA state ring algorithm is better than which of DES and chaotic sequence algorithm.

From the above data, it can get the encryption effect of QR code encryption algorithm base on ECA state ring. The experimental data shows that the algorithm can be executed and the effect is better. This algorithm is easy to realize.

### 4.4 Analysis of Key Space

The key of the above encryption scheme is $(rule, seed, T)$ .There are 256 keys in $rule$ .So there are $256 = 2^8$ kinds of choices. The pseudo random integer column $T$ is in the $seed$ of the random number generator. There are $8 = 2^3$ kinds of choices in each element of $T$ .For a given amount of QR code two value image is quantitative. There are $256 \times (2^3)^{seed} = 2^{8+3seed}$ kinds of choices in the decryption key. If decrypting the pixel gray value of cipher image directly, direct decryption is unable to realize. For version 7 QR code image, the two value image size is $53 \times 53$ and the $seed$ is 352.If being cracked by exhaustive method, the number of the operation is dependent on the random integer column $T$ .There are $2^{8+3\times 352} = 2^{1064}$ kinds of choices in the key. The version 20 QR two-dimensional code image which size is $105 \times 105$ .The $seed$ is 1379.There are $2^{8+3\times 1379} = 2^{4145}$ kinds of choices in the key. The calculations is huge. Therefore, the key space of encryption method based on elementary cellular automaton state ring is large. which can resist the key attack effectively.

### 4.5 The Test of Image Encryption and Decryption Speed

In order to validate the efficiency of ECA state ring encryption method, using Matlab2010 to do the simulation experiment by computer of which memory is 4.0, operating system is 64 bit and the processor is AMDA6, 1.5GHz.Version 7 and version 20 QR code image are the plain image, which are as shown in figure 3(a) and 3(b).Using DES algorithm, chaotic sequence algorithm and ECA state ring algorithm to encryption and decryption. Each method was tested for 20 times. Each method sums and takes the average. Measuring the time of encryption and decryption as is shown in table 3.

**Table 3. Test of the Encryption / Decryption Speed (unit: second)**

| Average time | Version 7 QR code | | | Version 20 QR code | | |
|---|---|---|---|---|---|---|
| | DES algorithm | Chaotic algorithm | ECA state ring algorithm | DES algorithm | Chaotic algorithm | ECA state ring algorithm |
| Encryption | 2.03167 | 0.16177 | 0.05290 | 4.15493 | 0.27694 | 0.16102 |
| Decryption | 2.20967 | 0.15194 | 0.07560 | 3.95456 | 0.26989 | 0.18498 |

Each 64 bit in images Do 16 rounds iterative operation with DES encryption algorithm. The data size is huge. It takes a long time to finish. The sequence generated by chaotic systems is the random sequence in $(0,1)$ .The gray value of QR two-dimensional code image is the two value image of 0 or 1.Each data is being compared with threshold value 0.5.Choosing data 0 or 1 and dealing with it. The original data would do 16 rounds XOR operation in encryption and decryption process. It takes a long time. Therefore, the encryption and decryption efficiency of ECA state ring is relatively high.

## 5. Conclusion

This paper mainly introduces the definition of cellular automata and its basic part. Introducing the concept of elementary cellular automata and state ring. The paper use the improved encryption method of QR two-dimensional code based on ECA state ring.

Copyright ⓒ 2015 SERSC

Describing the design principle of the algorithm together with encryption and decryption algorithm in detail. Doing the simulation experiment based on the ECA state ring encryption method. The experimental results show that the encryption speed of this method reaches 0.1 second, which is easy to realize, large space in the key, high safety. The encryption and decryption speed are faster than existing methods. It can meet the QR code information confidentiality requirements in common applications.

## Acknowledgements

This paper is supported by Natural Science Foundation of Heilongjiang Province of China (ZD201217977)

## References

[1] H. Wang, "Research on Registration Method of Point Cloud Data and Key Technology in Vision Measurement [D]", Journal of Harbin University of Science and Technology, **(2011)**.
[2] Z H. Zhang, "Review of single-shot 3D shape measurement by phase calculation-based fringe projection techniques [J]", Optics and Lasers in Engineering, vol. 50, no. 8, **(2012),** pp. 1097-1106.
[3] G. Chazan and N. Kiryati, "Pyramidal intensity-ratio depth sensor [R]", Technical Report, Center for Communication and Information Technologies, Department of Electrical Engineering, Technique, Haifa, Israel, **(1995).**
[4] H. Masuda and K. Fukuda, "Ordered metal nanohole arrays made by a two-step replication of honeycomb structures of anodic alumina [J]", Science, vol. 268, no, 5216, **(1995)**, pp. 1466-1468.
[5] T. Pribanic, H. Dapo and J. Salvi, "Efficient and low-cost 3D structured light system based on a modified number-theoretic approach [J]", EURASIP J Adv Sign Proc, **(2010),** pp. 1-11.
[6] B. Amberg, S. Romdhani and T. Vetter, "Optimal step nonrigid icp algorithms for surface registration [C]", Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on. IEEE, **(2007)**, 1-8.
[7] J A C. Yule, "Principles of color reproduction, applied to photomechanical reproduction, color photography, and the ink, paper, and other related Industries [M]", New York: Wiley, **(1967)**.
[8] T. Pouli, A. Artusi and F. Banterle, "Color Correction for Tone Reproduction [C]", Color and Imaging Conference. Society for Imaging Science and Technology, vol. 1, **(2013)**, pp. 215-220.

 Copyright ⓒ 2015 SERSC