International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.397-406
http://dx.doi.org/10.14257/ijsia.2013.7.5.36

An Encryption Method for QR Code Image Based on ECA

Yu Xiaoyang, Song Yang, Yu Yang, Yu Shuchun, Cheng Hao and Guan Yanxia

The higher educational key laboratory for Measuring & Control Technology and Instrumentations of Heilongjiang province
Harbin University of Science and Technology, Harbin, China
Songyang880503@163.com

Abstract

In order to improve security performance of the information stored in two-dimensional Code (Quick Response Code), a two-dimensional code encryption and decryption method based on Elementary Cellular Automata state rings is proposed in this paper. Cellular Automata can simulate complex phenomenon just using simple dynamical system. In addition, Cellular Automata and cryptography have a lot of similarities such as diffusivity and integrated chaos. Based on this feature, the method uses the Cellular Automata to encrypt and decrypt QR code binary image with the following parameters: the length is 8, the boundary condition is cyclic boundary condition and {0, 1} is the state space. The experimental results show that the method proposed in this paper has some advantages, such as high speed, good effect and high security.

Keywords: *QR code; Elementary Cellular Automata; image encryption; state rings*

1. Introduction

Information has become an important strategic resource of social development at present. People have attached great importance to information security and information hiding technology. Barcode technology is an emerging technology including coding, printing, data acquisition and processing. Two-dimensional code such as QR (Quick Response) code is widely used in Europe, America and other developed countries because of its large capacity of information, high reliability, supporting for multiple error level and confidential security. People can use two-dimensional code to encode the information of words, graphics, images and the others which can be digital. It has broad application prospects in many industries and fields in our country [1, 2]. Two-dimensional code as a kind of effective mode of carrying and transmission information has certain security function. But it can't meet the people's higher confidentiality requirements in the various communication network transmissions. How to carry on the development and application of encryption is still an urgent problem to solve and to explore [3]. There are two methods to encrypt the QR code: based on the DES algorithm and the Logistic Chaos algorithm [4].

In the QR code encryption method based on the DES algorithm, the DES encryption algorithm is used to encrypt the pepper-and-salt region of the QR code image in 64 bits. Then, the unencrypted dates of the white region around the QR are combined with encrypted data of the pepper-and-salt region in the middle of the QR. The data are written in binary digital image format, and then, they are stored as image file. It is the encrypted QR code image [5].

In the QR code encryption method based on the Logistic Chaos algorithm, the initial value and the parameter values which meet the requirements of the generating chaotic sequence is chosen at random. Then a size of $N * N$ Logistic binary Chaos sequence is generated. Then,

ISSN: 1738-9976 IJSIA

the XOR operation on the pixels of the QR code image is conducted and the data are written in the BMP image file for storage and transmission [6].

The key of both the DES encryption algorithm and the Logistic Chaos encryption algorithm are simple. It is hard to avoid information leakage caused by human factors. Besides, 16 times iterative operations are done on every 64 bits of the image in the DES encryption algorithm. So the amount of the data is large and this algorithm is time-consuming. Similarly, the Logistic Chaos encryption algorithm generates random sequence which range is from 0 to 1. But the binary image only has two states, 0 or 1. So it needs to compare every data with the threshold value. It also costs some times. That is to say, the two methods can't give consideration to both speed and safety.

According to the characteristics of QR code image and digital image, as well as the principle of digital image encryption and the dynamics system of Cellular Automata, an effective QR code encryption method which can ensure the high speed and high security is designed in this paper.

2. Cellular Automata Encryption Technology

2.1. The Relationship of Cellular Automata to Cryptography

Wolfram first proposed Cellular Automata encryption technology in 1986. Many researchers have done in-depth study of the cryptography features of Cellular Automata in the following years. Cellular Automata and cryptography have a lot of similarities because of the simplicity of inherent component unit of cellular space in cell automata, partial characteristics among the cells in the cellular space, the highly parallelism of the information processing in Cellular Automata and the complex global characteristics of the cellular evolution behavior. The cryptography features are shown in the Table 1.

Table1. The Relationship of Cellular Automata and Cryptography

	Cellular Automata	Cryptography
Similarity	Sensitive to initial conditions and transformation rules	Diffusion, by mixing up statistical relationship of plaintext
	Completely random, Chaos and confusion complex behavior	Pseudo random sequence
	Partial rules between the cells and complex global feature spread the chaos and random feature to the whole cellular space.	The cryptography algorithm have the desired diffusion and confusion through encryption round
	The partial transformation rules	The encryption key of the encryption algorithm
	The phase space: limited state set (integer)	The phase space: limited integer set

How to combine the cryptography features of Cellular Automata with classical theory of cryptography to create cryptographic algorithms with high efficiency and high security which can meet the modern information security transmission requirements becomes a hot spot of the current research. Especially in the multimedia information hiding and encrypting area, the cryptology characteristic advantage over Cellular Automata is gradually revealed step by step. The unique feature of Cellular Automata provides a new theoretical basis for modern cryptography. At the same time, it provides methods of the cryptography in image, video and other multimedia fields. The independence among cellular units determines the high

parallelism of the Cellular Automata information processing. It provides more favorable conditions for some encryption algorithm which require high algorithm performance [7].

2.2. Elementary Cellular Automata

Elementary Cellular Automata is one of the simplest cellular automatons. It is composed of cellular linear array and its neighbor radius is 1. The state of every cell can only be 0 or 1. That is to say the state space is $\{0,1\}$. S_i^t is the state of the i^{th} cells at the time of t. The partial transition function is a Boolean function. It can be described as Formula (1):

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

Wolfram has defined the rule of the Elementary Cellular Automata. At present the study of elementary Cellular Automata has been in-depth step by step.

The state ring is a part of the state transition diagram. An Elementary Cellular Automata with length of 8 has 256 different global states, which respectively are 0 to 255. The study of Elementary Cellular Automata can be realized by means of studying the state evolved by the Cellular Automata under corresponding rule. Each state ring contains 2, 4 or 8 states. The rest states which are not included in the Cellular Automata diagram evolve according to the last state on the state ring and along the ring. In these state rings, some state ring (such as 2, 3, 4, 11, 13, 14 and 16) possesses the following properties as Formula (2):

$$d \oplus state(1) \oplus state(2) \oplus \cdots \oplus state(k) = d \tag{2}$$

Symbol $\oplus$ represents the XOR operation. $state(i), 1 \le i \le k$ represents k states in the ring and d is an 8 bit binary data. XOR operation can start from any state, that is to say, $state(1)$ can be any state on the ring. The properties of state ring are the basic of the following encryption method. To get the encryption information, the method uses the t states of the ring to do XOR operation t times with the information d which is to be encrypted. Then, to get the original information, use the rest $k-t$ states of the ring which is obtained last step to do XOR operation $k-t$ times with the information encrypted. The rule 42 can be used for images encryption [8]. In addition, the phenomenon exits in other rules of Elementary Cellular Automata, such as 56, 112, 120 and 112.

3. QR Code Encryption based on ECA

In the size of $N*N$ QR codes binary image, the pixel's gray value is only 0 or 1. Therefore, the ECA state is used as the Cellular Automata in the method. Its length is 8 and the cyclic boundary condition is used as the boundary condition [9].

3.1. Settings of Key

The image encryption mode is the symmetric encryption mode, so the sender and the receiver use the same encryption key and decryption key. The key concludes three parts: the initial state of the state ring $state(1)$, the rules of ECA $rule$, and the seed of the random number generator $seed$. The paper uses the size of 256*256 QR code binary image to do the simulation experiment. The key is (53, 42, 8192). 53 represents the Elementary Cellular Automata's state in state ring 16 to the rule 42 [8]. The random number generator $seed$ is $seed = N*N/8 = 8192$.

3.2. Encryption Process

Firstly, the grey value matrix of plain image is converted into a one-dimensional array in the form of rows. Then the gray values of 8 consecutive pixels are divided into a group. For example, the size of $N * N$ QR codes binary image will be divided into $N * N / 8$ groups. From the random number $seed$, a length of $seed$ pseudorandom integer array T is got. T should satisfy the Formula (3):

$$T = \{t(n) \mid t(n) \in [1, k-1], 1 \le n \le seed\} \tag{3}$$

Among them, $t(n)$ represents the number of encrypt time of the n^{th} group's gray value in QR code binary image. Similarly, $k - t(n)$ represents the number of deciphering time. The size of 256*256 QR code binary image is used to do the simulation experiment, so N equals 256, k equals 8, and $seed$ equals 8192.

Second, each group of gray value is used as a unit to encrypt the QR code binary image. Each group of gray value is expressed as $pixel(n)$. XOR operation is conducted $t(n)$ times consecutively and each time the state of the state ring do the XOR operation bit by bit. These $t(n)$ states are consecutive on the state ring as Formula (4):

$$C(n) = pixel(n) \oplus state(i) \oplus \cdots \oplus state(i + t(n)) \tag{4}$$

Among them, $i = \mathrm{mod}(n, k)$, $state(i)$ represents the state at the beginning of encryption. $C(n)$ represents the n^{th} group of gray values of the ciphered-image after encryption. For example, for the eleven group of gray values, $i = \mathrm{mod}(11,8) = 3$, so the three states for the consecutive XOR operation are 212, 169 and 83.

After all data are processed, they are reassembled into binary image of the size of $N * N$.

In the size of $N * N$ QR codes binary image, the pixel's gray value is only 0 or 1. Therefore, the ECA state is used as the Cellular Automata in the method. Its length is 8 and the cyclic boundary condition is used as boundary condition [9].

3.3. Decryption Process

The receiver gets the random matrix T that used by sender according to the random number $seed$ in the key. Then the receiver can use the T to calculate random matrix for decryption. The element of the matrix is $k - t(n)$.

Similarly, the gray values of 8 consecutive pixels in the ciphered-image are divided into a group. There are $N * N / 8$ groups. Consecutive XOR operations are conducted $k - t(n)$ times bit by bit with each group of gray values $C(n)$ in the ciphered-image. Each time XOR operation is conducted with one state on the state ring. These $k - t(n)$ states are continuous. The decryption process can be described as Formula (5):

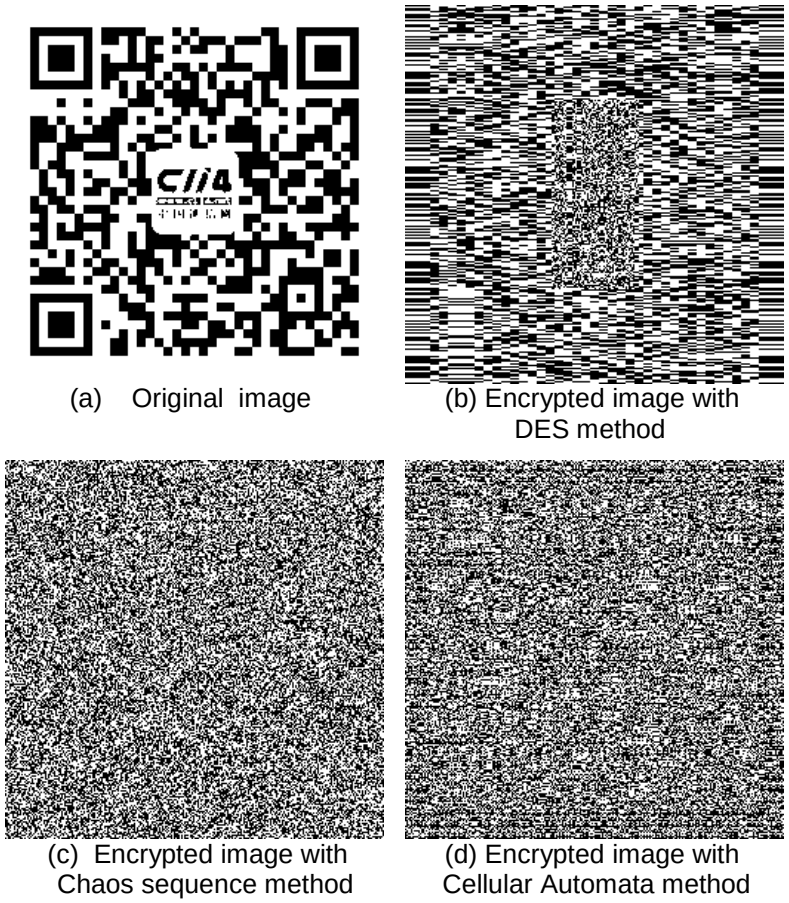
$$P(n) = C(n) \oplus state(i) \oplus \cdots \oplus state(i + k - t(n)) \tag{5}$$

In Formula (5), $i = \mathrm{mod}(\mathrm{mod}(n, k) + t(n), k)$, and $state(i)$ represents the state at the beginning of decryption.

When the data are all processed, they are reassembled into binary image of the size of $N * N$.

4. Experiment and Analysis

A size of 256*256 standard QR code binary image is used as the test image in this paper. Three kinds of methods are used to encrypt the test image, such as the DES, the Chaos sequence and the Cellular Automata method. The Cellular Automata method has the following parameters: the length is 8, the boundary condition is cyclic boundary condition, {0, 1} is the state space and the key is (53, 42, 8192).



(a) Original image (b) Encrypted image with DES method

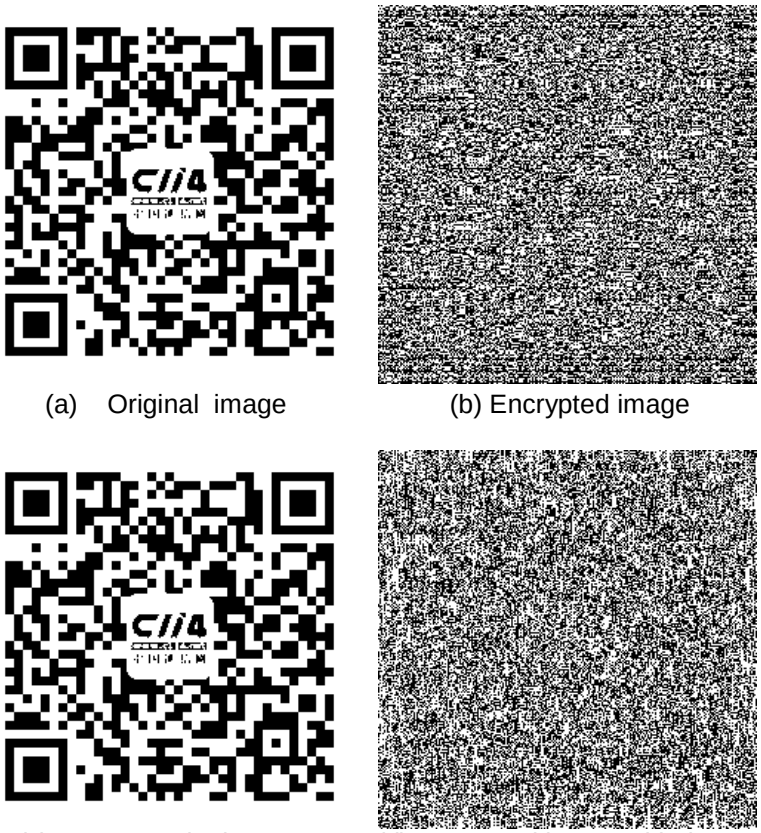
(c) Encrypted image with Chaos sequence method (d) Encrypted image with Cellular Automata method

Figure 1.Original Image and Encrypted Images with Three Kinds of Methods

The original image and the encrypted images with three kinds of methods are shown in Figure 1. The core evaluation criterion of an image encryption system is the security of the image encryption. The analyses of the security of the method are shown in the following aspects.

4.1. Sensitivity of Keys

Figure 2(a) is the original image. Figure 2(b) is the encrypted image with Cell Automata method. Figure 2(c) is the image decrypted correctly. Figure 2(d) is the decrypted image with the small deviation of key. For example, the first bit of *seed* is inversed. It can be seen from the image that the key has a high sensitivity.



(a) Original image (b) Encrypted image

(c) Decrypted image (d) Decrypted image with the small deviation of key

Figure 2. Sensitivity of Keys

4.2. Correlation of Adjacent Pixels

To test the correlation of adjacent pixels in the plain-image and ciphered-image, 1000 pairs of adjacent pixels are extracted randomly from the two images in the horizontal direction, vertical direction and diagonal direction. The formula of adjacent pixels' correlation is mentioned [10].

$$\gamma_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{6}$$

In Formula (6), x and y represent the gray value of the adjacent pixels. $\mathrm{cov}(x, y)$ is the covariance between x and y . $D(x)$ and $D(y)$ are the standard deviations between x and y .

It is difficult to indicate the correlation of adjacent pixels in the image because the grey value of binary image is only 0 and 1.But the correlation coefficients can be calculated by the Formula (6). Table 2 lists the correlation coefficients which calculated in the three directions respectively. It can be seen from the simulation result in Table 2 that the correlation of adjacent pixels is high in original image and the correlation coefficient is close to 1. But the correlation coefficient of adjacent pixels is close to 0 in ciphered-image. So the adjacent pixels are almost irrelevant. It means that statistical features of the original image have been spread into the random graph.

Table2. Correlation of Adjacent Pixels between the Plain-image and the Ciphered-image

Image	Correlation on every direction		
	Horizontal	Vertical	Diagonal
Plain-image	0.8457	0.8488	0.7572
Cipher-image	0.0059	0.0020	0.0044

4.3. The Disorder Degree of the Adjacent Pixels

The gray difference formula of pixel and its adjacent pixel are mentioned [10]. $G(x, y)$ represents the gray value of the (x, y), GD represents the gray difference or the gray distance. That is to say, GD is the average gray difference of the pixel and four adjacent pixels around it. Thus, GD is described in Formula (7):

$$GD(x, y) = \frac{\sum_{i,j} | G(x_i, y_j) - G(x'_i, y'_j) |}{4} \tag{7}$$

In addition to image pixels on the edge of image, the difference of the rest pixels and their neighbors is calculated. Then the mean value is calculated to obtain the average gray difference of adjacent pixels in the whole image. The average gray difference is shown in Formula (8):

$$E(GD(x, y)) = \frac{\sum_{x=2}^{M-1} \sum_{y=2}^{N-1} GD(x, y)}{(M-2) \times (N-2)} \tag{8}$$

Disorder has great influence on the random distribution of pixel values. Therefore, the pixel disorder degree is described in Formula (9):

$$GDD(I, I') = \frac{E'(GD(x, y)) - E(GD(x, y))}{E'(GD(x, y)) + E(GD(x, y))} \tag{9}$$

In Formula (9), GDD represents gray disorder degree. E and E' represent the average gray difference of adjacent pixels before and after encryption respectively. The range of such a definition for GDD is -1 to 1. If GDD is less than 0, it shows that the effect of disorder is worse than the original. Of course, this situation appears unusually. On the contrary, if GDD is greater than 0, it shows that the effect of disorder is better than the original. And GDD should be as close to 1 as possible.

Table 3. Evaluation of Disorder Degree of Three Encryption Method

Encryption Method	Evaluation Parameters		
	E(GD(x, y)	E'(GD(x, y)	GDD
DES	0.0682	0.2099	0.6983
Chaos sequence	0.0682	0.4583	0.7292
Cellular Automata	0.0682	0.5011	0.7604

$E(GD(x,y))$ is the average difference of adjacent pixels in image I when it hasn't been encrypted. Table 3 shows that the value is around 0.1. The result shows that the original image exists widespread smooth area filled with similar pixel (all 1 or all 0). The change of adjacent pixels' average gray difference is small.

$E'(GD(x,y))$ is average value of gray difference of adjacent pixels in image I' which has been encrypted. Table 3 shows that there are great changes between $E'(GD(x,y))$ and $E(GD(x,y))$ .The results show that each pixel of cipher-image tends to be randomly distributed. The difference of average value of gray deviation of adjacent pixels after encryption is large. The average gray difference of adjacent pixels has changed a lot.

The values of $GDD(I,I')$ are greater than 0.5.That is to say, the disorder degree of adjacent pixels is big and encryption plays an important role. $GDD(I,I')$ algorithm can well reflect the encryption effect of the QR code binary image. The GDD of Cellular Automata encryption method is closer to 1 than DES encryption method and Chaos sequence method. Therefore, the effect of Cellular Automata encryption method is best.

Table 3 analyzes their gray disorder degree in qualitative. In a word, the encryption method is feasible and the effect is obvious. The method is simple and reliable. It avoids the limitations of DES encryption method and chaotic sequence encryption method [11]. The method of encryption method can be open.

4.4. Speed Test of Encryption and Decryption

In order to validate the efficiency of encryption and decryption algorithm, the simulation experiments are done on the computer of 4.0 gigabyte memory, 64 bit operating system, 1.5 billion hertz processor. The experiments are implemented with matlab2010 software. The DES encryption method, chaotic sequence encryption method and Cellular Automata encryption method are respectively used to encrypt and decrypt the original image which size is 256*256. Each method does 20 times test respectively. The time of each method can be measured according to the average time of the 20 times test. The result is shown in Table 4.

Table 4. Speed Test of Encryption and Decryption

Encryption method	Evaluation parameters	
	Encryption time(second)	Decryption time(second)
DES	2.3642	2.4967
Chaos sequence	1.3432	1.3291
Cellular Automata	0.7084	0.7588

Because the DES encryption method needs to do 16 rounds iterative computation with every 64 bits, it is a large amount of data and it takes a long time. The sequence generated by the chaotic system is 256*256 random sequences which range is from 0 to 1. But the binary image only has two states, 0 or 1. So we need to compare every data with the threshold value, select data 0 or 1, and then start the process. As a result, the efficiency of Cellular Automata encryption method is higher.

4.5. Key Space Analysis

In Cellular Automata encryption method, the key concludes three parts: the initial state of the state ring, the rules of ECA and the seed of the random number generator. To crack this method, we try to decrypt image data flow directly. Apparently the decryption process cannot

be achieved. For the size of 16*16 image, if the exhaustive method is used and *seed* is 32, the number of operation time is 2^{256}. Similarly, for the size of 256*256 image, if *seed* is 8192, the number of operation time is 2^{65536}. The amount of computation is huge. Thus, the key space of the Cellular Automata encryption method is very large. The algorithm can resist the attack of key effectively.

5. Conclusions

In this paper, a kind of QR code encryption and decryption method based on Cellular Automata has been proposed. The Elementary Cellular Automata state ring is used to encrypt and decrypt the QR code binary image. Experiments results show that this method has high speed, good security, big key space and is easy to implement. In general, it is difficult to crack the cipher-image, so one scrambling process is enough for satisfying the security requirements of QR code information in general applications. More efficient, more security, and more applicable QR Code encryption method is still the research direction in the future, although this algorithm can almost meet the requirements of speed and security in the actual encryption process.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (Grant No.61071051 and No.61005035) and the Natural Science Foundation of Heilongjiang Province (Grant No.F201020).

References

[1] Z. Lihong and L. Shujia, "Research on OR code image processing and decoding method", Journal of Beijing Technology and Business University (Natural Science Edition), vol. 26, no. 2, **(2008)** January, pp. 63-66.
[2] S. Ming, F. Longsheng, Y. Xinting and Z. Shukui, "Image analysis method for QR code's automatic recognition", Journal of University of Electronic Science and technology, vol. 38, no. 6, **(2009)** November, pp. 1017-1020.
[3] Z. Mengzhu and Hulian, "Two dimensional code security protection model research", Computer Knowledge and Technology, vol. 9, no. 3, **(2013)**, pp. 470-471.
[4] R. Yongjin, "Research of QR code double encryption based on Rijndae and XOR operation", Magnificent Writing, no. 29, **(2012)**, pp. 338.
[5] Z. Dinghui, S. Juntao and J., "Encryption and Decryption of QR code based on DES, Technology Discussion", **(2011)** March, pp. 40-42.
[6] Z. Dinghui, G. Jingbo and J., "Encryption and Decryption of QR code binary image based on Chaos", Mobile Communication, vol. 35, no. 3, **(2011)**, pp. 131-134.
[7] L. Huijun, "Research and achievement of image encryption algorithm based on Chaos Cellular Automata", Master's degree thesis of Jiangxi University of Science and Technology, **(2011)**, pp. 23-24.
[8] X. Yonghong, "Digital image encryption algorithms based on Cellular Automata", Master's degree thesis of Chongqing University, **(2012)**, pp. 23-27.
[9] F. Yuechen, W. Fengjin, G. Rongchen, F. Fangchen and L. Chen, "Chaos of Elementary Cellular Automata rule 42 of Wolfram's class II", Chaos, vol. 19, no. 1, **(2009)** March, pp. 3140-3145.
[10] Y. Gelan, Z. Jianming and X. Desheng, "Binary image encryption algorithm based on Chaotic sequences", Computer Technology and Development, vol. 16, no. 2, **(2006)** February, pp. 148-155.
[11] Z. Shuo, C. Ruhua and F. Zhuzhen, "A binary image encryption algorithm based on coupled Logistic Chaotic map", Journal of Guilin University of Electronic Technology, vol. 29, no. 3, **(2009)** June, pp. 243-246.