Design of Image Encryption Algorithm Based on Compound Two-dimensional Maps

Feng Huang
College of Electrical & Information Engineering, Hunan Institute of Engineering, Xiangtan, China
Email: huangfeng25@126.com

Xilong Qu
School of Computer & Communication, Hunan Institute of Engineering, Xiangtan, China
Email: quxilong@126.com

***Abstract*—With the application of image in internet, security of image became an important issue. The paper designs an image encryption algorithm. Firstly, it analyzes a symmetric image encryption scheme based on a new chaotic map. Analysis shows it isn't enough safe. Because there are a lot of week keys and duplicate keys in encryption. The diffusion mechanism is too simple to resist plain-text attack. The paper uses two chaotic maps at the same time to solve the problems. The maps are completely different. It designs a method of key generation. Thus it has large key space and avoids the duplicate key. At the same time parts of the key are used as the parameters of classic logistic map. It solves the problem of weak key. Several simulation results show the effectiveness of the algorithm.**

***Index Terms*—Chaotic map, Image encryption, Security**

I. INTRODUCTION

More and more images are transmitted by internet or wireless networks today. How to protect the security of image is a serious and important issue. The encryption is an important tool to protect image from malicious attackers. Some traditional encryption technologies such as DES, RSA, etc are used for information encryption. But for image, the classic encryption technologies may be not so effective. That mostly because some intrinsic features of images, such as bulk data capacity and high correlation among pixels [1].

Some special methods can be used for image encryption act as SCAN patterns, chaos encryption, etc. SCAN patterns [2,3] is a formal language-based two-dimensional spatial accessing methodology which can generate very large number of scanning paths or space filling curves. But one of the questions is that the SCAN patterns require the plain image be square image and its size be even.

In [4], blowfish algorithm is used to encrypt transformed image. The plain image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm.

Researchers present a new method for image encryption by selecting specific higher frequencies of DCT coefficients [5]. They are taken as the characteristic values. Researchers encrypt them. The resulted encrypted blocks are shuffled according to a pseudorandom bit sequence.

Therefore, recent researches of image encryption algorithms have been increasingly based on chaotic systems. Chaos can be well applied in cryptography [6]. Chaos has many characteristics which can be connected with the "confusion" and "diffusion" property in cryptography, such as sensitive dependence on initial conditions and parameters, broadband power spectrum, randomness in the time domain, ergodicity, low-dimensional etc [7]. In fact the idea of using chaos for encryption can be trace back to the classical Shannon's paper [8] in which the basic stretch-and-fold mechanism of chaos was proposed which could be used for encryption.

There are some typical chaotic maps such as the cat map, the baker map, and the standard map etc. The cat map was introduced by Arnold and Avez. In [9] a symmetric image encryption scheme based on three-dimensional chaotic cat maps is proposed. The new scheme employs a cat map to shuffle the positions of image pixels and uses logistic map to confuse the relationship between the cipher image and the plain image. The baker map is another chaotic map, based on which Pichler and Scharinger first introduced their encryption schemes. In [6] a symmetric image encryption scheme is obtained. It is shown that the permutations induced by the baker map behave as typical random permutations. The cipher image has good diffusion properties with respect to the plain image and the key. But the baker map does not have simple formula and the key are limited by size of image. In [10], a new image encryption scheme based on the extended three-dimensional chaotic baker map was presented. In [11], a new invertible two-dimensional map was proposed. An image encryption scheme based on the map is developed and the execution of the algorithm is fast and the security key can be any long integer to satisfy the different security requirements.

Manuscript received November 1, 2010; revised December 20, 2010; accepted December 27, 2010.
Corresponding authors: Feng Huang (huangfeng25@126.com)

doi:10.4304/jsw.6.10.1953-1960

For the drawbacks of small key space and weak security in low-dimensional chaotic cryptosystems, researchers propose a coupled nonlinear chaotic map [1]. It is a symmetric key cryptography with a stream cipher structure. It provides an efficient and secure way for real-time image encryption and transmission

In [12], it uses a new two-dimensional chaotic map. It encrypts images by processing image stretch-and-fold. The chaotic map is divided into the left map and the right map. The process shuffles the positions of image pixels. The encryption has good diffusion properties with respect to the plain image and the key. A new image encryption scheme based on the chaotic map is developed which is composed with a diffusion mechanism.

But it isn't enough safe. Firstly there are a lot of week key and duplicate key. Secondly the diffusion mechanism is too simple to resist plain-text attack.

The paper used two chaotic maps at the same time to solve the problems. It designs a method of key generation. Thus it has large key space and avoids the duplicate key. Then it uses parts of key as the parameters of a classic logistic map which acts as the diffusion mechanism. The value of pixels of cipher image is charged by logistic map. Encryption is more sensitive to key. Simulation results show it solves the problem of week key and duplicate key and protects the security of the image.

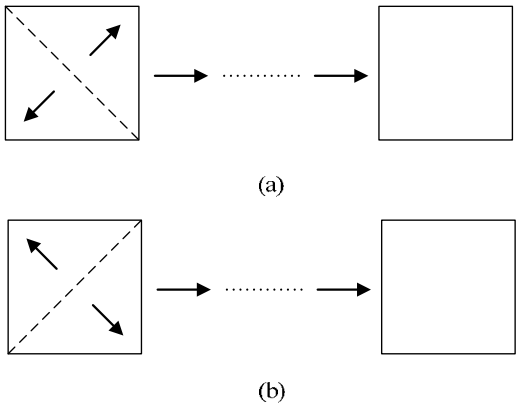
II. Introduction of the Chaotic Map

The two-dimensional chaotic map in [9] utilizes an important characteristic of images, which is each pixel of column of image can be inserted into adjacent two pixels of row of image. The new chaotic map can encrypt images by processing image stretch-and-fold.

The process of the chaotic map is seen in Figure 1. Firstly each pixel of diagonal of a square image is inserted into adjacent two pixels of adjacent diagonal pixels one by one. Then each pixel of the next diagonal pixels is inserted into adjacent two pixels of the adjacent diagonal. Then each pixel of the second diagonal of a square image is inserted into adjacent two pixel of the next diagonal. Repeating the process, the image is stretched and joins a line of pixels. Secondly the line is fold over to a new square image with the same size to the plain image. The map shuffles the positions of image pixels. All the process is invertible which is seen in Figure 1. The chaotic map is divided into two forms: the left map and the right map.

In order to explain the chaotic map more clearly, a simple example is given here.

The image with 4×4 pixels, that is N=4. The process of the map is shown in Figure 2. In upper triangle, pixel (0,0) can be inserted before pixel (0,1). Pixel (1,1) can be inserted between pixels (0,1) and (1,2). Pixel (2,2) can be inserted between pixels (1,2) and (2,3) and so on. Then the pixels join to a part of line: (0,0), (0,1), (1,1), (1,2), (2,2), (2,3)…. in lower triangle , pixel (1,0) can be inserted before (2,0). Pixel (2,1) can be inserted between pixel (2,0) and (3,1) and so on. The pixels join to another part of line. Then it connects two parts to a line. Lastly it is from a line to a square image different from the originally one.



(a)

(b)

(a) The left map
(b) The right map

Figure 1. Principle of the chaotic map.

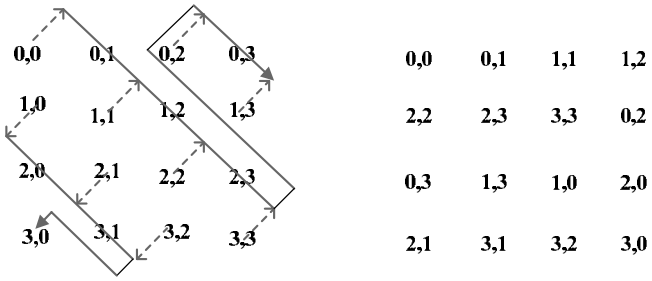


Figure 2. The process of the map.

Supposing the dimension of a square image is $N \times N$, where N is an integer. $A(i, j)$ is the matrix of a square image, in which each element corresponds to a gray-level value of the pixel (i, j); $L(i)$, i=0, …, N-1, j=0, …, N-1. N is a one dimensional vector mapped from A.

The left map

$$L(2i+(j-i)\times N-(j-i)\times(j-i-1)/2) = A(i,j) \quad while\ i \le j,\ j-i\ is\ even\ number \tag{1}$$

$$L(2i+1+(j-i-1)\times N-(j-i-1)\times(j-i-2)/2) = A(i,j) \quad while\ i \le j,\ j-i\ is\ odd\ number \tag{2}$$

$$L((N^2+N)/2+2\times j+1+(i-j-2)\times N-(j-i-1)\times(j-i-2)/2) = A(i,j) \quad while\ i > j, i-j\ is\ even\ number \tag{3}$$

$$L((N^2+N)/2+2\times j+(i-j-1)\times N-(j-i)\times(j-i-1)/2) = A(i,j) \quad while\ i > j, i-j\ is\ odd\ number \tag{4}$$

The right map

The right map is shown in Figure 1(b); first, a mirror process of the image is made. The algorithm of the mirror image is described with the following formula:

$$A'(i,\ j) = A(i,\ N\ -1-\ j) \tag{5}$$

where A′ is the matrix of the mirror image of a square image A.

$$L(2i+(j-i)\times N-(j-i)\times(j-i-1)/2) = A(i,N-1-j) \quad while\ i \le j,\ j-i\ is\ even\ number \tag{6}$$

$$L(2i+1+(j-i-1)\times N-(j-i-1)\times(j-i-2)/2) = A(i,N-1-j) \quad while\ i \le j,\ j-i\ is\ odd\ number \tag{7}$$

$$L((N^2+N)/2+2\times j+1+(i-j-2)\times N-(j-i-1)\times(j-i-2)/2) = A(i,N-1-j) \quad while\ i > j, i-j\ is\ even\ number \tag{8}$$

$$L((N^2+N)/2+2\times j+(i-j-1)\times N-(j-i)\times(j-i-1)/2) = A(i,N-1-j) \quad while\ i > j, i-j\ is\ odd\ number \tag{9}$$

The map from a line to a square image

The line of $N\times N$ pixels L is further mapped to a same size $N\times N$ square image, B. The map from line L to image B is described with the following formula:

$$B(i,\ j) = L(i\cdot N+\ j) \tag{10}$$

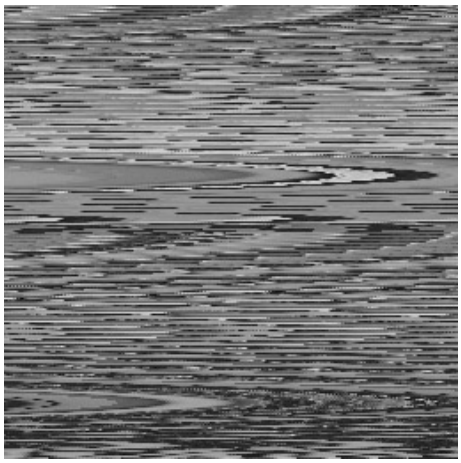
The map is invertible. So the process of the invertible map is the inverse process of map.

The image encryption is achieved by pixels permutation firstly. Since the chaotic map was divided into the left map and the right map, the numbers of the left map and the right map were used as secret key in image encryption. If the key are in decimal, from the least significant digit to the most significant digit, each digit (0-9) corresponds to the iteration number of the left map and the right map alternately.

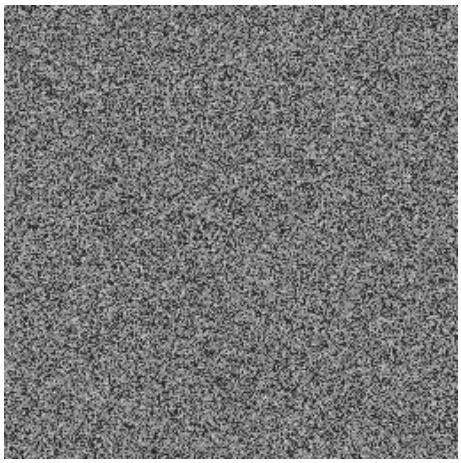
For example, a secret key "321" means that an image is mapped to another cipher image through an iteration of the left map, 2 iterations of the right map, and 3 iterations of the left map as shown in Figure 1. In another case where the key is represented in binary digit, from the least significant digit to the most significant digit, every four digits (0-15) correspond to the iteration numbers of the left map and the right map alternately. A simple diffusion mechanism was use to generate uniform histograms and achieves complete diffusion with respect to plain image. Since the length of the key of the map had no limit, its key space could be calculated according to the length of the key.

An image encryption is carried out based on the map. The plain image and cipher image are shown in Figure 3. It has 256×256 pixels with 256 grey levels. The plain image is encrypted using the chaotic map by the key "1" and "1234567890123456". It can be seen that the plain image has been encrypted. The plain image and the cipher image are equal for every pixel; the decrypted image is recovered completely. It shows the image encryption using the chaotic map has no message loss.

(a) Plain image



(b) Cipher image (key "1")



(c) Cipher image (key "1234567890123456")

Figure 3. Plain image and cipher images.

III. SECURITY OF ENCRYPTION

Key space

Since the length of the key of the map has no limit, its key space can be calculated according to the length of the key. Suppose the key are represented in binary bits. The relationship between the key space size and the key length is shown in Table 1. In theory, security key can be any long integer to satisfy the different security requirements.

TABLE I.
KEY SPACE SIZE VS KEY LENGTH

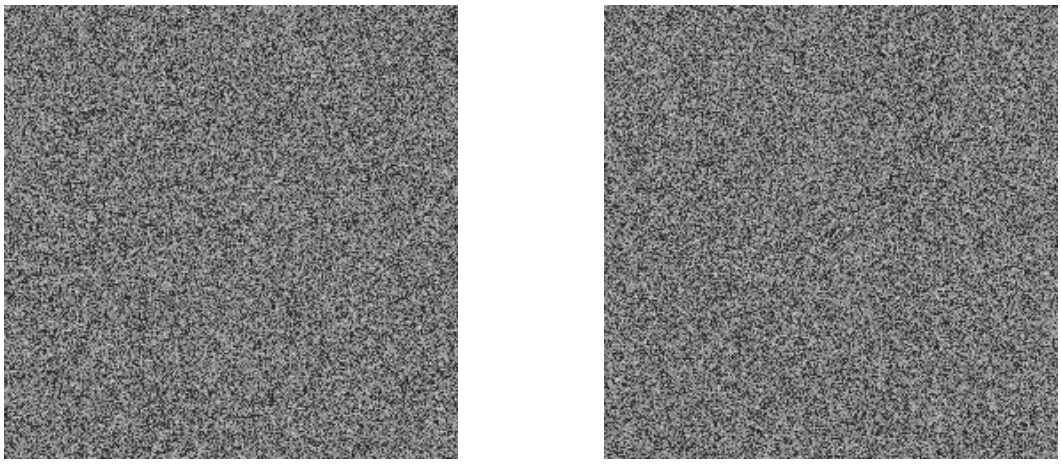
Key length (bits)	64	256	512
Key space size	1.84×10^{19}	1.16×10^{77}	1.34×10^{154}

Key Sensitivity

Assume that an image is encrypted using the map with key is "1234567890123456", just as seen in Figure 3.

Now, the least significant bit of the key is changed and the test is done for image decryption. The original key "1234567890123456" is changed to $keys_1$ "1234567890123455" and $keys_2$ "1234567890123457", both of which are used to decrypt the cipher image by the original key "1234567890123456" respectively.

The two decrypted images by two different key are shown in Figure 4. It can be seen that the image cannot be decrypted using both two key, which are different from the correct key only in the least bit one. Therefore, the security of the image encryption using the chaotic map is much effective.



(a) Decrypted image (key "1234567890123455") (b) Decrypted image (key "1234567890123457")

Figure 4. Decryption by two error keys.

Correlation

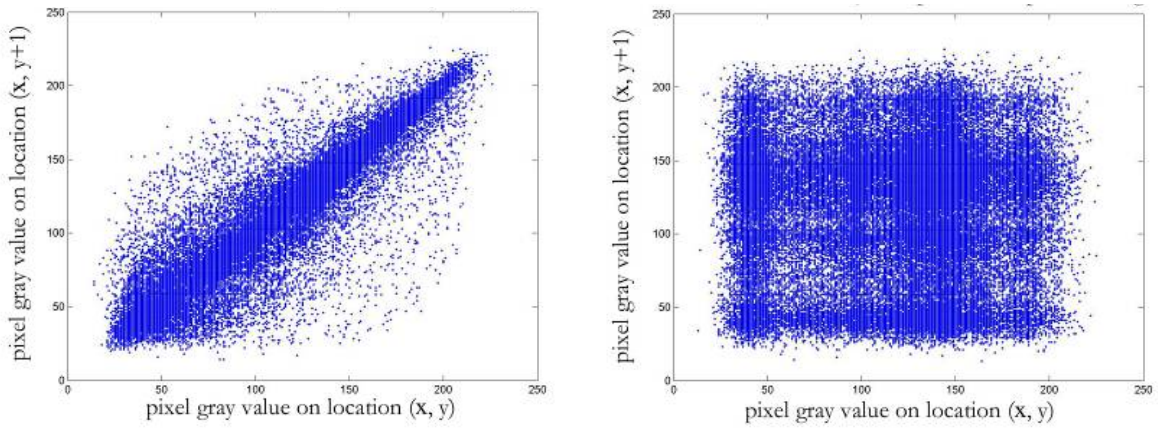
Correlation of two adjacent pixels in a cipher image:

$$cov(x,y) = E(x - E(x))(y - E(y)) \tag{11}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{12}$$

Where x and y are gray-scale values of two adjacent

Fig 5 shows the correlations of two horizon-tally adjacent pixels in the plain image and the cipher image: the correlation coefficients are 0.9442 and 0.0017. Similar results for diagonal and vertical directions were obtained and are shown in Table 2.



(a) Plain image (b) Cipher image

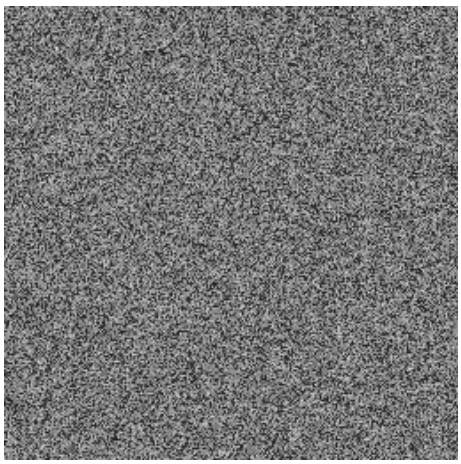
Figure 5. Correlations in plain image and cipher image.

TABLE II.
CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS

	Plain image	Cipher image
horizontal	0.9442	0.0014
vertical	0.9711	0.0011
diagonal	0.9187	0.0054

Week key and duplicate key

But there are some problems in key generation. Suppose the key are six decimal numbers, act as "012345". Obviously the first digit "0" can't play any role. The "0" is a weak key. At the same time, the iteration number of map means the level of permutation of image. If each even digit of the key is zero, sum of the rest key is the frequency of left map. Act as the key are "103050", sum of the iteration number is 9. Then there are other key: "10107", "10206", "10303" and so on can decrypt the cipher image. They are equivalent key. An example can be seen in Figure 6. Obviously the cipher image was decrypted by equivalent key.



(a) Cipher image (key "103050")

(b) Decrypted image (key "10107")

Figure 6. Decryption by an error key.

In fact, if key_1 are $k_1k_2k_3k_4k_5k_6$…, key_2 are $k_1'k_2'k_3'k_4'k_5'k_6'$…while $k_2=k_4=k_6=\ldots=k_2'=k_4'=k_6'=\ldots=0$, then key_1 and key_2 are equivalent key. It is similar when each odd digit of the key is zero.

There is another serious security problem. The process of chaotic map must cost time. If the numbers of the left map and the right map were used as secret key in image encryption, the whole encryption time may disclosure the iteration number of chaotic map. In fact it is the key.

By above example, if the key are "103050" the whole encryption time is about 0.02s (the CPU of pc is Intel's L2300, the ram is 1G, and the operating system is windows XP). While key is "1" or "01" the time is about 0.0023. Obviously, the iteration number is about 9. The sum of all the bits of key is about 9. Theoretical the original key space is 10^6. But in fact the key space is only 2,002 which are much smaller than the theoretical values. Parts of theoretical and real key space of six decimal numbers key can be seen in Table.3, the sum express the sum of all the bits of key. In fact the real key space is also smaller than the values in table by previous conclusions. Act as when sum is 1, the key space only is 2 which much smaller than theoretical value.

TABLE III.
PARTS OF THEORETICAL AND REAL KEY SPACE OF SIX DECIMAL KEY

Real key space							
Sum is 1	Sum is 2	Sum is 3	Sum is 4	Sum is 5	Sum is 6	Sum is 7	Sum is 8
6	21	56	126	252	462	792	1287

It can be noted that it is not safe when the sum of all the bits of key is small. The key space becomes bigger and bigger with the increase of sum of all the bits of key.

Issue of diffusion mechanism

The paper [12] used a diffusion mechanism which can be described as follows:

$$x_k' = x_k + G(x_{k-1}')\bmod L$$
$$x_{-1} = \textit{initial value} \quad (13)$$

where x_k is value of pixels, L is the grey levels of image, x_k' is new value of pixels, k is the serial number of pixel. The function G is an arbitrary function of the gray level, here x_{-1} =150, $G(x)$ =5x.

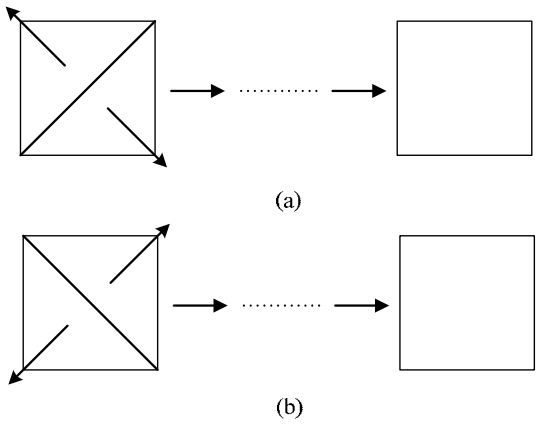
The part of key of security is x_{-1} and $G(x)$. Here x_{-1} is a fixed value and $G(x)$ is a linear function.

It is very insecure and can't resist plain text attack. It can choose a special image act as a white image to get the value of x_{-1} and a black image to get function of $G(x)$.

IV. AN IMPROVED IMAGE ENCRYPTION ALGORITHM

Here the key are six decimal numbers. It can be known that zeros are best to avoid becoming main parts of the key firstly. Secondly, it must have a mechanism to increase the key space. Thirdly the diffusion mechanism must be complex nonlinear process.

It can use multiple chaotic maps to avoid the week key and duplicate key. Here the paper used another chaotic map [11]. It is seen in Figure 7.



(a) The left map
(b) The right map

Figure 7. Principle of the chaotic map.

Supposing the dimension of a square image is $N \times N$, where N is an integer. $A(i, j)$ is the matrix of a square image, in which each element corresponds to a gray-level value of the pixel (i, j); $L(i)$, i=0, …, N-1, j=0, …, N-1. N is a one dimensional vector mapped from A.

Left map

$$L((2N-2j+1)\times j+2(i-j)-1)=A(i,j) \quad i+j<N,\ i>j, \tag{14}$$

$$L((2N-2i+1)\times i+2(j-i))=A(i,j) \quad i+j<N,\ i\le j \tag{15}$$

$$L(N^2-(2j+1)\times(N-1-j)-2(j-i))=A(i,j) \quad i+j\ge N, i<j \tag{16}$$

$$L(N^2-(2i+1)\times(N-1-i)-2(i-j)-1)=A(i,j) \quad i+j\ge N,\ i\ge j \tag{17}$$

Right map

$$L((2N-2j+1)\times j+2(i-j)-1)=A(i,N-1-j) \quad i+j<N,\ i>j \tag{18}$$

$$L((2N-2i+1)\times i+2(j-i))=A(i,N-1-j) \quad i+j<N, i\le j \tag{19}$$

$$L(N^2-(2j+1)\times(N-1-j)-2(j-i))=A(i,N-1-j) \quad i+j\ge N, i<j \tag{20}$$

$$L(N^2-(2i+1)\times(N-1-i)-2(i-j)-1)=A(i,N-1-j) \quad i+j\ge N, i\ge j \tag{21}$$

The line of $N \times N$ pixels L is further mapped to a same size $N \times N$ square image, B. The map from line L to image B is same to formula (10).

Key generation

At first, the key are an arbitrary six decimal numbers, act as “654321”. It can be proved the real key space only 13,992. Obviously it is unsafe.

But there are two chaotic maps. The key can be designed as the number of two chaotic maps. The idea is similar to the scan pattern. If there are more chaotic map, the will be more flexible. Here the odd digit represses the number of the first chaotic map the even digit represses the number of the second one. At the same time odd digits in the odd digits repress the number of the left map. Even digits in the odd digits repress the right map. If the key are “654321”, it means that “6” time left map of the first map, “5” time left map of second map, “4” time right map of the first map, “3” time right map of second map, “2” time left map of the first map and “1” time left map of second map.

Diffusion mechanism

The second step is to add a diffusion mechanism to confuse the value of pixels and change the demographic characteristics of the cipher image. It can use the logistic map:

$$X_{n+1}=a\times X_n\times(1-X_n) \tag{22}$$

Here $a\in(0,4)$, $X_n\in(0,1)$, $n=1,2,3\ldots$.

Simulation

Suppose a=3.9 and X_0 is a function of origin key. Act as a simple function X_0=*key*/100000. So the X_0 is 0.654321.

The result of simulation can be seen in Figure 8. The time of permutation is about 0.3s and the time of diffusion is 0.005s.

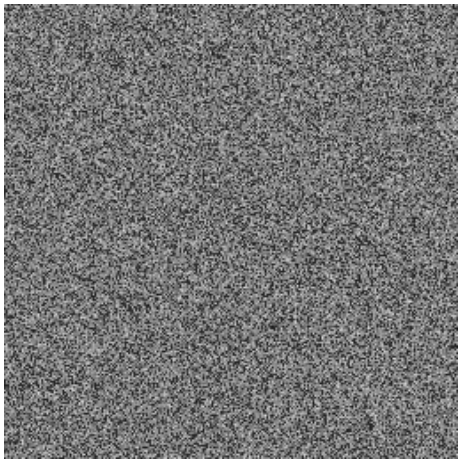
IV. SUMMARY

The paper analyzes a symmetric image encryption scheme based on a new chaotic map. The map can encrypt image by shuffling the position of pixels of image. It includes two different maps: left map and right map. The numbers of the two maps are used as the secret key of encryption. But analysis shows that there are a lot of week key and duplicate key in encryption. At the same time the diffusion mechanism is too simple. The paper uses two chaotic maps at the same time to avoid week key and duplicate key. It also has a large key space. Parts of the key are used as the parameters of classic logistic map. Simulation results show the effectiveness of the method.

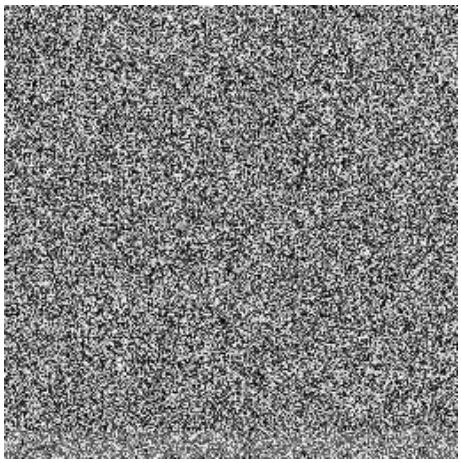
ACKNOWLEDGMENT

The authors wish to thank Fangfang Lei. Authors gratefully acknowledge the Projects Supported by Scientific Research Fund of Hunan Provincial Education Department (08B015, 08A009) for supporting this research. Project supported by Provincial Natural Science Foundation of Hunan (10JJ6099) supports the research. Project supported by Provincial Science & Technology plan project of Hunan (2010GK3048) supports the research.

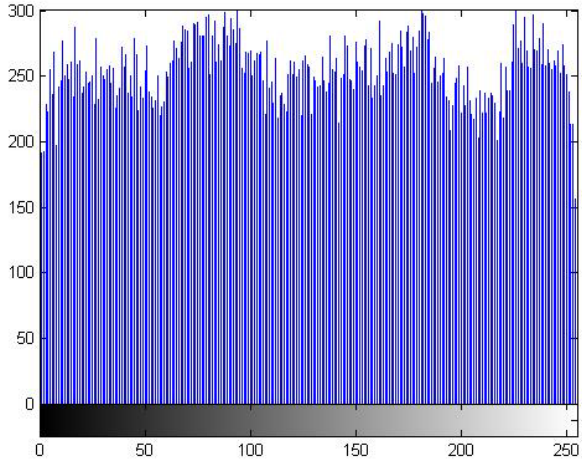
(a) Plain image



(b)Shuffled image



(c)cipher image



(d) Histogram of the cipher image

Figure 8. Process of simulation

REFERENCES

[1] S. Mazloom, A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," Chaos, Solitons & Fractals. vol. 42(3), pp. 1745-1754, 15 November 2009.

[2] N. Bourbakis, C. Alexopoulos, "Picture data encryption using SCAN patterns," Pattern Recognition, vol.25(6), pp.567-58, 1992.

[3] S. S. Maniccam, N. G. Bourbkis, "Image and video encryption using Scan Patterns," Pattern Recognition, Vol.37(4): pp.725-737, 2004.

[4] B. Y. Mohammad Ali and J. Aman, "Image encryption using Block-Based transformation algorithm," IAENG Int J Computer Science, vol. 35(1), pp. 15-23, 19 February 2008.

[5] L. Krikor, S. Bab, T. Ari and Zyad Shaaban, "Image encryption using DCT and stream cipher,". European Journal of Scientific Research, vol.32(1), pp.47-57, 2009.

[6] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps,"Int J Bifurcat Chaos, vol.8, pp.1259-1284, 1998.

[7] L. Kocarev, "Chaos-Based cryptography: a brief overview," IEEE Circuits and System Magazine, vol.1(3), pp.6-21, 2001.

[8] C. E. Shannon, "Communication theory of secrecy systems," The Bell System Technical Journal, vol.28(4), pp.656-715, 1949.

[9] G. Chen, Y. Mao, and C. K. Chui, "A Symmetric Image Encryption scheme based on 3D chaotic cat maps,"Chaos Solitons and Fractals, vol.21, pp.749-761, 2004.

[10] Y. Mao, G. Chen and S. Lian, "A novel fast image encryption scheme based on 3D chaotic Baker maps," Int J Bifurcat Chaos, vol.14, pp.3613-3624, 2004.

[11] F. Huang, Y. Feng. " A symmetric image encryption scheme based on a simple novel two-dimensional map," Int J Innovative Computing, Information and Control, vol.3, pp1591-1600, 2007.

[12] F. Huang, F. F. Lei. " A novel symmetric image encryption approach based on a new invertible two-dimensional map," IIHMSP 2008, pp 1340 - 1343, 2008.

Feng Huang (1978-), was born in Shaoyang, Hunan, P. R. C. He received the B.S. degree in automatic test and control form Harbin Institute of Technology, P. R. C., in 2000, the M.S. degree in Power Engineering form Harbin Institute of Technology, P. R. C., in 2002, and the PHD degree in Power Electronics and Power Drives from Harbin Institute of Technology, P. R. C., in 2007. He is an associate professor of College of electrical & information engineering, Hunan Institute of Engineering, Xiangtan, P. R. C. His research interests include image encryption, design of Automated Test System. He had several years experience in teaching, research and development in projects and published over 20 scientific papers.

Xilong Qu (1978-), was born in Shaoyang, Hunan, P. R. C. He received the PHD degree from Southwest Jiaotong University, P. R. C. in 2006. Now he is an associate professor of Hunan Institute of Engineering, master supervisor of Xiangtan University, the key young teacher of Hunan province, academic leader of computer application technology in Hunan Institute of Engineering. His research interesting is web service technology, information safety and networked manufacturing. He has published over 30 papers in some important magazines.