An chaos image encryption algorithm based on binary sequence and baker mapping[1]

Runhe Qiu, Cheng Zhu and Shihui Liu

College of Information Sciences and Technology
Engineering Research Center of Digitized Textile & Fashion Technology, Ministry of Education
Donghua University, Shanghai 201620, P. R. China

email: qiurh@dhu.edu.cn, air_zc@yeah.net, 877979689@qq.com

Keywords: sequence; chaos encryption; baker mapping; diffusion

Abstract. based on the chaotic binary sequence and the baker mapping, this article puts forward an image encryption algorithm combined image scrambling and diffusion. Firstly, we use an improved baker mapping algorithm to scramble the primary image, which expands the range of the mapping to a non-square image. Then, we encrypts the scrambled image through binary sequence, so that the values have been greatly changed, and the relevance with around as well. After several times of iteration, we get an encrypted image. Through the simulation analysis, the algorithm gets an ideal encrypted image and restores the image correctly. The algorithm has a large key space, it is hard to be decrypted and is easy to be carried out.

Introduction

In today's society, information technology is developing rapidly, information exchange is also becoming much more often as well as lots of problems on security of information. As a result, we should pay much more attention on the information security technology to deal with the rapidly developing information exchange technology. With the development of cryptography, chaos theory had been used to design an image encryption algorithm[1-2]. In the phylogeny of chaotic cryptography, Shannon was the first to come up with two basic encryption technologies[3], namely scramble and diffusion, which became very important theories for cryptography designing in the late years. The susceptibility of chaotic system to parameter and the nature of random alike concur well with the chaos principle of traditional encryption system. In 1998, Fridrich put forward a Symmetric ciphers based on two dimensional chaotic maps[4]. This algorithm enables the key to change the length, so that we can get security of different levels. It was also suitable for large amount of data and had higher encryption rate. In the same year, Scharinger designed an image encryption technology based on chaotic Kolmogorov stream[5], this algorithm worked through the chaos encryption key control system which based on Kolmogorov flow, using psendo random sequence to scramble the data. In 2004, Chen put forward a Symmetrical image encryption algorithm[6], Xuefeng Zhang introduced chaos system to the image fusion technology[7]. Changzhen Xiong made an effort working on the process of image encryption to provide large key space[8]. Comparing to the traditional cryptography, the chaotic system spread the initial scope throughout the entire phase space by means of iteration for several times. The chaotic system has many good features, such as good pseudo-random characteristics, the tracks of the unpredictability, extremely sensitive to the initial state and structural parameters. These all correspond to the demand of the cryptography. Despite the advantage mentioned above, we also find some disadvantages, such as periodicity and the capacity of resisting disturbance. This article puts forward a new method of image encryption, which combines the chaos binary sequence with image fusion technology through scrambling and diffusion. This method not only scrambles the position of pixel, but also use the chaos binary sequence to encrypt the pixel one by one. After several times of iteration, it achieves a good result. So this diffusion-fusion-based encryption algorithm taking full consideration

[1] Supported by Innovation Program of Shanghai Municipal Education Commission

of the characteristics of the image itself, with higher reliability and easy to realize, has much more advantages over traditional methods.

Chaos image encryption based on binary sequence and baker mapping

Fundamental of the algorithm

Viewing from the space distribution, we may find that the image is a rectangular piece which is made up of several pixels. In the process of encryption, we need to rearrange the position of the pixels, further more we should process the size of the pixel in order to make it more safety. There are some basic scrambling methods that based on chaos[9] such as Arnold mapping, 2D-logistic mapping, FASS curve and so on. But each of them has its boundedness[10]. For example, they all relate to periodicity. In some methods, we can't define the operator, because it is fixed and has nothing to do with the key. In some others, the key space is too small to provide a high safety coefficient. This article firstly comes up with an improved algorithm, and then introduces the method of diffusion. So that the encrypted size of the pixel not just relates to its primary position and size, but relies on the size of the pixels around it. Figure 1 is the flow chat of this algorithm.

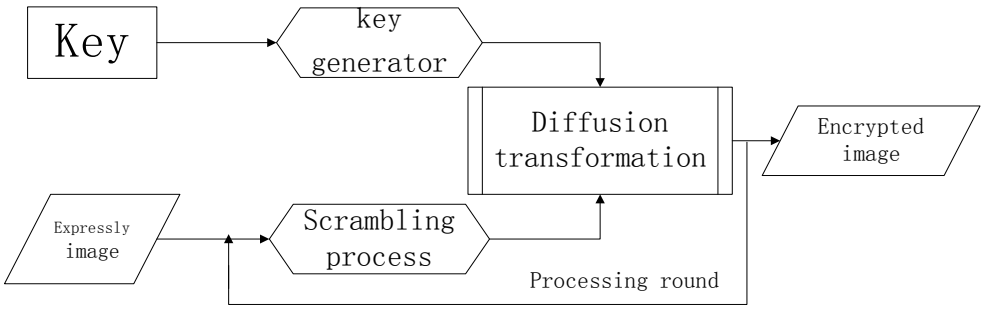


Figure 1 flow chat

Chaos Bingary Sequence

In the certainly nonlinear system of dynamics system, if there exists a kind of random phenomena made by nonlinear interaction in the interior system without any additional random factors, we can call it Chaos. Logistic[1-2] mapping is a simple but widely researched dynamic system, it is defined as formula (1):

$$x_{k+1} = \mu x_k (1 - x_k) \qquad (1)$$
$$x_k \in [0,1], \mu \in [0,4], k = 0,1,...$$

For each μ, we may get corresponding serials values $x_0, x_1, ..., x_k$. When the is μ in the range of [3,4], the shape dynamics system is complex, the system change from the periodic state into chaotic state. The research of chaotic dynamics shows that when $3.5699456 < \mu \leq 4$, the logistic mapping is in the state of chaos, producing an aperiodic sequence $\{x_k, k = 0,1,2,3,...\}$, which is sensitive to the initial value with no convergence. The chaotic sequence produced by logistic mapping has some significant statistical property. For example, the average time of the sequence is 0; when we select two different initial values, the cross-correlation function we get is 0. Besides that, we knows that the logistic sequence is sensitive to the initial value, even a tiny difference can make a big difference. In the meanwhile, it's hard for us to infer the initial condition of the chaotic sequence. This makes the encryption algorithm more reliable.

We can use several different ways to produce chaotic sequence by logistic mapping, like real-valued sequence, binary sequence, bit sequence, etc. The real-valued sequence is easy to produce but not very secure, bit sequence has much more safety but it's not convenient to be carried out on

the hardware platform. In consideration of the safety and the realizability on hardware platform, this text produces a binary form the traditional logistic sequence. The binary sequence enhances the reliability of the key, and it can reduce the time complexity. At the meantime, it's easier to practice on the hardware platform. The binary sequence is defined in the following formula (2):

$$\Gamma(x)\begin{cases}0 & -1 \le x \le 0\\ 1 & 0 \le x \le 1\end{cases} \quad (2)$$

Through the formula above, we can get a binary sequence based on logistic chaotic sequence, we will apply it the process of diffusion.

Chaos Confusion

The document[11] used a kind of discretized Kolmogorov change to scramble the image, because of the imaging of the process, we call it baker mapping, formula (3) is the initial definition of two dimension baker mapping[7-8]:

$$\begin{cases}B(x, y) = (2x, y/2), 0 \leqslant x \leqslant 1/2\\ B(x, y) = (2x-1, y/2+1/2), 1/2 \leqslant x \leqslant 1\end{cases} \quad (3)$$

This method has a larger key space , a better dispersion and un certainty . But the traditional baker mapping is only suitable for the $N * N$ image, this article puts forward an improved method which can suit an $N * M$ image. The algorithm is described below:

For the image of $N * M$, suppose a series of sequence made of k integers: $\delta = (n_1, n_2, n_3 \ldots n_k) 0 \le n_i \le N$, and also 1. $\sum_{i=1}^{k} n_i = N$, 2. Each integer n_i can be divided by M. Suppose $q_s (s = 1,2 \ldots\ldots, k)$ is determined by $q_s = M / n_s$, meanwhile q_s is positive integer, N_s is the left border in vertical zone

After plug the above expression

The above formula means: the image is a rectangle of $N * M$ which is divided into rectangular pieces with a height of M and a width of n_i. Then horizontal stretched the rectangular pieces, and compress them in vertical direction, that turn the $M * n_i$ rectangle into $n_i * M$ rectangles. During the actual simulation using MATLAB, we divided the image into several parts of the same size, then execute with different transform formula, so as to get a better scrambling image effect, and also a stronger anti-decryption ability.

On the base of above mapping, the reversed substitution formula $T_{n,\delta}^{-1}$ can be described as the following formula (4):

$$T_{n,\delta}^{-1} = (q_s (x - N_s) + (yMODq_S), (yDIVq_s + N_s)) \quad (4)$$

Chaos diffusion

Next is the diffusion of the scrambled image. Imagine the grey level of pixel is L, and $g_{i,j}$ is the corresponding grey level of pixel, (i, j), $g_{i,j} \in \{0, \ldots\ldots L-1\}$. To ensure the security, beside the relevancy of their own, the diffusion pixel should also be relevant to their own positions and other pixels. The related transform formula[12-13] can be described as following formula(5):

$$h(i, j, g_{i,j}) = \left(g_{i,j} + h'(i, j)\right) \bmod L \quad (5)$$

In above formula, h can be a random function that use i, j as the independent variable and $h(i, j, g_{i,j})$ as the pixel after diffusion. The specific transform[12-13] formula (6) used in the article is as below:

$$h(i, j, g_{i,j}) = g_{i,j} \text{XOR} (i, j \bmod L) \quad (6)$$

During the diffusion step, we execute OR in the image that already finished binary sequence and scrambling. Here the OR step may be explained as: After mocking up the chaos sequence,

transform to the bit series with a corresponding decimals, meanwhile also transform the scrambled pixel, then execute OR of the two bit by bit, and finally get the diffusion pixel.

Repeat above scrambling and diffusion steps until the encryption round meets the prescriptive time.

The decryption process is similar with the encryption process; firstly, does the diffusion transform inverse operation of encrypted image, then does inverse transformation of the pixel position. Repeat the above process until the original image is recovered.

Specific Steps of Image Encryption and Decryption

Basic steps of image encryption and decryption algorithm based on chaotic sequence:

Step1 Use Logistic mapping expression to produce chaotic sequence, $x(n)\ (n = 0,1,\ldots\ldots M_n)$

Step2 Use transform condition to produce binary sequences, notes for $z(n)\ (n = 0,1,\ldots\ldots M_n)$

Step3 Take $N * M$ elements from $Z(1)$ to consist a matrix $Z_1(i, j)$ of $N * M$

Step4 Scramble the original image $I(i, j)$ using modified hashing algorithm, get the scrambling image $I^*(i, j)$

Step5 Diffuse the scrambling image $I^*(i, j)$ using matrix $Z_1(i, j)$, get the diffusion image $H(i, j)$

Step6 Repeat the process m times, get the final encrypted image $H^*(i, j)$.

The process of image decryption, which is the inverse process of encryption process, decrypt the image on the foundation of having the encrypted image and the correct secret key, and the basic steps is the same as the image encryption.

Matlab Simulation Experiment Result and Analysis of Merit and Demerit

Simulate the original image a using Matlab with a pixel of 256*256, shown in Fig.2. Take the Key value as μ=4, the initial value of chaotic sequence of x0=0.9, the simulation result is showed as follows:

Fig.2 Original a

Fig.3 encrypted for one time

After encrypt for one time, the image is showed as Fig.3. Then after encrypt for 15 time, 30 times, the images are showed as Fig.4, Fig.5.

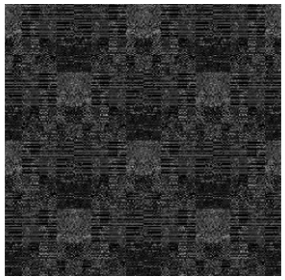


Fig.4 encrypted for 15times

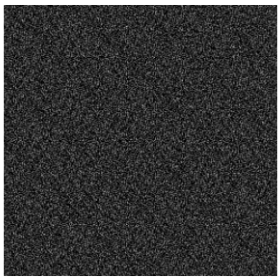


Fig.5 encrypted for 30times

It can be seen that after several encryption, the image got excellent encryption result. Then according to the principle and steps of image decryption, the decrypted image is showed as Fig.6.

Fig.6 Decrypted image

As Fig.6 showed, the decrypted image restored the original image accurately.

If choose the original image with a pixel of 200*192, showed as Fig.7, and the encryption time is 30, we will also get a good encryption result. The encrypted image is showed in Fig.8 and the decrypted image is Fig.9.

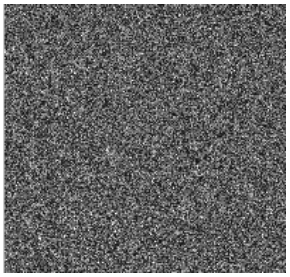
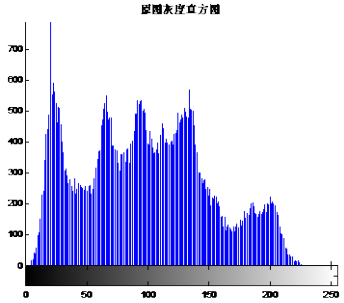


Fig.7 Original b Fig.8 Encrypted Fig.9 Decrypted

This article used MATLAB to simulate the image encryption. According to the efficiency of simulation, the running time of the encrypted process is very short, and with an increasing number of the encryption round, the decryption time is also increasing. From the encrypted images, we can see a great difference between the original and encrypted images. After 15 times' encryption, it's hardly to identify the image. After 30 times' encryption, the encryption result is amazing. The encryption process is very fast. From the decrypted image, we can get the decrypted image quickly and accurately with the correct secret key and the specific encryption algorithm, which also explain the high integrity and reliability of this algorithm.



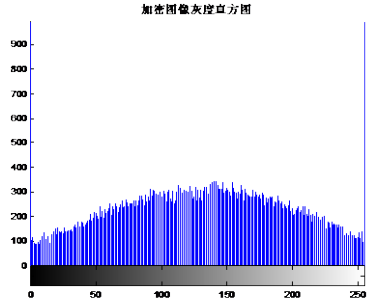


Fig.10 (a) Original grey level histogram (b) Encrypted grey level histogram

Fig.10(a)、(b) are the original grey level histogram and the encrypted grey level histogram. According to the comparison of the two images, the encrypted grey level histogram met the uniform distribution in the whole interval, and also concealed the distribution rule of the original grey level histogram which completed the encryption perfectly.

Compared with the traditional image encryption algorithm, e.g. single use scrambling technology or chaotic sequence to encrypt, the traditional encryption algorithm doesn't change the image pixel but only scramble the position or modify the size of the image pixel. The encryption algorithm used in this article changes not only the position but also the size of the image pixel. Firstly, the binary sequence has a better statistical property, and a better balance than common Logistic sequence. Secondly, during the algorithm simulating, scramble the original image from each region, then use different baker mappings in each region so as to get a better encryption result and hardly cracked

encrypted image. On one hand, this algorithm keeps the sensitivity of the encryption key to the encrypted image, on the other hand enhances the security of the image encryption. Meanwhile, use multiple iterations to get better encryption results. Because of the algorithm which mixed the scrambling and diffusion, the encryption result is no doubt preferable, but the time complexity of the encryption process is relatively high. When dealing with a higher pixel hd image, the encryption time is long and likewise the decryption time is also long. According to the principle of the algorithm, the pixel changing strategy in this article is realized by binary sequence, so the changes of image pixel are not great. If use other diffusion methods, it may cause a great change in pixel and also increase the time complexity of the algorithm.

Conclusion

In this paper, an algorithm based on the mixture of a scrambling and diffusion of chaos binary sequence is provided. Compared with the traditional algorithm, the binary sequence not only keep the randomness of logistic and initial value sensitivity, but also merge together with the scrambling image to change the size of image pixel. Through the simulation analysis, this algorithm can be better applied to image encryption technology to get a preferable encryption result. The next step is to increase the efficiency of the algorithm and reduce the time complexity at the same time, so as to apply the image encryption technology to more engineering fields.

Reference

[1] Wang Yong, Li Changbing, He Bo. Chaotic encryption algorithm and Hash function structure research. [M]. Beijing: Electronic Industry Press, 2011. 94-99.

[2] Zhang Yunpeng, Zuo Fei, Huo Zhengjun. Summary of digital image decryption based on chao. [J]. Computer Engineering and Design, 2011, 32 (2): 463-466

[3] Shan C E. Communication theory of secrecy systems [J]. Bell System Technical Journal,1942,28(4):656-715

[4] Fridrich Jiri. Symmetric ciphers based on two dimensional chaotic maps[J]. Int J Bifurcation and Chaos,1998,8(6):1259-1284

[5] Scharinger J.Fast encryption of image data using chaotic Kolmogrov flow [J].J Electronic Eng,1998,7(2):318-325.

[6] Chen Guanrong,Mao Yaobin,Charles K.A symmetric image encryption scheme based on 3D chaotic cat maps [J]. Chaos, Solitons and Fractals, 2004, 21(3):749-761

[7] Zhang Xuefeng, FAN Jiulun. Digital image hiding technology based on chaos system [J]. Computer Engineering, 2007, 28(9): 134-136.

[8] Xiong Changzhen, Zou Jiancheng, Qi Dongxu. A new digital image encryption algorithm based on chaos mapping. [J], Journal of Sun Yat-sen University (natural science edition), 2004, 43(2): 29-33.

[9] Wen Zhiqiang, Li Taoshen, Zhang Zengfang. A new image encryption technology based on chaos sequence. [J]. Computer engineering, 2008, 31(10): 130-131.

[10] Fengling Han，Xinghuo Yu，Songchen Han. Improved Baker Map for Image Encryption [A] . IEEE，2009

[11] Xu Kebing, Huang Wenpei. A binary scrambling image encryption based on Baker mapping. [J]. Microcomputer Information, 2008, 43(18): 59-61.

[12] ZHANG Xuefeng，FAN Jiulun. Extended Logistic Chaotic Sequence and Its Performance Analysis. [J]. TSHINGHUA SCIENCE AND TECHNOLOGY，2007，12（5）：156-161.

[13] J．Fridrich，Symmetric cipher based on two dimensional chaotic maps，International Journal of Bifurcation and Chaos，1998，Vol.8，No.6：1259-1284.