Open Journal of Applied Sciences
Supplement: 2012 world Congress on Engineering and Technology

Research on compound chaos image encryption method with clock- varying

MENG Xing[1], WANG XiaoMan[*], CHU Ying[1]
Department of electronics and communication
Chang Chun University of Science and Technology
Chang Chun,Jin Lin
meng_xing1987@163.com

Abstract—In this paper, we suggest one compound chaos image encryption method with time- varying multilevel initial parameters. This algorithm combines Subsection-linearity mapping, Chebyshev mapping with Logistic mapping in order to disturbing values of each image point and the array of original images based on chaotic second-scrambling way. The chaotic system uses time-varying system clock to change the first chaotic mapping initial parameter, and takes those chaotic sequences which generated by the first chaotic mapping as the initial parameters for the second chaotic mapping, then generate two-dimensional image pixel position scrambling matrix, and uses the same system clock to lock Chebyshev mapping initial parameter, then generate two-dimensional image pixel value transforming matrix. By this way for using the time-varying system clock, The encryption system can randomly changes many initial parameters of chaotic image encryption system to enhance image transmission security, has the capability of "one time one secret". The simulation results show that this algorithm is simple, safe, easy to achieve with software and has huge secret key space.

Keywords: Image encryption; Chebychev mapping; Logistic mapping; Secret key

1. Introduction

According with the rapid development of network technology and defense technology, digital image transmission and recognition in battlefield are more and more widely. Safety and high-efficiency encryption method has become hotspot topic. America meteorologist called Lorenz has originally lodged chaos theory. Chaos is the complexity movement patterns of a deterministic nonlinear system, it has too much useful characteristic, such as: good pseudo-random characteristics, unpredictability track, inherent randomness, the overall stability and local instability, extremely sensitive to initial conditions. Those excellent characteristics make it very easy to construct cipher system.

There are many different approaches for image encryption. Traditional methods for image encryption are based on cryptograph concept such as Data Encryption Standard (DES) [1] and Advanced Encryption Standard (AES) [2, 3].They consider image as a data sequence or stream and encrypt them byte by byte or block by block.

However, their encryption/decryption processes have huge computation complexity.

The principium of chaos encryption communication is that the sender disturb image information by using chaos signal in channel, this makes the image information like stochastic yawp. The receiver wipe off chaos signal and resume image information[4].This paper combines Subsection-linearity mapping, Chebyshev mapping with Logistic mapping and use system clock to control chaos system parameters, suggest one compound chaos image encryption method with time- varying, this method not only solves small key space and low security of chaos encryption system, but also makes the encryption system very complexity and highly stands against cipher attack capability, and attains "one time one secret".

2. Chaos Image Encryption Theory with Time- Varying Parameters

In this paper, use clock information to change initial parameters of compound chaos encryption system. For the sender, obtain the clock information, encrypt clock information by RSA system and send this information in common channel. At the same time, use time-varying clock to change multilevel parameters of chaos system and finish the image encryption. Cryptograph will be sent in secret channel to receiver. The Fig.1 is the encryption and decryption scheme.

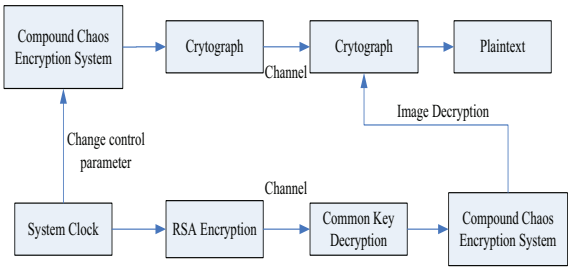


Figure 1. Chaos image encryption/ decryption principle with time-varying parameters

A. Compound Chaos Encryption System

Firstly we introduce three chaos models in this system.

1) Subsection-linearity mapping [5]

$$x_{n+1} = x_n / p \qquad x_n \in (0, p) \qquad (1)$$

$$x_{n+1} = (1 - x_n)/(1 - p) \qquad x_n \in (p, 1) \qquad (2)$$

When 0< p <1, the Lyapunov exponent is over zero and will happen chaos phenomena.

2) Logistic mapping [5]

$$x_{n+1} = u x_n (1 - x_n) \qquad (3)$$

In above equation, $0 \le u \le 1$, u is called control parameter, when 3.5699456< u <4, the system will go into chaos status.

3) Chebychev mapping [6]

$$x_{n+1} = \cos[k \arccos(x_n)] \qquad (4)$$

The definition range of this equation is (-1, 1), when the parameter k is equal to six, the Lyapunov exponent of Chebychev system is 1.7917333, so the mapping works in chaos status.

So, base on the above three chaos mapping, suggest chaos image encryption method with time-varying parameters. Fig.2 shows the process of image encryption and decryption of a simple chaotic system for this method.

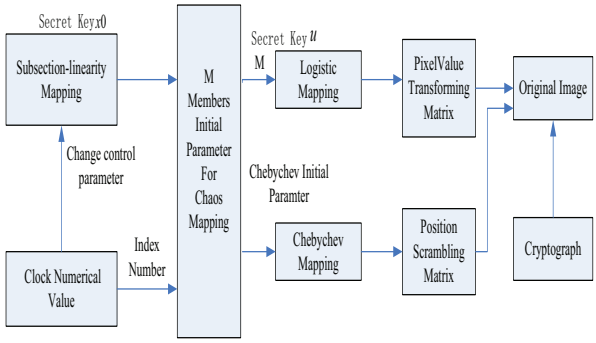


Figure 2. Compound chaos image encryption systemwith time-varying parameters

B. Compound Chaos Encryption Process

The main technology of this method describe in following.

Firstly, we use system clock information to disturb control parameter p of Subsection-linearity mapping, for the same secret x_0, the firstly Subsection-linearity mapping can be considered as many different models as to enhance chaos system capability for attack parameter p .The last, by using clock information to lock initial parameter of second chaos Chebychev mapping, it can enhance security exponent of encryption system, it means that when both the secret x_0 and control parameter p not change, the system clock can make index number difference ,then make two-dimensional image pixel value transforming matrix difference. By the above method, it makes chaos driver system more complexity, and achieves both pixel position scrambling matrix and pixel value transforming matrix changed in real time. Even the same image, if we encrypt it in different time, it will have different cryptograph. The following is the encrypt method, the system clock contains year, month, date, hour, minute, second.

The first step: change year, month, date into numerical value for hundred bit, ten bit, entries bit, and add those values, and map result for the value between zero and one. By the initial secret key, the Subsection-linearity mapping generates chaos sequence, the number of chaos sequences are the same as the row numbers (such as M) of image, and take those values as the initial parameters for Logistic mapping. For the Logistic mapping will be iterative of N detracting one times, and generate N sequences, and obtain $M \times N$ chaos sequences.

The second step: use the $M \times N$ chaos sequences which generate in the first step to obtain $M \times N$ bits matrix J according to the row first principle. Late, arrange the elements of J from the large to small, and generate matrix G by the row first principle. Then, we obtain one-dimensional pixel position scrambling matrix C by recording the position coordinate for the elements of matrix G in matrix J.

The third step: as the first step, make the hour, minute, second information to numerical values and add the integral part of those values and map the result for the value between zero and M. Then, take it as the one index number of M chaos sequences in the step one and take the value by this index number as initial parameter of Chebychev mapping. For the Chebychev mapping will be iterative of N times, and generate $M \times N$ chaos sequences, and change those chaos sequences to pixel value transforming matrix H by the row first principle. A last, system uses matrix H and matrix C to finish image two-dimensional encryption.

Decryption arithmetic is the symmetrical reverse process. Firstly, operate XOR between the gray matrix H and cryptograph image, obtain position transforming image P and use one-dimensional position transforming matrix C to transform image P. Then , we can decrypt original image.

3. Simulation Results

In this paper, all the results are simulated on image "cameraman.tif"(256×256) by using Matlab.For the encryption process, the values of system secret keys are as following: x_0 is equal to 0.17, u is equal to 3.581, k is equal to five, other is time-varying clock information. The clock information is obtained by the clock function in Matlab before the start of encryption arithmetic. For the encryption process, the system time is equal to

2011-5-15-10-05-45.234. For the wrong parameter decryption process, not change the parameter x_0, u and k, only make the initial parameter difference of Chebychev mapping by the clock information. The clock value is 2011-5-15-10-10-13.187 at the starting of decryption arithmetic. The Fig.3 shows the simulation results. (a) and (b) are corresponding to original image and cryptograph, (c) and (d) are corresponding to the histogram of original image and the histogram of cryptograph, (e) and (f) are corresponding to decryption image by right parameters and decryption image by the wrong parameters, (g) and (h) are corresponding to the histogram of decryption image by right parameters and histogram of decryption image by the wrong parameters .

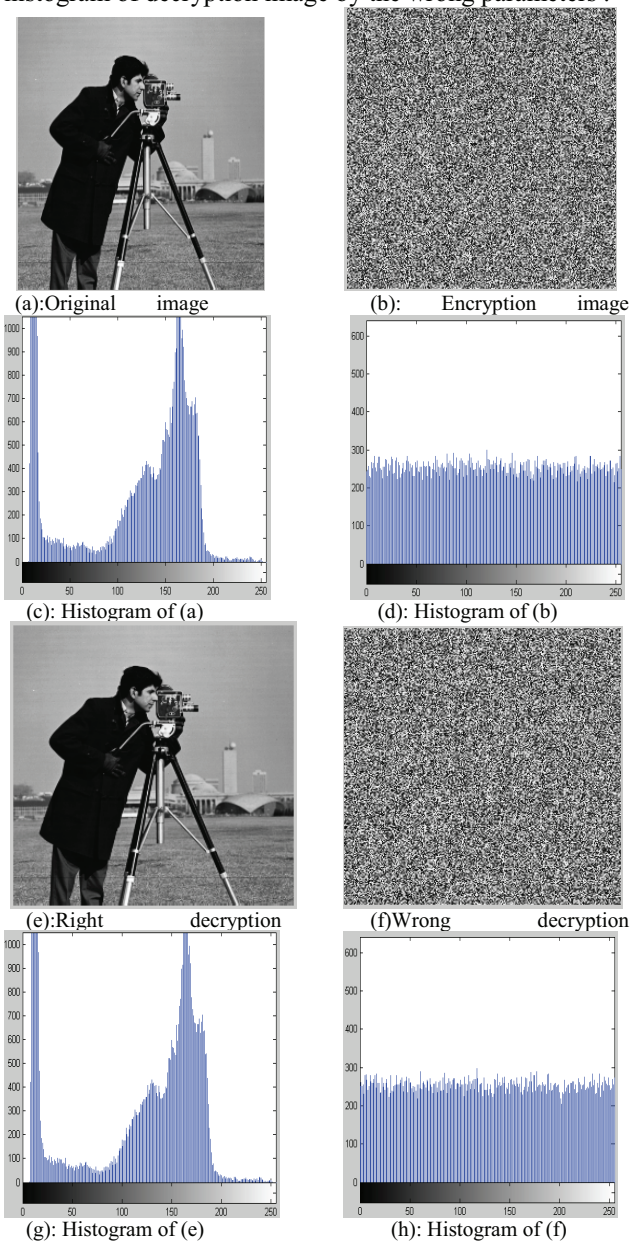


Figure 3. Image encryption / decryption simulation results

Form the above results, we can conclude that original image has been transformed and replaced and can not be seen clearly in frank. When use the right parameter encryption, the decryption image is the same as the original image, when the parameter has the little difference, the decryption image is very different from the original image.

4. Capability Analysis

A. Principle Analysis

In this system, use one-dimensional chaos mapping drive two two-dimensional chaos mappings and achieve to transform and replace. Comparing to literature[7,8], use time-varying clock information to change control parameter of one-dimensional chaos mapping, So, change chaotic parameter one time, it means replacing chaos equation one time. For one encryption process, not only change control parameter of one-dimensional chaos mapping, but also change the initial parameter of two-dimensional chaos mapping. Then it can enhance complexity of chaos sequence.

B. Secret Key Space and Secret Key Sensitivity Analysis

Secret key of this chaos system contains four members, initial parameter x_0 of Subsection-linearity mapping, control parameter u of Logistic mapping, control parameter k of Chebychev system and time-varying secret key(in this system is clock information).By this ,it can huge enhance secret key numbers and secret key space. The secret key space is many times than single one-dimension chaos mapping. It can fully resist infinitude attack.

Sensitivity analysis: an ideal image encryption algorithm should be sensitive to both the cryptic key and plaintext image. Change on one pixel bit in cryptic key or the plaintext will produce one different encryption image. It also means that the small difference on decryption cryptic key will not correctly decrypt the cryptograph image. In this system, only change clock information and obtain clock information before encryption algorithm start, one is 2011-5-15-22-7-48.218, another is 2011-5-15-22-14-23.203. Then compare two cryptograph images. Fig.4 shows the difference of two cryptograph images by the different secret key encryption. From the results, we can see that the cryptograph will be quite different by the little change on the secret key for the same original image. The more times results show that the cryptograph will be quite different even little change on the same secret key

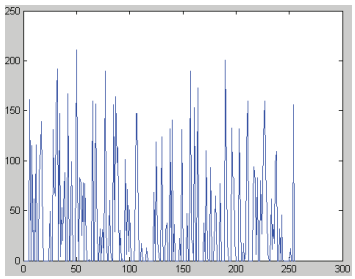


Figure 4. Pixel value difference distributing of two Ciphertexts

C. Histogram Analysis

The histogram is used for describing gray number of one image, it can give the statistical characteristic of one image. After comparing (c) and (d) of Fig.3, we can see that the pixels of original image are very asymmetric in all

Due to big secret key space, sensitive to the secret key, and strong statistical analysis of resisting the attack. Chaos image encryption technology has been widely used, and also reflected good encryption effect in practice. In this paper, describe one chaos image encryption method with the gray value, but the pixels of cryptograph image is very symmetrical in the gray value. So, the encryption algorithm destroys statistical characteristic of original image and fully diffuse and confuse cryptograph and plaintext.

D. Correlation of pixel

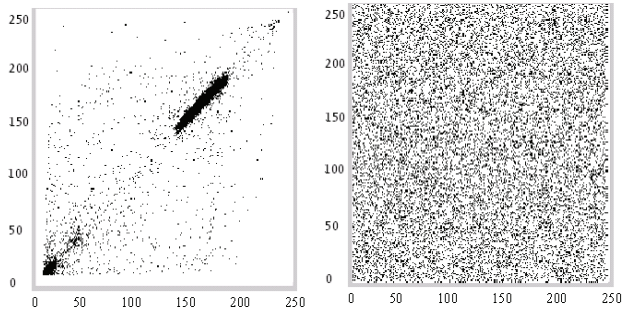
We also analyze the correlation of two adjacent vertical direction pixels, two adjacent horizontal pixels and two diagonal adjacent pixels of plaintext image and cryptograph image. There, analyze the correlation of original image 3(a) and cryptograph image 3(b). Analysis process is as following: Firstly, randomly select 16384 pairs of adjacent pixels from image. Then use the following two formulas calculating their correlation coefficients:

$$\operatorname{cov}(x, y) = E(x - E(x))E(y - E(y)) \quad (5)$$

$$r_{xy} = \operatorname{cov}(x, y) \Big/ \sqrt{D(x)}\sqrt{D(y)} \quad (6)$$

Where, x and y are the adjacent pixels of the image. Among the numerical value counting.

Fig.5 describes the correlation of two adjacent horizontal direction pixels of original image and cryptograph image. In the picture, the abscissa represents the pixels value of original and cryptograph in position (i,j), the y-axis represents the pixels value of original and cryptograph in position (i,j+1). At the same time, Table 1 gives the correlation of three directions. From the table1, we can see small correlativity of cryptograph, but high correlativity of original image.



(a): original image (b): Encryption image

Figure 5. Correlation of Horizontal Direction Adjacent Pixel

TAB.1 THE CORRECTION COEFFICIENTS OF PLAINTEXT IMAGE AND CRYPTOGRAPH IMAGE

Direction of Adjacent Pixels	Original Image	Cryptograph Image
Horizontal	0.9931	0.0307
Vertical	0.9806	0.0295
Diagonal	0.9685	0.0304

5. Conclusions

time-vary multilevel parameters. The outstanding characteristic is that use time-vary clock information to change many parameters of chaos system. It not only enhances secret keys and secret space, but also achieves the encryption requirement of “one time one secret”. The simulation results show that this algorithm is simple, safe, easy to achieve with software and has huge secret key space.

REFERENCES

[1] Zhang AiHua, Jiang ZhongQin. Improving for Chaotic Image Encryption Algorithm Based on Logistic Maping. Journal of Nanjing University Of Posts and Telecommunications (Natural Science).2009,29（4）: 1-2.

[2] National Institute of Standards and Technology, "Data Encryption Standard (DES)." 2001,http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[3]Hou Qibin and Wang Yangsheng, "Security traffic image transmission based on EZW and AES," in Intelligent Transportation Systems.2003. Proceedings. 2003 IEEE, 2003, 1(1) :86-89.

[4]Chen Ling , Pan ZhongLiang. An Encryption Method for Color Images Based on Logistic and Henon Chaotic Systems. Equipment making technic. 2010:1-4.

[5]Huang Hao,Huang RuiSheng, “Chaos and Application,” Wu Han University Press,2007.

[6]Zhang YunPeng, Zuo Fei, Zhai ZhengJu. A Color Image Encryption Algorithm Based on Chaotic Chebychev and Variable-Parameters Logistic Systems. Journal of No~hwestem Polyteehnical University. 2010 , 28(4):3-4

[7]YANG Fan, XUE Mo-gen. Research on digital image encryption algorithm based on compound chaotic image

second-scrambling. Journal of He Fei University of Technology. 2009, 32(8):4-5.

[8]Zhou Zhigang, Li Su-gui. Digital image hiding technology based on chaotic system with variable parameters. Journal of Computer Applications. 2009, 29(7) :2-4.

[9]Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah. An Efficient Chaos- Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption .Information. 2007:121–129 .

[10]Yicong Zhou, Karen Panetta, Sos Agaian. ImageEncryption Based on Edge Information. Proc. of SPIE-IS&T Electronic Imaging.SPIE-IS&T/ Vol. 7256 725603-1.

[11]Fethi Belkhouche,Ibrahim Gokcen, U. Qidwai. Chaotic gray-level image transformation. Journal of Electronic Imaging.2005,14(4).

[12]Mohamed Amin. Efficient modified RC5 based on chaos adapted to image encryption. Journal of Electronic Imaging.2010,19(1).