Perception image harsh protection based on chaos theory

Chang Liang[1, a], Chang Jiang[2] and Wang Wen-de[3]

[1] Information and electronic technology institute of Jiamusi University, China

[2] Mechanical engineering institute of Jiamusi University, China

[3] Application of electronic technology institute of Jiamusi University, China

[a]chang-liang1980@163.com

Keywords: chaos theory; image protection; perception harsh; encryption matrix

Abstract. With the development of the internet and computer technology, the image protection becomes more and more important. In order to strengthen the robust and safety of the image protection , this paper mainly improve the encryption algorithm of harsh sequence and propose the theory of using chaos theory to encrypt the image protection through analyzing the basic feature of the chaos theory. It also proposes new image protection solution by using encryption matrix methods, Pseudo random sequence block and image scrambling method in the image protection experiment. The experiment shows that these methods have better usefulness, safety and versatility which can satisfy the needs of image data encryption and image safety.

Introduction

With the spread and application of computer and internet technique, the information safety becomes the focus of the people. Image protection is one of important issue resulting from the development of information era[1].

The image protection is a process of encrypting the image data. There are mainly two kinds of encryption algorithm, one is the password analysis and the other is password design. In the password design, it can be fatherly divided into traditional password and chaos password [2]. The representative of traditional password is DES/IDEA/AES and so on which are mainly based on number theory. The chaos password is based on the initial value sensitivity to produce the password [3].

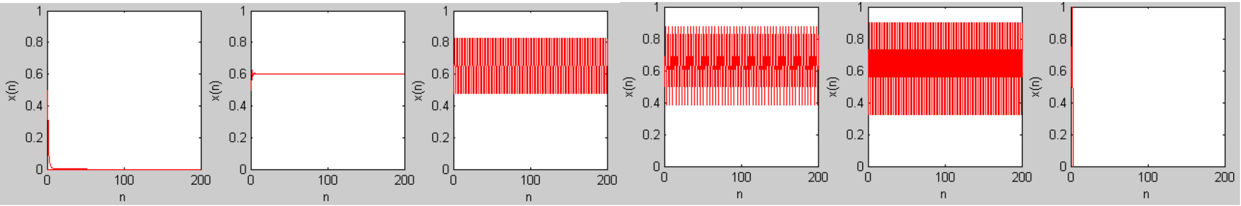
The essential qualities of the chaos theory

Chaos phenomenon is the certainty and similar random process arisen in the non-linear dynamical system. Such a process is neither cyclically nor convergence and dependency to the initial value and sensitivity [4].

The following is the Logistic mapping in the chaos dynamic system:

$x_{i+1} = \mu x_i (1 - x_i)$ $0 \le \mu \le 4$ ----branch parameter $x_i \in (0,1)$

The following is the function changing situations when μ take different values. Four situations 0~1、1~3、3~4 and more than 4 are taken separately, the experiment is denoted as figure 1.



μ=0.5 μ=2.5 μ=3.3 μ=3.5 μ=3.6 μ=4.4

Figure 1. the Logistic mapping chaos model when μ take different values

Published by Atlantis Press, Paris, France.

From figure 1, we get that when $3.5699456\cdots\cdots < \mu \le 4$, Logistic mapping work in chaos. Through simple transformation, Logistic mapping can be defined between (-1, 1) as denoted in Eq. (2).

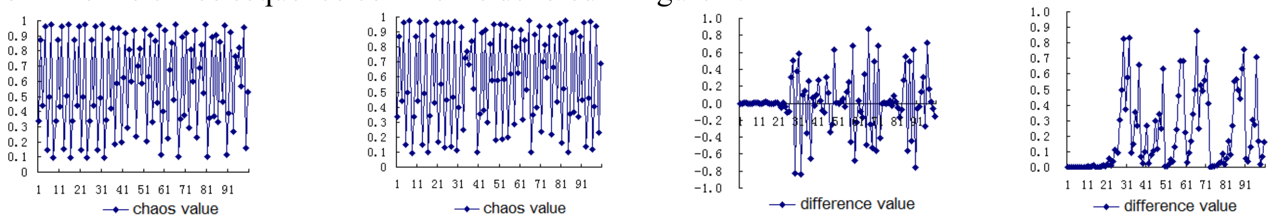
$$x_{i+1} = 1 - \lambda x_i^2 . \ \lambda \in (0,2) \qquad (2)$$

When the surjection $\lambda = 2$, the PDF (Probability Density Function) of Logistic mapping sequence is denoted in Eq. (3).

$$\rho(x) = \begin{cases} 1 \big/ (\pi\sqrt{1-x^2}), & -1 < x < 1 \\ 0, & else \end{cases} . \qquad (3)$$

Through calculating $\rho(x)$, we can get the statistic character of the chaos sequence generate from Logistic mapping [5].

According to the initial value sensitivity of chaos sequence, take the initial value 0.3366 and 0.3367 to make the chaos sequence contrast as denoted in figure 2.



(a) (b) (c) (d)

Figure2. initial value sensitivity testing chart of chaos sequence. (a) Chaos sequence figure with initial value 0.3366 (b) Chaos sequence figure with initial value 0.3367 (c) Difference value chart of two chaos sequences (d) Positive change difference value chart of two chaos sequences

Chaos sequence generate from the mixed optical bistable model, the model[6] is as follows:

$$x_{n+1} = A\sin^2(x_n - x_B) . \quad (4)$$

When A=4, x_B=2.5, this formula is in chaos, we can get different chaos sequence with different initial value x_n .

Image protection method based on chaos sequence

Method based on encryption matrix

Take the Logistic mapping as the example [7], and generate $n \times n$ encryption matrix A. The image itself is a two-dimension matrix, suppose it as $m \times m$ dimension matrix B among which m is the multiple of n. Therefore, image matrix B can be divided into k $n \times n$ matrix blocks $B_1, B_2, ..., B_k$.

$x_{i+1} = \mu x_i (1 - x_i)$ is the chaos sequence generator, μ takes 3.9,the initial value takes 0.3255. Multiply matrix A with $B_1, B_2, ..., B_k$ respectively in matrix B to get encryption matrix G.

$$G_i = A \times B_i \ (i = 1,2,...,k)$$

Advantage of this method: calculating speed is fast and simple. Disadvantage: the encryption matrix generated from the chaos sequence is not sensitive to the initial value at the very beginning that is the difference between encryption matrixes generated from different initial value is not great. Therefore, when the encryption matrix dimensionality is very tiny, it is too easy to crack; the blocking effects are easily come out because of the block encryption to the image matrix.

The method based on Pseudo random sequence block

Just like the above thought that encryption images in blocks. First, take the image as a matrix B and generate pseudo random number K according to secret key. Divide the image into random overlap-able m image area blocks in line with K. Then recombine m area blocks and encrypt each block with encryption matrix A, a new encryption image data blocks is generated.

The generation of secret key can be preset by the user or extract according to the image. Such as compress the image B into b with DCT, and generate secret key through the value of b as denoted in figure 3.

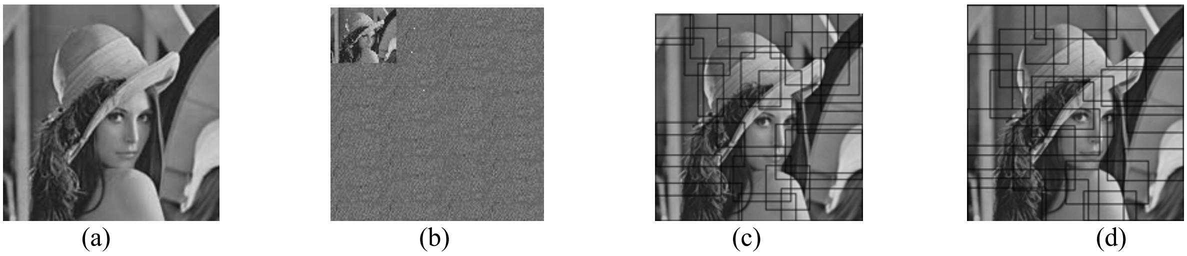


Figure3. Extract the value of key in the image. (a) The image of testing. (b) The image of extracting the value of key. (c) The rendering image generated from secret k_1 in blocks. (d) The rendering image generated from secret k_2 in blocks.

Divide the image in accordance with the value of key, (c) and (d) in figure 3 is the block situation of image under different key values.

The method based on image scramble

First suppose image matrix D as $M \times N$ dimension, M is the row vector number, N is the line vector number. Shifting randomly every row in the row vector and the random shifting number K can be generated from chaos sequence. Similarly, shift randomly the line vector accordingly to generate new matrix D after the image scramble. It also use chaos sequence to generate random unit matrix A and B, make use of the image matrix multiply A at left and B at right to achieve vector shifting and generate scramble image matrix D.

The encryption matrix S generated by chaotic sequences is $m \times n$ dimension, encrypted the Scrambling matrix $D^{'}$, $D^{''} = S \times D^{'}$ and $D^{''}$ is the new encryption matrix.

The advantage of this method is that it has good quality of hiding plaintext and has good secret key safety, anti aggression and good practicability. The disadvantage is that because using iteration to achieve scramble that the encryption ratio is low, the calculating time is long.

The test result of encrypting the image with image scramble method is denoted in figure 4.

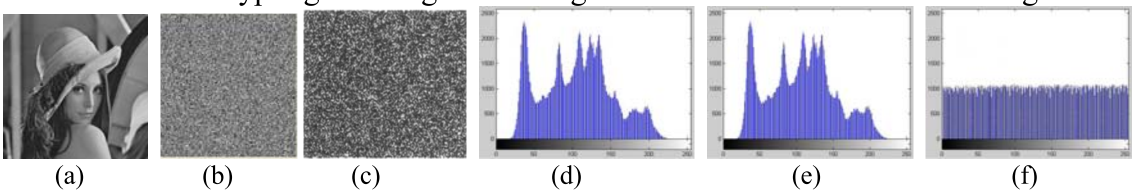


Figure4. Image scramble and encryption test rendering. (a) Original image(b) Image after scramble(c) Encryption image(d) Original image histogram(e) Scramble image histogram(f) Encryption image

Method base on high-dimension chaos sequence

As the above three image encryption methods can only achieve encryption to gray image and secret key room is too small. The high-dimensional chaos sequence encryption is proposed with the core is high-dimensional chaos model. The following are two usual high-dimensional chaos models.

The high-dimensional chaos system has good random quality, unpredictability, security and safety. Moreover, it has high encryption efficiency and reduces the calculating volume. Compared with the traditional chaos system, the sequence generated from this method is more difficult to predict and crack.

Conclusions

This paper mainly studies the improvement of the harsh sequence encryption algorithm and after analyzing the basic feature of the chaos theory the image protection encryption based on it is proposed. And through the encryption matrix method, pseudorandom sequence block method and image scrambling into the image protection experiment, a series of image protection formula is proposed. The experiment result tests that these methods have better practical applicability, safety and flexibility which can satisfy the demand of image data encryption and protect the image fatherly.

Acknowledgment

This work is supported by Science and Technology Research of Heilongjiang Province Educational Committee under Grant No. 12513090.

References

[1] C.Soutar, Security Considerations for the Implementation of Biometric Systems: N.Ratha and R. Bolle (Eds.), Automatic Fingerprint Recognition Systems, Springer, (2004), p. 415~431.

[2] Moon D, Gil Y, Ahn D, Pan S, Chung Y, Park C. Fingerprint-Based authentication for USB token systems. In: Chae K, Yung M, eds.Proc.of the WISA 2003.LNCS 2908, Berlin: Springer-Verlag, (2004), p. 355~364.

[3] G.I.Davida, Y.Frankel, and B.J.Matt. On enabling secure applications through off-line biometric identification,in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, p. 148-157,Oakland,Calif,USA, (1998)

[4] A.Juels and M.Wattenberg,A fuzzy commitment scheme,in proceedings of 6th ACM Conference on Computer and Communications Security(ACM CCS'99),PP.28-36,Singapore,November1999.

[5] F.Hao, R.Anderson, and J.Daugman, Combining crypto with biometrics effectively, IEEE Transactions on Computers,vol.55, no.9, p. 1081~1088, (2006)

[6] P.Tuyls, A.H.M.Akkermans, T.A.M.Kevenaar, G-J.Sehrijen, A.M.Bazen,and R.N.J.Veldhuis, Practical biometric authentication with template Protection, in Proceedings of the 5th International Conference Audio-and Video-Based Biometric Person Authentication (AVBPA'05), vol.3546 of Lecture Notes in Computer Science, p. 43-446, Hilton Rye Town,NY,USA, (2005)

[7] A.Juels and M.Sudan, A fuzzy vault scheme, in Proceedings of the IEEE Imitational Symposium on Information Theory, p. 408,Piscataway,NJ,USA, (2002).

Published by Atlantis Press, Paris, France.