International Journal of Latest Research in Science and Technology **ISSN (Online):2278-5299**
Volume 2, Issue 5: Page No.32 -36 ,September-October 2013
https://www.mnkpublication.com/journal/ijlrst/index.php

RESEARCH ON IMAGE ENCRYPTION ALGORITHM BASED ON WAVELET TRANSFORM

[1,2] **Yunpeng ZHANG*,** [1]**Wenquan LV,** [1]**Renjie ZHAO,** [1]**Ding YU**
[1]College of Software and Microelectronics, Northwestern Polytechnical University, Xi'an, 710072, China.
[2]CMR Unit, Imperial College London, London, SW3 6NK, U.K

Abstract- A Chaotic Image Encryption Algorithm based on existing image scrambling encryption algorithm. Before encrypting, the authors scramble image to reduce the correlation of pixels of the original image, then, encrypt images, and the deciphering process is on the contrary. Experimental results show this Algorithm can effectively overcome the short cycle effect and good PN character of the only logistic mapping under the influence of limited accuracy, which is effective.

Keywords - Wavelets transform, chaos encryption, image encryption

INTRODUCTION

With the rapid development of Internet technology, In society today, digital multimedia information has been widely spread through the network, and at the same time, the network safety becomes a cause of concern day by day, because it involves privacy, commercial interests and even state secrets, etc. the image is an important information transmission media. With the development of multimedia and network, not only lots of image transmission are required, but it is required that quality premise with less space to store images, and a low bit rate to transform images. Uncompressed digital image information is too large, so we'd better use ascertain method do image compression, which is convenient for image storage and image transmission. Doing reliably processing of digital images of transmission encryption, has become one of important research directions in the current information encryption area. The traditional cryptography focus on the encryption process of text material, which provides the most straightforward theory basis for digital image encryption technology, but its object, is binary data flow, the image digital production and visual effect ignored. Meanwhile, as digital image data is large, real-time is required when encrypting, which is difficult for the traditional encryption approach to achieve. The chaotic system has a false randomness and rail unpredictability, and is extremely sensitive for the initial value and the parameters. So the chaotic encryption technology based on the chaos theory is especially suitable for image encryption. At present, the image encryption technology based on chaotic technology becomes a frontier technology in the encryption field.

Another characteristic of the image is the large quantity of data, for this reason, the space and time complexity of image encryption is difficult to achieve the desired degree. Image Data Compression is mainly used for the image compression to save storage space. I think that the Image Data Compression can be applied to encryption algorithm. The algorithm in this article is to do image compression processing first and then do new chaotic encryption algorithm encrypting, the advantage of which is to reduce the amount of data of encryption, so as to save the space and time complexity of the algorithm, to improve the efficiency of the encryption.

Yen and Guo proposed CKBA encryption algorithm [1]. In 2002, Li and Zheng had pointed out some shortcoming in the literature [1] and discussed some possible corrective method [2]. In 2004, Chen et al. proposed one symmetrical image encryption algorithm [3]. The authors of literature [4] talk about that they are difficulty to resist the known certain attack.

SOME COMMONLY USED CHAOS MAPPING

1. Chebychev Mapping.

Chebychev mapping is a mapping method of simple form, and the Chebychev mapping with k order can be expressed as follows:

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

When the parameter k=6, the Lyapunov index of Chebychev system is 1.791733... , mapping is in a mess. The Chebychev system has strong sensitive dependence on the initial state. After a few steps of evolution, two tracks setting off from the adjacent initial values of x_0 = 0.20000 and x_1 = 2.0001, become obviously different.

2. Henon Mapping.

Henon, as a two-dimensional mapping, is the simplest mapping of high dimensional nonlinear mapping, the mathematical formula of which is:

$$\begin{cases} x_{n+1} = 1 + by_n - ax_n^2 \\ y_{n+1} = x_n \end{cases} \qquad (2)$$

Publication History
Manuscript Received : ***24 October 2013***
Manuscript Accepted : ***27 October 2013***
Revision Received : ***28 October 2013***
Manuscript Published : ***31 October 2013***

When a is 1.4, b is 0.3, the system approaches to the chaos state. What Fig.1 shows is the Henon mapping of chaotic attractor.

In particular there is an inverse mapping decided by the monodrama in the Henon mapping, which is:

$$\begin{cases} x_n = y_{n+1} \\ y_n = \dfrac{1}{b}(x_{n+1} + a y_{n+1}^2 - 1) \end{cases} \quad (3)$$

3. Logistic Mapping.

Logistic Mapping i.e. population model, which is a kind of chaos mapping being studied widely at present. The meaning of Logistic mapping can be Explained as follows: When a single species of insect breed from a certain range , the number of offspring is far greater than the number of parents, so we can deem after the offspring was born the number of the parents can be ignored. Assuming x_n is the number of a certain species of insect in the nth year, the number and the year are relevant. 'n' is only numerical, so in the (n + 1)th year the number is x_{n+1}[5].

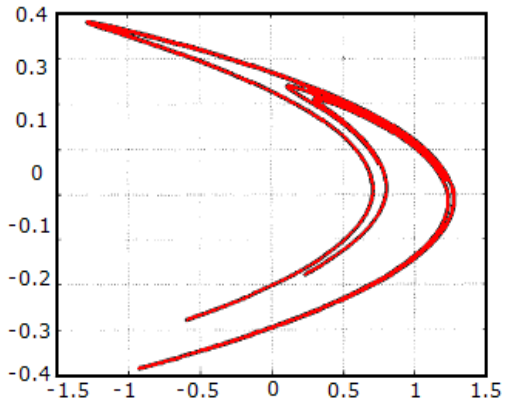


Fig.1 Attractor of Henon mapping (p = 1.4, q = 0.3)

The mathematical expression of one-dimensional Logistic mapping is as follows:

$$x_{n+1} = \mu x_n(1-x_n) \quad n \in \{1, 2, \ldots\} \qquad (4)$$

Among them, $0 \leqq x \leqq 1$,μ is the control parameter，$0 < \mu \leqq 4$

When $0 < \mu \leqq 1$, this system has a constant solution 0 (i.e. when the initial value is 0, the sequence created will be all 0), and no matter what the initial value is, through multiple iteration, the sequence will ultimately converge to 0.

When $1 < \mu \leqq 3$, the constant solution is 0 and $1 - 1/\mu$, through multiple iteration, the sequence will converge to either of the two values.

When $3 < \mu \leqq 4$, the system approaches to chaos by Period-Doubling. Especially, when $3.5699456... < \mu \leqq 4$, the system approaches to the chaotic state and the value created iteratively is in a pseudo random distribution state. What's more, the closer μ is to 4, the stronger the chaotic property is. When $\mu = 4$, the Lyapunov Index of Logistic mapping is ln2 = 0.6931.

IMAGE SCRAMBLING ENCRYPTION

Scrambling technology is doing substitution for the position space of analog image in the early time , and as for the digital image, scrambling encryption process can not only proceed in the space (including position space and color space) domain of digital image , also in its frequency domain and space-frequency domain. In this paper before the image is encrypted by double chaotic system substitution, do image scrambling to reduce the correlation of pixels of the original image. Literature [6] points out that the scrambling encryption before the airspace substitution encryption can conceal the scrambling encryption information, and enhance the scrambling capacity against attack.

If encrypting image Source image is $I_{W \times H}$, W is the width of the image, H is the height of the image, gauged by pixels. A pixel P in the image is composed by three pieces of eight bits. In the process of studying in this paper the Chebychev chaos mapping is used and the address mapping table is gotten by sorting chaotic sequence. The scrambling procedure in this paper is as follows:

Step1. Let Source_image as an input and store it in the two dimensional array P [W] [H].

Step2. Initial Key key1 is input by the user and the Chebychev chaos mapping is iterated W times, drawing the chaotic sequence { X_a}（a=0，1…W-1）.

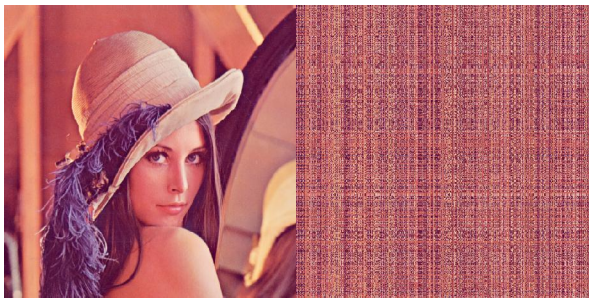
Step3. Initial Key key2 is input by the user and the Chebychev chaos mapping is iterated H times, drawing the chaotic sequence {X_b}（b=0，1…H-1）.

Step4 Sort the chaotic sequence { X_a } by size, getting a chaotic sequence { X'_a }, and then get the address mapping table according to the changes of the position of the element from the two chaotic sequences.

Step5 Sort the chaotic sequence {X_b} by size, getting a chaotic sequence {X'_b}, and then get the address mapping table according to the changes of the position of the element from the two chaotic sequences.

Step6. By the Rows and Columns of address mapping table, let each pixel P (x, y) of the original image map to a new position P (x', y')

According to the scrambling algorithm, the effect is shown in fig. 2.



(a) Original image (b) Scrambled image

Fig.2 Effect of the scrambling algorithm

(a) Scrambled image (b) Anti-scrambling image

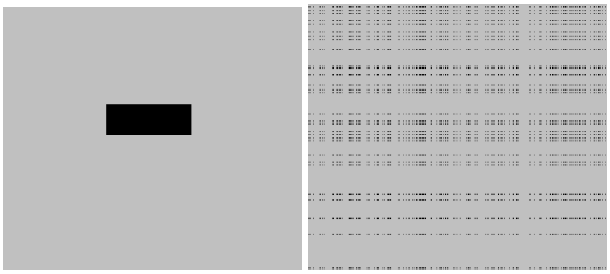
Fig.3 The anti-scrambling rendering of the scrambling algorithm

The Fig.2 (a) is the original image; the Fig.2 (b) is the image scrambled original image. We can see from them, the images scrambled obviously show some horizontal lines and vertical lines, and a certain law. The scrambling effect of the above algorithm is not ideal. In order to get the disadvantages in it, the author made a special image scrambling effect as follows:

IMAGE ENCRYPTION ALGORITHM BASED ON WAVELET TRANSFORM

1. scrambling algorithm

As we can see from Fig.4, the black part in the right image is regularly dispersed in the whole picture. According to the scrambling algorithm, a pixel in a line may be substituted to any position of this line, but the scrambling range is limited to one line. So, the effect of the scrambling algorithm is substituted in a unit of l Rows or Columns. The unit is obviously too large, causing laws in it. In order to avoid this, the author made the following improvement: store the original image Source_image in one dimensional array P [W×H], and only one address mapping table need generating. When scrambling is completed, restore the image to the 2 d image. The procedure of new scrambling algorithm is as follows:



(a) Original image (b) Scrambled image

Fig.4 Scrambling rendering of the special image

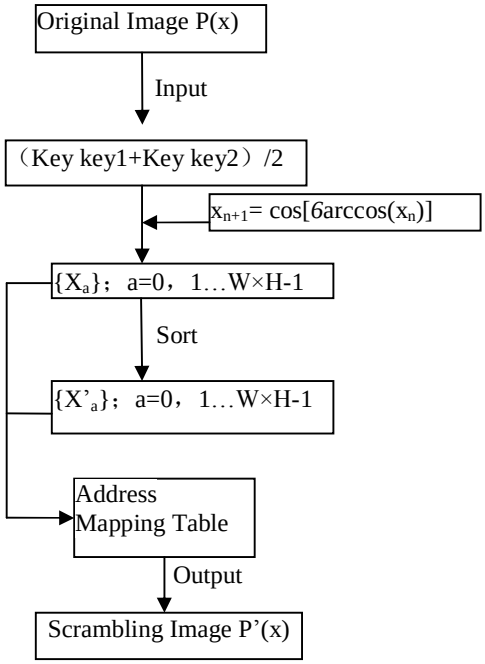


Fig.5 The flow chart of the new scrambling algorithm

Step1. Let Source_image as an input and store it in the one dimensional array P [W] [H].

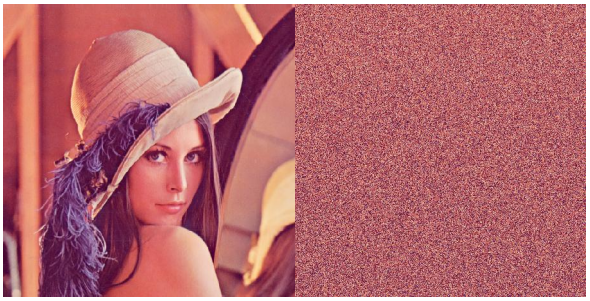
Step2. Initial Key key1 and key2 is input by the user and the Chebychev chaos mapping is iterated W×H times, drawing the chaotic sequence {X_a}（a=0，1…W×H -1）.

Step3. Sort the chaotic sequence {X_a} by size, getting a chaotic sequence {X'$_a$}, and then get the address mapping table according to the changes of the position of the element from the two chaotic sequences.

Step4. According to the address mapping table, let each pixel P (x, y) of the original image map to a new position P (x'，y')

Step5. The flow chart of the new scrambling algorithm is shown in Fig.5.

The scrambling effect of the new scrambling algorithm, rendering of decrypting the new scrambling algorithm, and new scrambling rendering of the special image is shown in Fig.6-8.

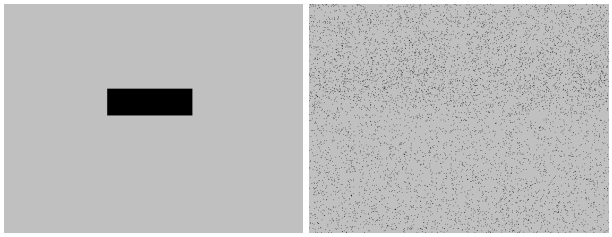


(a) Original image (b) Scrambled image

Fig.6 Rendering of the new scrambling algorithm

(a) Original image (b) Scrambled image

Fig.7 Rendering of decrypting the new scrambling algorithm



(a) Original image (b) Scrambled image

Fig.8 New scrambling rendering of the special image

Chaotic encryption of image

If encrypting image Source_image is $I_{W\times H}$, W is the width of the image, H is the height of the image, gauged by pixels. A pixel P in the image is composed by three pieces of eight bits. In this paper the value of double precision key_1~ key_5 is adopted as keys and input by users at the beginning of the encryption. The procedure of encryption is as follows:

Step1. The user input the 5 keys key_1~ key_5.

Step2. Let the gray value of the pixel in image Source_image be a 2 d matrix $P_{(x, y)}$. And transform it to a one d pixel array $P_{(h \times x + y)}$, namely P_0, P_1, P_2, P_3,... P_n, including n = w × h. let the above be a sequence $\{P_i\}$.

Step3. Input key_1 and key_2, key_1, $key_2 \in (1, 1)$. Scramble the Source_image and output the scrambling sequence $\{P'_i\}$.

Step4. Input key_3, key_4, key_5, key_3, $key_4 \in (1, 1)$, $key_5 \in (3.6, 4)$ as the initial key of the double chaotic system. First, use the chaotic sequence generated by key_3 and key_4 through Henon chaotic mapping. Take the decimal part of the numerical value in the chaotic sequence as the first Logistic chaos mapping X_n input. Key_5 is the original value of the parameter μ, thus iterating double chaos with combination. In this system iterative W * H * 2 times, generating chaotic sequence $\{X_c\}$. Later, divide $\{X_c\}$ into even sequence $\{X_{ci}\}$ and odd sequence $\{X_{cj}\}$.

Step5. Take the decimal part of the numerical value in the sequence {Xcj} and the sequence of the image scrambled is $\{P'_i\}$. By transforming formula:

$$\mu=（4-\mu_{min}）* (P'_j/255)* |X_{cj}|+\mu_{min};;\ \mu_{min}=3.57$$

Reach the sequence $\{\mu_i\}$. P'_j, j=（i+1）MOD（w×h），i=0，1…w×h-1.

Step6. Take the decimal part of the sequence $\{X_{ci}\}$ and reach a sequence $\{\mu_i\}$ as a parameter of the second Logistic mapping input. Then iterate n times, reaching a chaotic sequence $\{X_d\}$.

Step7. After taking the decimal part of each element in the sequence $\{X_d\}$, magnify 28 times and take mod of 256.Then do XOR operations with the corresponding elements in the $\{P'_i\}$.At last, reach the encrypting image.

The process of decryption is the inverse of the process of encryption.

EXPERIMENTAL RESULTS AND ANALYSIS

Input key (0.52, 0.32, 0.2, 0.6, 3.74), the crypto map reached by the chaotic image encryption algorithm based on the wavelet transform in this paper is the right image. As shown in Fig.9, it is obvious that encrypting results of the image present uniform chaos sequence in a style of carpet and the original information cannot be identified.

(a) Original image (b) Encryption image

Fig.9 Experimental result of encryption algorithm

A lot of chaos mapping is multiply used in this paper. So the key space is huge. On the assumption that the precision of the computer is 10-8, the estimated result of the key space is 3.2×1040. Using this algorithm, encrypting Image Lena one time needs 9.547 seconds. If the key space is calculated with 3.2×1040, one-time exhaustive attack need $9.547\times3.2\times1040=30.5504\times10^{40}$ seconds, about 9.6×10^{33} years. It is thus clear that the intension of this algorithm can resist the exhaustive attack effectively.

Affected by the finite precision effect, the chaotic binary sequence generated by Logistic Mapping will perform a minor-cycle act. Its ACF will emerge divided peak value, no longer a δ-like function. We use the Iteration output generated by Heono chaos system(and the values are chosen randomly) as the parameter of Logistic Mapping, which remarkably increases the variation of μ, thus, increases the subsequence cycle of Logistic Mapping. The test proves that the key subsequence generated by this algorithm successfully fixes the minor-cycle effect in Logistic Mapping, and with good PN character. What's more, the safety of Logistic Mapping largely relies on the randomness of key sequence, theoretically, if the key sequence is perfectly random and as long as the plaintext, this cipher will be completely undisciphered [7]. This algorithm provides well pseudo-random key stream, for which reason the encryption scheme based on this algorithm have a good anti-attack capability. The encryption scheme presented in this text also performs well in defending attacks based on phase space reconstruction,

which proves the feasibility of this encryption scheme in practical application.

CONCLUSIONS

Among digital image compression technologies, the compression technology based on wavelet transform has high compression ratio, high efficiency and other features. So in the field of digital image encryption technology it has a considerable development in the last ten years.

In this paper I sketch the digital image compression technology based on the wavelet transform and the digital image encryption technology based on the chaotic system and applies the compression technology to the encryption technology on the basic of the summarizing. The new algorithm combines the mature chaos mapping systems and design ideas at present, and did some creating. The algorithm of image scrambling and gray change in this paper are based on the chaotic system and two encryption schemes are combined organically, making the effect of encryption better, which meets the higher standard in security.

ACKNOWLEDGEMENTS

This work was supported by the Fly Star Fund of North western Polytechnical University(2011).

REFERENCES

[1] J.C. Yen, J.I. Guo, *A new chaotic key based design for image encryption and decryption[C]*. Proceedings of the IEEE International Symposium Circuits and Systems, 2000, 4: 49–52.

[2] S. Li, X. Zheng, *Cryptanalysis of a chaotic image encryption method[C]*. Proceedings of the IEEE International symposium on circuits and systems, Scottsdale, AZ, USA, 2002.

[3] Kwok-Wo Wong *, Sun-Wah Ho, Ching-Ki Yung *A chaotic cryptography scheme for generating short ciphertext [J]*. Chaos, Solitons and Fractals, 2004, 3(21): 749-761.

[4] Banks J., Brooks J., Cairns G., Davis G.& Stacey P., *On Devaney's definition of chaos[J]*, Amer. Math. Monthly, 1992, 99:332-334.

[5] Pareek N K, Patidara V , Sud K K. *Discrete Chaotic Cryptography Using External Key[J]* . Physics Letters A ,2003 ,309 :75 - 82.

[6] J.C. Yen, J.I. Guo, *A new image encryption algorithm and its VLSI architecture[C]*. Proceedings of the IEEE workshop signal processing systems. 1999: 430-437.

[7] Richard Spillman . *Classical and contemporary cryptology[M]* . Ruanjian Ye, Ying Cao, Changfu Zhang, etc, translation. Beijing: Tsinghua University Press，2005，1-23.