International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.241-250
http://dx.doi.org/10.14257/ijsia.2016.10.12.19

A New Kind of Image Encryption Algorithm based on Improvement Bit Plane

Honge Ren[1, 2], Xiyan Xu[1], Jian Zhang[1, 2*], Yali Chen[1]

[1]*College of Information and Computer Engineering, Northeast Forestry University, Harbin, Heilongjiang, 150040, China*
[2]*Forestry Intelligent Equipment Engineering Research Center, Harbin, Heilongjiang, 150040, China*
*nefu_rhe@163.com, 1773521007@qq.com, *zhangjianok00@163.com*

Abstract

The paper presents a new Image Encryption Algorithm. First of all, we utilize the common plane analysis process and Logistic to generate seven groups of chaotic sequence of different range value, and then, the order of the "exclusive or" of Scrambling Figures in the plane analysis of 8 groups different information content was determined by the generated Chaotic sequences with different range values and the information in Bit Plane Analysis. We use 7 groups of different values of every Logistic and select the corresponding pixels of different groups to process 'exclusive or' operation, in the end we will get encrypted image. Decryption is the inverse process of encryption. This Algorithm implementation is simple, and due to the generated different chaotic sequence, this algorithm has large key spaces. Other than that, the experiment verifies that new Image Encryption Algorithm is free from the histogram, plain text attack, etc.

Keywords*: image encryption; scrambling; chaotic; Logistic*

1. Introduction

With the rapid development of computer technology, protection of digital images illegal copying and distribution has become more and more important .Utilizing the merits of chaos-system to protect image security is a research hot point. The chaos-based image encryption algorithm in [1-4] includes two phases: First, the pixel positions of the permuted image are encrypted by a chaotic system. The algorithm has lots of merits, such as the sensitivity to the secret keys and the large key space. Beside, compared to the common direct pixel scrambling and chaotic spread, the bit plane encryption realize scrambling effect at the same time, also has carried on the encryption processing [5].

In this paper, according to a common bit plane encryption, we combined with chaos characteristic and digital image itself, and put forward a new kind of image encryption algorithm. First of all, we use the ideas of NCA chaotic to scramble image, then process binary decomposition and conduct 8 groups.

Using Logistics chaotic thoughts conduct different range of value chaotic sequence, and finally we use 8 image and chaotic sequence and select different group "exclusive or" operation their own group decomposition matrix, and get the final encrypted image. This paper use classical woman image and Lena image to demonstrate the superiority of the algorithm, this algorithm has a large amount of key space and can resist various attacks.

2. NCA Scrambling and Bit Plane Decomposition

Conventional digital image encryption algorithm is generally the use of the digital image itself pixel to "exclusive or" encryption, the method is simple, but there is a

ISSN: 1738-9976 IJSIA

potential safely hazard, easy to be cracked. So we first carried out on the digital image over the NCA scrambling operation, then a binary decomposition, divided into eight groups. In general, image data between adjacent images have very strong connected, so this paper uses the NCA scrambling plane image to disturb the high correlation between pixels.

The specific procedures of nonlinear chaos algorithm process are as follows:

From left to right and top to bottom, we transform two-dimensional image to one-dimensional image $P1(i), i = 1, 2, ..., N \times N$ .Starting from certain initial condition x_0 and parameters α, β , after iterated K times, we continue to iterate the above $N \times N$ times, where $x_i \in (0,1), i = 1, 2, ..., N \times N$.

3. In this time, X include original image of NCA scramble, Transform $P2$ to encryption image base on the inverse processes of step1.

For scrambling image $P2$,Matrix as $B(M, N)$, And for matrix $B(M, N)$,each element has binary decomposition,, the decomposed matrix is extended to 3dimension $C(M, N, 8)$ .In this time, the end of dimensionality the 3 d matrix C preserved the original image gray value of the binary representation, for three-dimensional matrix, according to the last dimension is divided into eight groups of two-dimensional matrix.

$C(M, N, 1)$, $C(M, N, 2)$, $C(M, N, 3)$, $C(M, N, 4)$, $C(M, N, 5)$, $C(M, N, 6)$, $C(M, N, 7)$, $C(M, N, 8)$, Each Matrix express image gray value of the different weight decomposition ,and different matrix on behalf of the image are binary image, for example ,classic Lena ,as shown in figure 1.

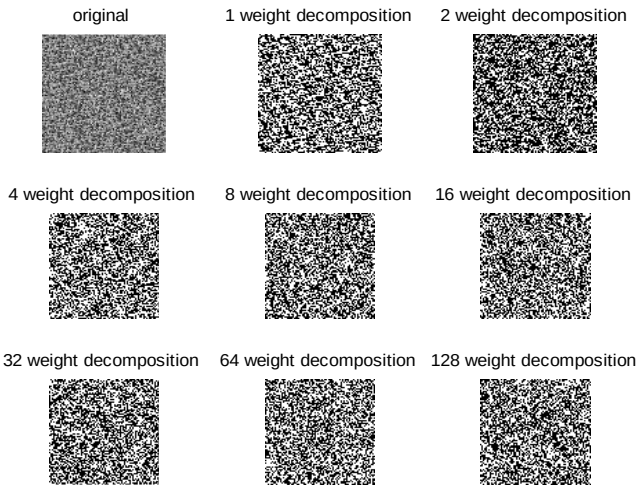


Figure 1. The Group Lena Bit-plane Decomposition

3. Fusion Image Encryption

On the process of decomposition, it can be seen that different bit pixels that are included in the percentage contribution is also different, from experiment study, high four image have 94.125% for example, Lena image, table 1 shows the percentage of pixel information different digits.

Table 1. The Percentage of Pixel Information by Different Contribution

(i+1)weight pixel	Take up of the pixel information $P(i)\%$
1	0.3922
2	0.7843
3	1.5686
4	3.1337
5	6.275
6	12.55
7	25.10
8	50.20

In table 1, we can seen that the decomposition of high weight image can contain most information of original image, so in image encryption ,we mainly consider the high weight image.

We use Logistics chaos in the process of encryption, compared with conventional process of chaotic encryption. We only use Logistics to produce different groups of chaotic sequence. Now introduce Logistic chaotic:

Because the Logistic operation is simple, it has the character of chaos sequence, and can be applied very extensive, so we choose the chaotic system to generate sequence, Logistic chaotic mapping is a classic, and its definition is shown in the following type,

$$x_{n+1} = \mu * x_n * (1 - x_n) \tag{1}$$

Where, $\mu \in (0,4]$ is the Logistic mapping of the control parameters, $x_n \in (0,1)$.

Conventional bit plane encryption, for high weight, it is using the separate cryptographic hashing, and for low weigh, it is using unified handling, the algorithm has shorter time, but it failed to fully considering the importance of high information encryption, this paper use characteristic of bit plane encryption and itself image feature, combined with Logistic to generate chaotic sequence to encrypt a single pixel level computation, specific steps are as follows:

In order to more specific encryption process, we use 3*3 as experiment example.

$$I = \begin{bmatrix} 185 & 78 & 5 \\ 48 & 56 & 207 \\ 19 & 71 & 56 \end{bmatrix}$$

According to the principle of a bit plane encryption ,we can be concluded into 8 groups of different binary matrix, where the weights of the order from low to high, for example 185, its binary decomposition is 10011101, correspond to the following 8 groups of the first element; For decimalize pixel value 78, its binary decomposition is 01110010, corresponds to the second element of the following 8 matrix, decomposition in turn, we get 8 groups of matrix.

$$IF1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}、 IF2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}、 IF3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}、 IF4 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}、$$

$$IF5=\begin{bmatrix}1&0&0\\1&1&0\\1&0&1\end{bmatrix}、IF6=\begin{bmatrix}1&0&0\\1&1&0\\0&0&1\end{bmatrix}、IF7=\begin{bmatrix}0&1&0\\0&0&1\\0&1&0\end{bmatrix}、IF8=\begin{bmatrix}1&0&0\\0&0&1\\0&0&0\end{bmatrix}.$$

We use Logistics to generate 7group chaotic sequence of different initial value ,size of is 3*3, G .Then we process operation that is expansion and Integer to the scope of different value, and get the new sequence Gu .but due to the generated sequence of Logistic may appear the integer is 0.So according to the Logistics iterative sequence diagram, we take u=3.6, then the Logistic chaotic sequence generated mostly between 0.4 ~ 1,so after we use expansion and Integer operation ,there was a few 0, we rule that if this operation generate 0, then set 0 to 1,Specific operation as follows as shown below. Make u = 3.6,7 groups of 3 * 3 size generated by Logistic chaotic sequence of values.

G(1)=[0.78695 0.83627 0.66693 0.50377 0.40705 0.43887 0.53557 0.87 0.430 16]、

G(2)=[0.89078 0.58557 0.81674 0.98785 0.93634 0.993 0.747880.808510.64922]、

G(3)=[0.79614 0.9031 0.77279 0.56287 0.51948 0.74968 0.85622 0.67666 0.583]、

G(4)=[0.60518 0.74084 0.87689 0.5514 0.579230.6541 0.717890.7407 0.92462]、

G(5)=[0.57384 0.62225 0.97411 0.92545 0.79687 0.70931 0.78432 0.87653 0.40901]、

G(6)=[0.60472 0.82164 0.71355 0.84238 0.57065 0.60037 0.52544 0.43551 0.86077]、

G(7)=[0.72045 0.72794 0.92809 0.48191 0.68153 0.65974 0.62789 0.76172 0.98251].

$$Gu(i)=UINT8(G(i)\times i)(i=1,3,\cdots 7)$$

$Gu(1)$ =[1 1 1 1 1 1 1 1 1]、

$Gu(2)$ =[2 1 2 2 2 2 1 2 1]、

$Gu(3)$ =[2 3 2 2 2 2 3 2 2]、

$Gu(4)$ =[2 3 4 2 2 3 3 3 4]、

$Gu(5)$ =[3 3 5 5 4 4 4 4 2]、

$Gu(6)$ =[4 5 4 5 3 4 3 3 5]、

$Gu(7)$ = [5 5 6 3 5 5 4 5 7]

Explain the above every matrix, IF is matrix that is the bit-plane decomposition of original encrypted data I . Gu is 7 group of chaotic sequence after Logistic chaotic extension and integer value, it's function is basis that applied to choose IF different matrix corresponding to the pixel "or "operation.

Algorithm realization process is as follows:

1. Due to the low weight contains less information (image information), so we don't do processing with the first matrix $IF1$.

(1)After we use expansion and Integer operation, all the $Gu(1)$ is 1, its express all elements of $IF2$ will take 'or 'operation with $IF1$ corresponding element ,for the 9 elements of $IF2$,we take "exclusive or" operation one by one base on the chaotic sequence $Gu(1)$,the final result is

$$\underline{IF2}=\begin{bmatrix}1&1&1\\0&0&0\\0&0&0\end{bmatrix}.$$

(2)For the third group Matrix $IF3$,firstly we choose the first element $IF3(1,1)=0$, according to $Gu(2,1)=2$, it express $IF3(1,1)$ will process 'exclusive or 'operation with the second Matrix $\underline{IF2}(1,1)$ (not original decomposition Matrix $IF2$), is $0 \oplus 1=1$, for $IF3(1,2)=1$,we also use this same way, according to $Gu(2,2)=1$,it express $IF3(1,2)$ will take "exclusive or" operation with the first Matrix $IF1(1,2)$,is1&0=1, we take "exclusive or" operation one by one base on the chaotic sequence $Gu(2)$,the final result is

$$\underline{IF3}=\begin{bmatrix}0 & 1 & 1\\ 0 & 0 & 1\\ 0 & 1 & 0\end{bmatrix}$$

(3) For the following $IF4, IF5, IF6, IF7, IF8$ Matrix, We use above process, the final results $\underline{IF4}, \underline{IF5}, \underline{IF6}, \underline{IF7}, \underline{IF8}$ respectively is.

2. According to the above step 1 case analysis, we take I extend to Lena (256*256) of digital matrix, the Logistics choose sequence will extend to 256*256, the encryption process is above process, we will get the final Lena encryption image.

3. Repeat the above for 3 times will be the final encryption image, three times can select different initial value in the process of encryption key, this key will be very big.

The encryption algorithm process low weight data using "exclusive or" operation. In general, lowest don't do operation, the security is low, but for high weight data, we select the pixel image encryption required the more chaotic sequence. Such as the highest amount of information is the $IF8$,for $IF8$,when we use or operation to the $IF8$ of each element, we should select $Gu(7)$ elements, but $Gu(7)$ include 1~7,this mean that for $IF8$ of each elements ,we might utilize one of the $IF1, \underline{IF2} \sim \underline{IF7}$, it need 7groups different matrix ,and it produce more information. This also consistent with the analysis of group of images of different information, so it can have good encryption effect.

4. Algorithm Simulation and Performance Analysis

This algorithm use the analysis of bit plane of each image with different way, the encryption process is very strict. Compared to common encryption processing of using "exclusive or" operate chaotic sequence generated values with the original image.

This paper use Lena ,woman as experiment image, and 7.0 version MATLAB, in Windows 7 operate system , the size of experiment image is 256*256, 256*256, we use following initial value to generate 7 groups Logistics chaotic sequence, the initial value and key respectively is:

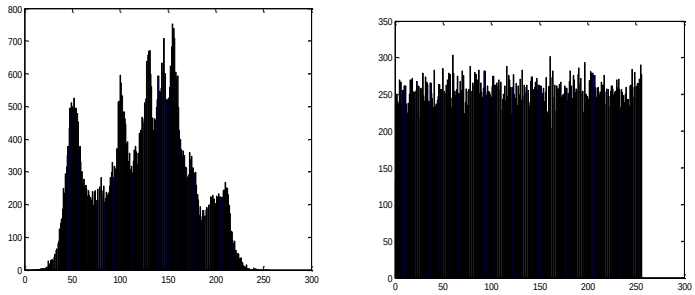
$x_1=0.786$, $x_2=0.456$, $x_3=0.866$, $x_4=0.136$, $x_5=0.436$, $x_6=0.286$ $x_7=0.193$, $u=3.6$,NCA(Non-linear chaos)initial value is $x_0=0.6$, $\alpha=1.1$, $\beta=24$, $K_0=10000$。 The original Lena image and the corresponding encryption image, as shown in the below.

Figure 2. Lena and Encryption Image

4.1. Statistic Analysis

Statistical attack on the encryption algorithm can test resistance to attack ability in confusion and diffusion properties, any standard image has certain correlation between adjacent pixel, so the analysis of the correlation of encrypted image has much effect on the encryption algorithm, we will one by one analysis three aspects ,histogram statistics, information entropy, correlation of the adjacent pixels.

Image histogram reflects an the distribution of pixel values, standard image histogram are generally has a set of regularity, and encrypted histogram is almost close to the uniform distribution, Figure 3 respectively represents the standard Lena images and the corresponding histogram, encryption image and the corresponding histogram. Compared with encryption image and its corresponding histogram, it can be seen that the difference is very big, just rely on histogram statistics attack is invalid.



(a)-Lena (b)-Lena of encryption

Figure 3. Clear Image and the Cipher Image Histogram

Image information entropy can reflect the distribution of gray value, it is the important indicators to measure the algorithm randomness and security .The result display that the more greater of gray scale, the distribution will be more uniform ,for an ideal random images, the information entropy is equal to eight, So the image information entropy is more closer to 8, this show more random information distribution ,and it is able to demonstrate excellent characteristic of encryption effect. According to the Shannon theorem.

$$H(m) = -\sum_{i=0}^{L-1} p(m_i) \log_2 p(m_i),$$

$$\sum_{i=0}^{L-1} p(m_i) = 1 \tag{2}$$

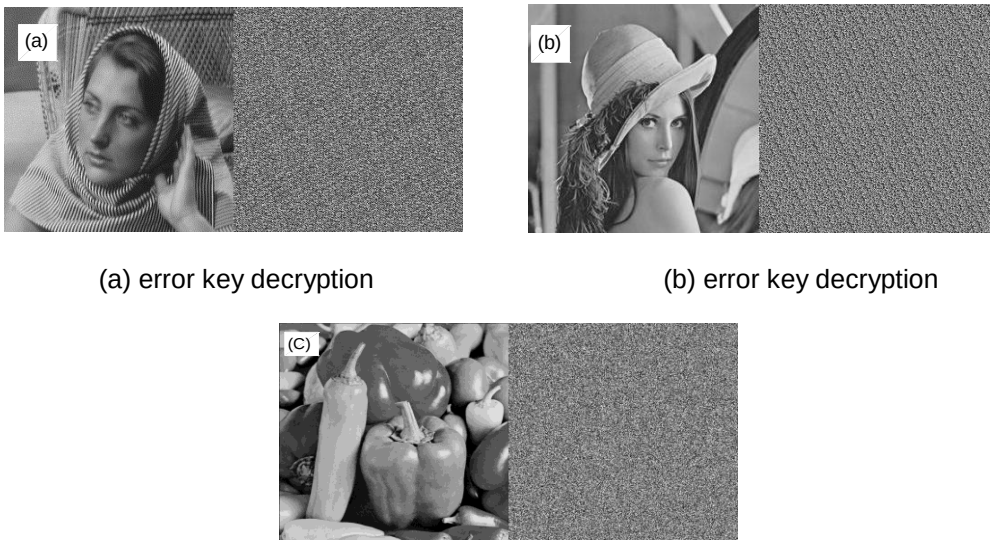
Where m_i is value of gray I ,L is the number of gray value, this paper is closer to 8 and has good information entropy, when Lena encryption iterative three times, the information entropy can reach 7.97982.So it indicates well random, it can resist information entropy attack.

4.2. Sensitivity Analysis

Because this article need eight different Logistic initial value, and the high weight of decryption may impact overall encryption security, and in this paper if we want to decryption high weight image ,we first must obtain low weight 7image, the one of eight image access error ,it will ultimately lead to poor decryption. Key sensitivity analysis, it is that the small nuances of original keys are likely to affect the final decryption image. The following is the right initial value:

x_1=0.786, x_2=0.456, x_3=0.866, x_4=0.136, x_5=0.436, x_6=0.286, x_7=0.193=6, x_8=0.266, u=3.6, x_0=0.6, α=1.1, β=24, K_0=10000

We just change the x_6=0.296,and keep the other parameter constant, Figure.4 respectively shows the correct secret key to decryption and wrong decryption of three sets of image



(a) error key decryption (b) error key decryption

(c) error key decryption

Figure 4. Key Sensitivity Analysis Diagrams

The decrypted image is shown in the following figure, according to the figure.4, we can be seen that the original key only made slight changes, the decrypted image will be a big change, so it can be seen that the algorithm is sensitive to the key.

4.3. Resist Attack Analysis

For common image encryption algorithm, the strength of the ability to resist attack is the important performance to measure an algorithm of robust performance factors, this paper based on the common shear resistance attack and anti noise attack as a test.

Because the digital signal transmission environment is not ideal, digital image in the process of transmission is often will encounter all sorts of different interference. Sometimes the encryption image be intercepted by a third party, although it cannot decrypt image, but it might take malicious attacks, such as adding noise, shear to

destroy the image, so the encrypted image recovery after noise or shear attacks has certain practical significance. To test algorithm against attack, we use cropping attacks to the encrypted image, the experiment use classic image Lena (256 * 256), a Woman (256 * 256) and pepper (512 * 512), for shear attack experiment, the shear range of 1/4, 1/2, 3/4 , for verifying the robust performance of the algorithm, at the same time the shear experiments use high gray value to cover the pure white of different experiments, the experimental range and shear are the same, the experimental results are shown in figure.5.

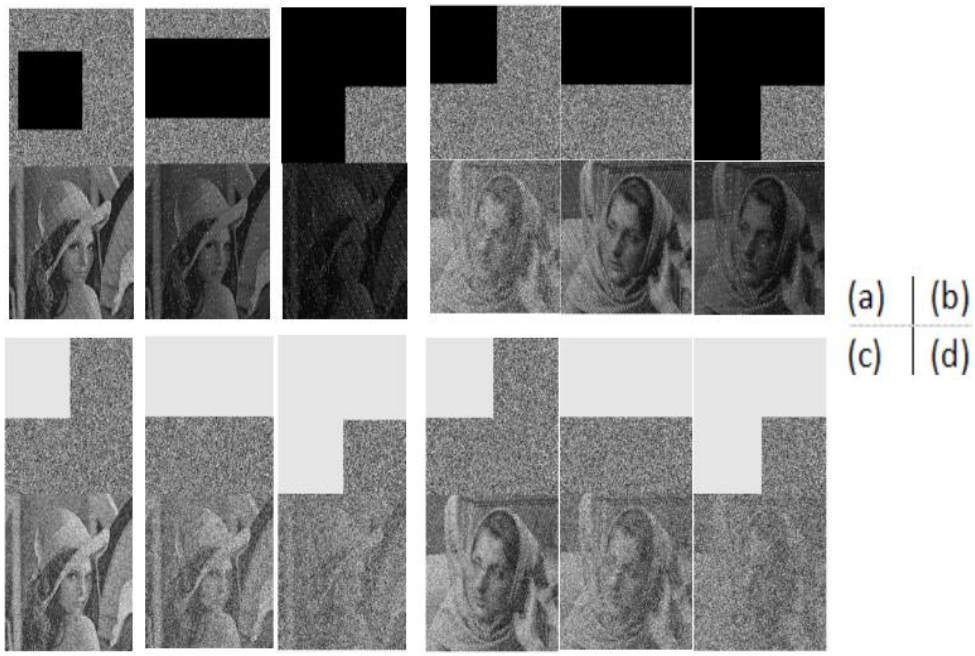


Figure 5. Shear Resistance Analysis Diagram

From the above figure, we can seen that in the (a) of the results, the cryptographic image cut part of the assignment is zero in shear, therefore, when we take decrypted, because the decryption is the reverse process of encryption ,so decryption process will still conduct a lot of zero, and the entropy image will be more darker, we can seen that in the shear range of 1/4、1/2,from the final encryption image, it show a lot of original image information, when shear range to 3/4,the impact on the decrypted image is large, but we also can see the general information, in the results of (d),the experiment is high gray value to replace zero, for effect of display ,we set the high gray is 240.compared with general shear attack ,we can seen that high gray value will conduct more impact on the image of decryption, in the cover range of 1/4、1/2,the image of decryption can be seen important information of original image, but the range to3/4,the image of decrypted is blurred, we can only roughly distinguish the original image information. In general, on the different experiment images, different gray value cover and different range shear attack, this paper have good shear resistance, and strong robustness.

Due to the signal fluctuation, noise in the signal transmission is often produce, in addition to, the intercepted cryptographic image often be noise attacks to damage information of original image .So test the image encryption algorithms ability to resist noise attack is a one of the important standards of good practicality, this experiment use Lena (256*256) as example, adding different intensity of salt pepper noise. The noise factor respectively is 0.02, 0.2.

(0.02 factor) (0.2factor)

Figure 6. Resist Noise Attack Graph with Different Noise Factor

From the experiment results, we can seen that adding different intensity noise factor also can decrypt the original image information, and under the strong noise will still be able to decrypt the key information of the original image, we can see this algorithm has good performance in different noise.

5. Conclusion

This algorithm makes full use of the NCA chaotic thoughts, Logistic chaotic thoughts and the combination of a graphic image itself and take binary decomposition encryption to original image. Using chaotic sequence generated by Logistics decided to order of "exclusive or" with different pixel, different matrix, it fully ensure the high complexity of encryption. Algorithm on the basis of experiment using Lena and Woman as experimental graph, the experimental results show that the proposed algorithm encryption effect is very good, compared with a bit plane encryption algorithm, it is more practical than normal, in terms of detection against attack, this algorithm is very good, and shearing ability to resist noise is also very good, it have a large amount of key, and can resist various attacks, with a strong robustness.

Acknowledgement

The work is supported by Natural Science Foundation of Heilongjiang Province of China (ZD201203).

References

[1] Bhatnagar G Wu Q M Jonathan, Ｒaman B. Image and video encryption based on dual space- filling curves ［J］.Computer Journal**(2012)**,Vol. 6, pp.667-685.
[2] Chen Guanrong, Mao Yaobin, Chui Charkes K.A symmetric image encryption scheme based on 3D chaotic catmaps [J].Chaos Solutions＆Fractals,**(2004)**, Vol. 3, pp.749-761.
[3] Xu zhu, Chen zhigang, OuYangWenWei. A new image encryption based on generalized Chen chaotic system , [J] journal of central south university: natural science edition, **(2006)**,Vol. 6, pp.1142-1148.
[4] Chen Yan- feng,Li Yi- fang. Image encryption algorithm based on reciprocally- disordered diploid chaotic sequences alternated in subsection ［J］.Journal of South China University of Technology: Natural Science Edition, **(2010)** ,Vol. 5, pp.27-33.
[5] Zhu Cong xu. A novel image encryption scheme based on improved hyper chaotic sequences ［J］.Optics Communications**,(2012)** ,Vol. 1, pp.29-37.
[6] Wen Chang- ci, Wang Qin, Huang Fu- min, et alSelf adaptive encryption for JPEG color image ［J］. Journal of Computer Aided Design＆Computer Graphics, **(2012)** ,Vol. 4, pp.500-505.
[7] Bhatnagar G,Wu Q M Jonathan.Chaos- based security solution for fingerprint data during communication and transmission ［J].IEEE Transactions on Instrumentation and Measurement, **(2012)** ,Vol. 4, pp.876-887.
[8] Akhshani A, Akhavan A, Lim SC eta. An image encryption scheme based on quantum logistic map[J].Communications in Nonlinear Science and Numerical Simulation,**(2012)** ,Vol. 12, pp.4653-4661.

[9] Bhatnagar G, Wu Q M Jonathan, Raman B. Image and video encryption based on dual space- filling curves[J]Computer Journal**,(2012)** ,Vol. 6, pp.667-685.
[10] Xiao Yong-Liang, Xia.An Image Encryption Using a Shuffling Map Chinese Physical Society and IOP Publishing Ltd[J], **(2009)** ,Vol. 6, pp.876-880.
[11]Xie Guobo, Ding Yuming. Based on Logistic mapping parameters of variable image encryption algorithm. Microelectronics and computer **,(2015)** ,Vol. 6, pp. 111-115.
[12]Wenchang, Wang Qin xiang-hong liu, huang FuMin, Yuan Zhishu. Based on the affine and complex new chaotic image encryption algorithm. Computer research and development [J]. **(2014)** ,Vol. 2, pp.319-319.
[13]Luo Yuling, ming-hui du. Quantum Logistic mapping based on wavelet domain image encryption algorithm [J]. Journal of south China university of technology (natural science edition) ,**(2013)** ,Vol. 6, pp.210-214.
[14]Sun Xiehua .Image Encryption Algorithms and Practices with Implementations in C#.Science Publications of china,**(2013)**, Vol. 6, pp.978-1001

Author

Honge Ren, She was born in 1962. She received the Ph.D. degree from Northeast Forestry University, China, in 2009. She is currently professor of information and computer engineering college at school of Northeast Forestry University, supervisor of Dr. Her main research interests include the pattern recognition and intelligent control.

