Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **3**, May **2016**

Image Encryption Method Based on Discrete Lorenz Chaotic Sequences

Qi Zhang, Yuchao Guo, Wangshu Li and Qun Ding

Electronic Engineering College
Heilongjiang University,
Harbin, China
ljittss@163.com, qunding@aliyun.com

Received January, 2016; revised March, 2016

Abstract. *Image transmission is very popular in the field of modern communication, the image may contain a large number of private information, and its security in the transmission process is difficult to be guaranteed.So it is particularly important to encrypt the image before its transmission.Due to the nature of the chaotic system, it has very good encryption performance.This paper presents an algorithm for image encryption based on chaotic sequences generated by Lorenz chaotic system. We choose the Lorenz chaotic system, which is a continuous system, if you want to use it to encrypt the image, the system should be discrete. Here we choose Euler method to discrete the system, then we quantify the obtained sequences to get the two value sequence.Lorenz chaotic system will produce three sets of sequences, but not each sequence will have a very good encryption characteristics,so we choose classic statistical test and NIST standard test to test and analyze the chaotic sequence code,select the best sequence of encryption features for image encryption.The MATLAB simulation showed that the method can realize the image encryption and decryption, the effect is good, and it can guarantee the security of data transmission.*

Keywords: Lorenz chaotic system; Euler method;Statistical test; Image encryption

1. **Introduction.** Under the drive of science and technology development, transmission of network information security has become an issue of the greatest concern. Because the information is easy to leak in the transmission process, people's privacy is threatened. Therefore, the development of data encryption technology is very important. Image as an important carrier of information transmission, which may contain a large number of personal identity information, once it has been intercepted the consequences could be disastrous, so the image transmission of image encryption is very important. As the chaotic movement shows the inner randomness, initial sensitivity and other characteristics [1]. Chaotic systems iterates through the adjacent finite iterations can get entirely different sequence. Therefore digital data encryption chaotic system is widely used in data encryption. Based on the current chaotic system to encrypt data focused on the one-dimensional and two-dimensional chaotic system [2]. Data encryption scheme based logistic chaotic system are widely used [3]. As it has a small key space, there have been some attacks to crack it. And Zheng Yanbin [4] proposed the existence of local periodic sequence of chaotic sequences, which also makes it possible to crack the chaotic code. Due to the high dimensional chaotic system has better randomness and larger key space, it can improve the security of data encryption. Therefore, this paper presents a three-dimensional image encryption method based on continuous Lorenz system. It describes the generation

principle of the Lorenz system [5]. By chaotic attractor and Lyapunov exponent shows the random and initial value sensitivity of the system [6, 7]. The Runge-Kutta method is the common method to be used to discrete chaotic systems [8], this paper uses the Euler method to discrete the output data of chaotic system, after the discretization of the chaotic sequence, the 0-1 two value sequence is generated. The three-dimensional Lorenz chaotic system can produce three direction sequences, although they are all chaotic sequence, the characteristics of each sequence are different. We choose to use the chaotic sequence to encrypt the image, so we rely on the good randomness and unpredictable of the chaotic sequence. So in this paper, through the power spectrum test, autocorrelation test and standard NIST test, after the analysis we select the best sequence in the three directions for encryption.

Then process the image, obtain the 0-1 binary sequence of the image, make it xor with the chaotic sequence to achieve the encryption effect. Decryption process is the inverse of the encryption process, it is easy to achieve. Finally, through the test of the encryption results, this method can realize the image encryption and the encryption effect is good.

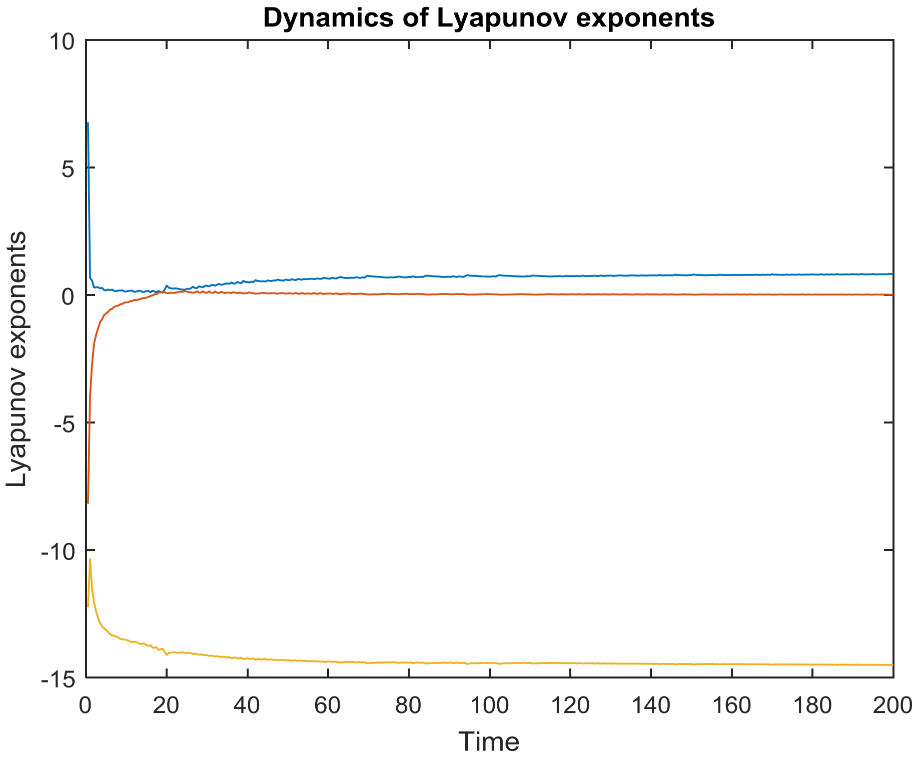


Figure 1. Lyapunov exponents of Lorenz map.

2. Lorenz continuous chaotic system.

2.1. The characteristics of the chaotic system.

(1) Overall stable local instability

The difference between chaos and order is that it not only has the overall stability and local instability. Stability is the property and ability of the system to maintain the state of the original state after the system is disturbed, and it should be allowed the local instability in the overall stability, this instability is the basis of evolution. In the chaotic motion, this point is very obvious.

(2) Initial value sensitivity

Initial value has little change, after a long time, the movement may be far away. This means that the chaotic motion has an unstable in the sense of Lyapunov [10]. The larger the Lyapunov index is, the more rapidly the phase space motion trajectory is, the more sensitive to initial conditions, and the more chaotic system is.

So far, the method of calculating the Lyapunov characteristic index can be divided into direct method and Jacobi method [11]. Because of the high reliability of the Jacobi method, this method is mainly introduced in this paper.

In general, N dimension map should have N Lyapunov index, which is positive and negative. As long as there is a positive Lyapunov exponent, that is, there is a strange attractor, it can be judged that the system is a chaotic system. For the three-dimensional Lorenz mapping, when the initial value is $x_0 = 0$, $y_0 = 0$, $z_0 = 0$, the Lyapunov index of the system is shown in Figure 1.

We can see that there are positive Lyapunov exponents of the Lorenz chaotic system, which indicates that the system is sensitive to the initial conditions, and the system is chaotic.

(3) Chaos attractors

A global stability factor, but the orbit is not stable, this makes it stretched, twisted, and folded in the shape of the phase space. The formation of self similar structures with a fine, infinite nested. That is the chaos attractor. When $\alpha = 0$, the attractor of the Lorenz chaotic system is shown as the figure 2:

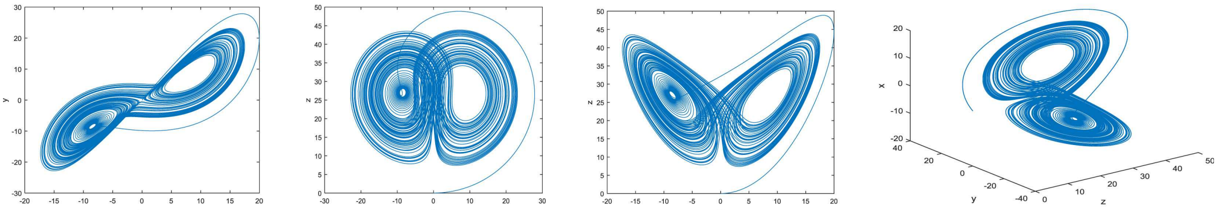


FIGURE 2. Lorenz attractor.

From this graph we can see that the chaotic attractor of the new structural system has a strong attraction, with complex folding and stretching of the trajectory, suggesting that the instability of the new system in the local has become more.

2.2. **Lorenz chaotic system.** In 2001, Lv Jinhu and Chen Guanrong proposed a model of three-dimensional continuous unified chaotic system. The system is only used to establish a link between the Lorenz chaotic system and Chen chaotic system with one parameter [12]. At that time, the unified chaotic system is in a chaotic state, which can express all the chaos system between the Lorenz system and the Chen system. Unified chaotic system. Among them, parameters $\alpha \in [0, 1]$, the unified chaotic system has been realized from a chaotic system to another chaotic system. When $0 \leq \alpha < 0.8$, Lorenz equation:

$$\begin{cases} \bar{x} = -10\,(x - y) \\ \bar{y} = -xz + 28x - y \\ \bar{z} = xy - 8z/3 \end{cases} \tag{1}$$

3. **Discretization and quantification of Lorenz chaotic system and statistical test.**

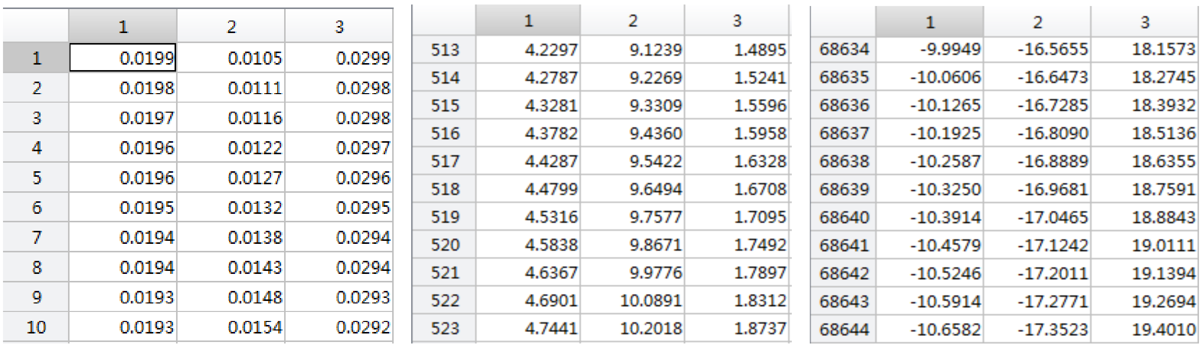
3.1. **Discretization of continuous Lorenz system based on the Euler method.** The numerical solution of the differential equation is obtained by using various methods. Differential equations are transformed into differential equations by means of discretization. First, solving the approximate value $y_0, y_1, \cdots y_n, y_{n+1}, \cdots$ of $y(x)$ in a series of discrete nodes $a = x_0 < x_1 < \cdots x_n < x_{n+1} < \cdots$. Then the recursive formula of approximate value y_n is established for $y(x_n)$ and the approximate value of $y(x)$ at each node is obtained. The spacing between two adjacent nodes is called the step size $h = x_{n+1} - x_n$. This section always assumes that the h is constant, then the node $x_n = x_0 + nh$, $n = 0, 1, 2, \cdots$. Here we choose the Euler method for discretization of the equation. Defined by the definition of the derivative, for sufficiently small:

$$\frac{y(x_{n+1}) - y(x_n)}{h} \approx y'(x_n) \approx f(x_n, y(x_n)) \tag{2}$$

Through it we can draw $y(x_{n+1}) \approx y(x_n) + hf(x_n, y(x_n))$, according to the Lorenz equation method for the use of the derivative with respect to discrete:

$$\begin{cases} x_{n+1} = x_n + 10\left(y_n - x_n\right)h \\ y_{n+1} = y_n + \left(28x_n - y_n - x_n z_n\right)h \\ z_{n+1} = z_n + \left(x_n z_n - 8z_n/3\right)h \end{cases} \tag{3}$$

By this difference equation, in MATLAB programming, set initial value $x = 0.02$, $y = 0.01$, $z = 0.03$, step size $h = 0.001$, run the program. We can get X, Y, Z three directions of the output discrete sequence, the output result is shown in figure 3:



	1	2	3
1	0.0199	0.0105	0.0299
2	0.0198	0.0111	0.0298
3	0.0197	0.0116	0.0298
4	0.0196	0.0122	0.0297
5	0.0196	0.0127	0.0296
6	0.0195	0.0132	0.0295
7	0.0194	0.0138	0.0294
8	0.0194	0.0143	0.0294
9	0.0193	0.0148	0.0293
10	0.0193	0.0154	0.0292

	1	2	3
513	4.2297	9.1239	1.4895
514	4.2787	9.2269	1.5241
515	4.3281	9.3309	1.5596
516	4.3782	9.4360	1.5958
517	4.4287	9.5422	1.6328
518	4.4799	9.6494	1.6708
519	4.5316	9.7577	1.7095
520	4.5838	9.8671	1.7492
521	4.6367	9.9776	1.7897
522	4.6901	10.0891	1.8312
523	4.7441	10.2018	1.8737

	1	2	3
68634	-9.9949	-16.5655	18.1573
68635	-10.0606	-16.6473	18.2745
68636	-10.1265	-16.7285	18.3932
68637	-10.1925	-16.8090	18.5136
68638	-10.2587	-16.8889	18.6355
68639	-10.3250	-16.9681	18.7591
68640	-10.3914	-17.0465	18.8843
68641	-10.4579	-17.1242	19.0111
68642	-10.5246	-17.2011	19.1394
68643	-10.5914	-17.2771	19.2694
68644	-10.6582	-17.3523	19.4010

Figure 3. The output sequence.

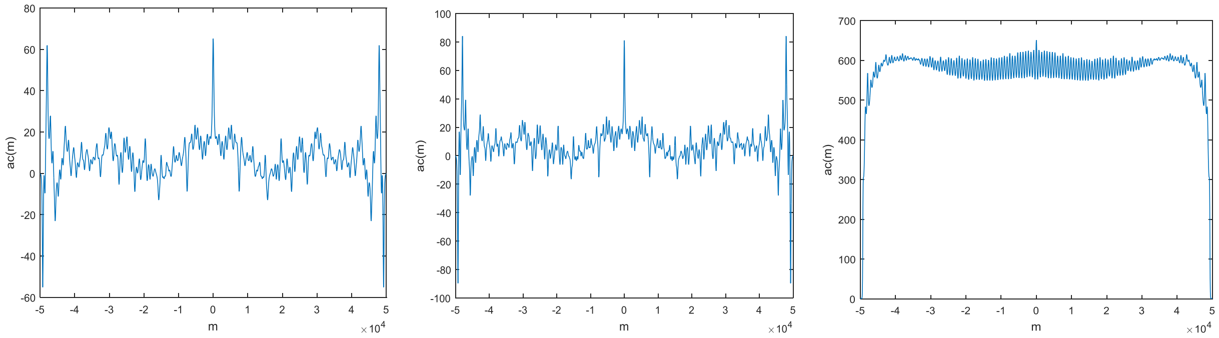
3.2. Characteristic analysis before quantification.

3.2.1. *Auto correlation properties.* For three sets of sequences generated by the Lorenz chaotic system, we can make the auto correlation test to them. Autocorrelation is a measure of the degree of sequence dependent, it is also a correlation between a sequence of a sequence and a new sequence of its own after a shift process. The sequence of the auto correlation function is defined as follows:

$$ac(m) = \frac{1}{N} \sum_{i=1}^{N-m} b(i)b(i+m) \tag{4}$$

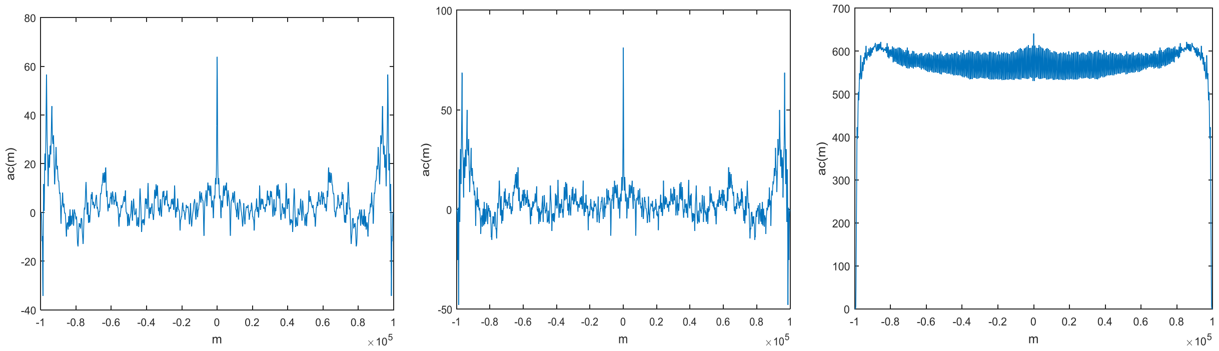
In the formula, N represents the length of the sequence, m is the step parameter. Here we choose the sequence length of 50000 and 100000, and then the X, Y, Z direction of the sequence generated by the test. Test results are shown in the figure 4 and figure 5:

From the results of the output sequence can be seen, when the sequence length is 50000 and 100000, the correlation characteristic is very similar. But from the X, Y, Z three



X. 50000 Y. 50000 Z. 50000

Figure 4. Auto correlation test of Lorenz chaotic system with a length of 50000 sequence.



X. 100000 Y. 100000 Z. 100000

Figure 5. Auto correlation test of Lorenz chaotic system with a length of 100000 sequence.

direction analysis we can clearly see, there will be a sharp peak at the $m = 0$. And in other places, X, Y direction is relatively rough, only the direction of the Z is relatively smooth. For the significance of the correlation function. The correlation between the size of the function value and the correlation between sequences is proportional relation. The larger the function value, the stronger the correlation, and vice versa. In this way, we can see that the function value of Y, X direction is close, and it is obviously less than Z direction, so the correlation is smaller. Sequences generated by Lorenz chaotic system is used to encrypt. So the correlation is small, so we can choose X and Y direction according to the sequence correlation.

3.2.2. *Power spectral density.* Power spectrum density is a reflection of the distribution of signal power in frequency domain. The chaotic sequence can be regarded as a random sequence, then the power spectral density function should be considered as the statistical average of every possible power spectrum. Because the output sequence of the chaotic system is non-periodic, so its power spectral density should be continuous. Power spectral density curve also reflects the randomness of random sequences, the more smooth the curve is, the better. In this paper, we choose the PSD-Welch method, with the output sequence length 100000 as an example, the power spectrum density curve of Lorenz mixed degree system is shown in the following figure:

From the results we can see that the Y, X direction of the power spectral density curve is almost overlapping, and relative to the Z direction of the curve is more smooth, less

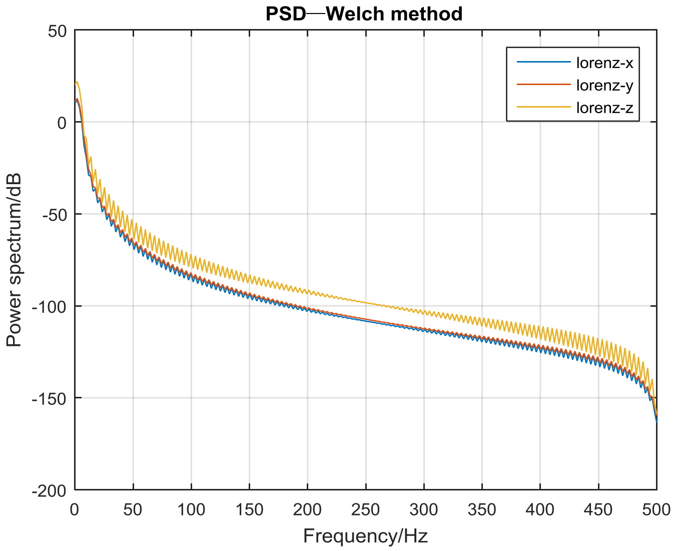


Figure 6. Power spectral density.

volatile, so we can judge that the power spectral density is better, that is, the two output sequence with the relatively is good, so we will choose these two output sequence.

So the analysis of autocorrelation and power spectrum density showed that Y, X direction of the output sequence is significantly better than the Z direction, so in the choice of encryption data, you can choose X or Y sequence before the quantification.

3.3. **The quantification of the sequence.** In the process of quantization of the classical Logistic chaotic sequence, we choose the method to take the average value of the output sequence, if it is larger than the average value, it becomes 1, or it is less than that, it becomes 0. But we can see from figure 3, Lorenz discrete chaotic sequence values from 0.0199 to 4.6866 to -14.1203, from these data, data span is relatively large, if you take the mean value quantization method, the sequence period is serious. So we can not take this approach to quantify, here is a new method for the quantification of Lorenz chaotic sequences, the process is as follows:

1) Absolute value of all sequence values.
2) Determine the sequence value, if it is less than 0.1, it is multiplied by 10.
3) If the sequence value is greater than 1, remain the fractional part.
4) Take the average value of the output sequence, if it is larger than the average value, it becomes 1, or it is less than that, it becomes 0.

We take the output of the X sequence as an example, the process can be expressed by the expression, as shown in the following:

$$X = \begin{cases} |x_i| \cdot 10 & |x_i| < 0.1 \\ |x_i| - fix\,|x_i| & |x_i| > 1.0 \end{cases} \tag{5}$$

Where x_i is the discrete elements in sequence, fix is integral function. After (5) obtained the X sequence to quantify, the expression as follows:

$$X_{0,1} = \begin{cases} 1 & X \geq \overline{X} \\ 0 & X < \overline{X} \end{cases} \tag{6}$$

Where $\overline{X}$ is the average value of X sequence. The quantization process of Y, Z sequence is the same as above. After such a quantitative process to get X, Y, Z three 0-1 two value sequences.

3.4. **NIST standard test.** The NIST Test Suite is a statistical package consisting of 15 tests [13, 14] that were developed to test the randomness of (arbitrarily long) binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence. Some tests are decomposable into a variety of subtests. The final measure of the 15 kinds of tests is P-value, if P-value >= 0.01, said the test successfully, the sequence in this test showed good randomness. Since the test suite is running in the Linux system environment, the test data can not be generated with MATLAB, we use C program generated sequence, the generated 0-1 two value sequence in the form of. txt file to save. Taking the Runs test as an example, the final test results are shown as the p-value is 0.533509.

Where p-value $= 0.533509 > 0.01$, which means that the test is passed. Then we test the X, Y, Z three 0-1 sequences respectively, and the test results are shown in the following table1:

Table 1. NIST test result

Test name	P-value X		P-value Y		P-value Z	
Frequency	0.527039	success	0.767189	success	0.454177	success
Block Frequency	0.310214	success	0.621674	success	0.000142	**failure**
Runs	0.533509	success	0.227541	success	0.012585	success
Long Runs	0.637851	success	0.013889	success	0.077415	success
Rank	0.884512	success	0.351944	success	0.186547	success
Discrete Fourier	0.001256	**failure**	0.364587	success	0.001426	**failure**
OverlappingTemplate	0.115668	success	0.000899	**failure**	0.000561	**failure**
ApproximateEntropy	0.875601	success	0.114569	success	0.079521	success
CumulativeSums	0.085644	success	0.364498	success	0.047664	success
LinearComplexity	0.700914	success	0.147785	success	0.165455	success
Serial	0.232241	success	0.658424	success	0.465414	success
Universal	0.112117	success	0.851164	success	0.004791	**failure**
Non-Overlapping	0.548777	success	0.462851	success	0.415416	success
RandomExcursions	0.600128	success	0.648574	success	0.000000	**failure**
RandomVariant	0.097741	success	0.004541	**failure**	0.000000	**failure**

Through the analysis of NIST test results, it is obvious that there is only one failure in X sequence to pass the test, and it is the best sequence of randomness. Compare the text result without quantization, we choose the X vector as the encryption sequence. At this point we have the X vector of the autocorrelation test, the results as shown in Figure 7:

From the figure, X direction sequence is more close to the δ function, which shows better pseudo random property.

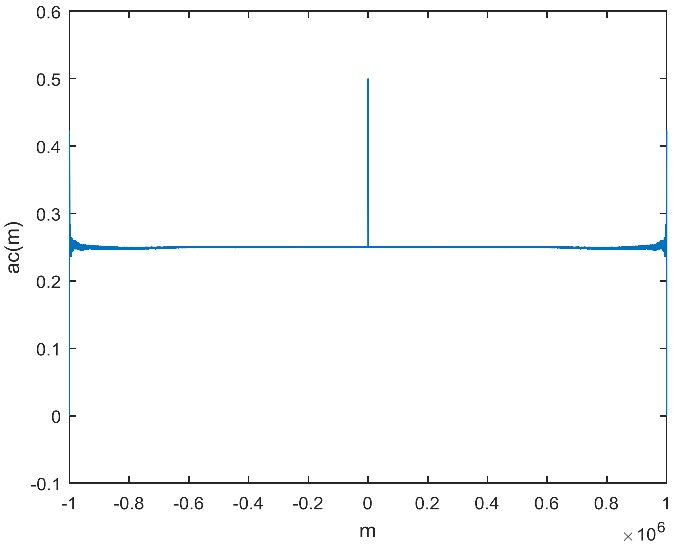


Figure 7. Auto correlation test of X.

4. Image encryption.

4.1. **The principle and result of image encryption.** Through the above analysis, we use the output of the X direction sequence for image encryption. First we take the standard 256 × 256 Lena image as an example, the image is processed. A digital image can be converted into a two dimensional matrix, each element is the gray value of the pixel of the image. The matrix is processed, converted into a one-dimensional array. Then the Lorenz chaotic sequence in Y direction and XOR the array. This get the encrypted data, and then convert the one-dimensional data into a two-dimensional matrix, restore the encrypted image, then the image is encrypted image, encryption process as shown below:

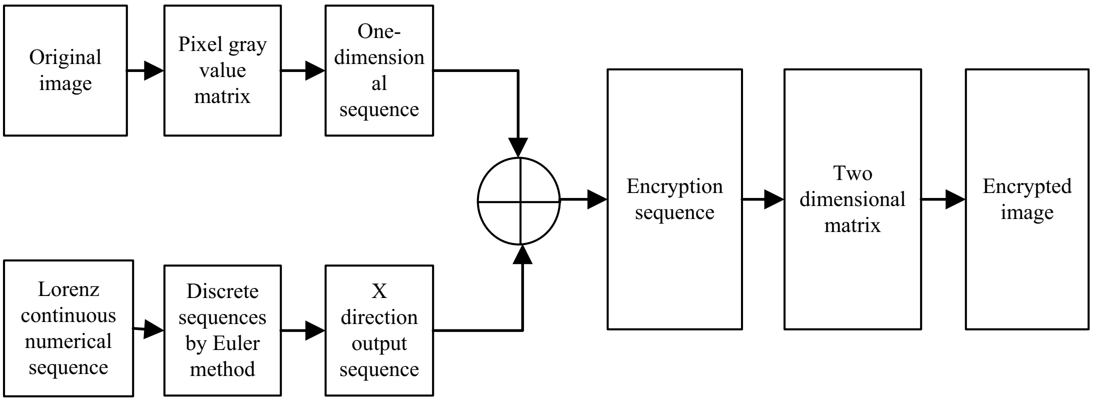

Original image
Pixel gray value matrix
One-dimension al sequence
Lorenz continuous numerical sequence
Discrete sequences by Euler method
X direction output sequence
Encryption sequence
Two dimensional matrix
Encrypted image

Figure 8. Encryption process.

According to the image encryption process, we can encrypt the image, the following is the results of the encryption as figure 9 and figure 10:

From the encryption of the image, we can see intuitively, we have been unable to get any information of the original image, so from this we can see Lorenz encryption algorithm can achieve the effect of image encryption. Below we also through the MATLAB for image decryption operations, decryption is the inverse operation of the encryption, the results shown in the following figure 11 and figure 12.

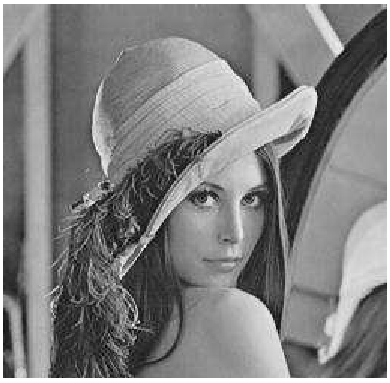


Figure 9. The original image.

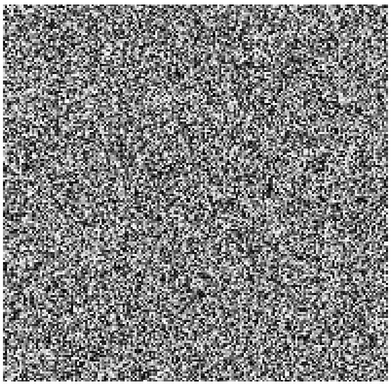


Figure 10. The encrypted image.

From the decrypted images, we can see the decrypted image and the original image is almost the same, so you can see good encryption effects, which can also be proved that the encryption algorithm for image encryption operation.

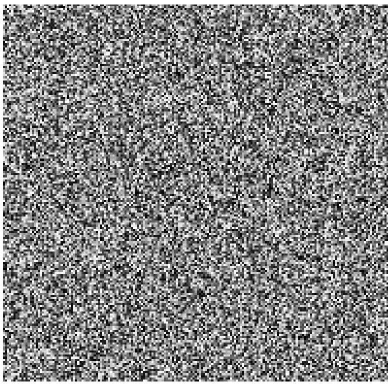


Figure 11. The encrypted image.

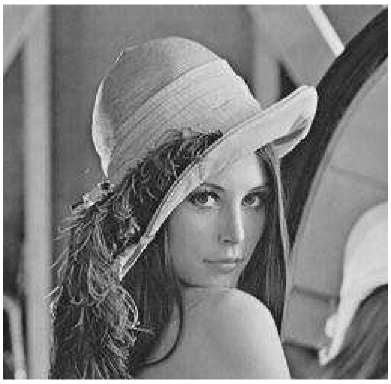
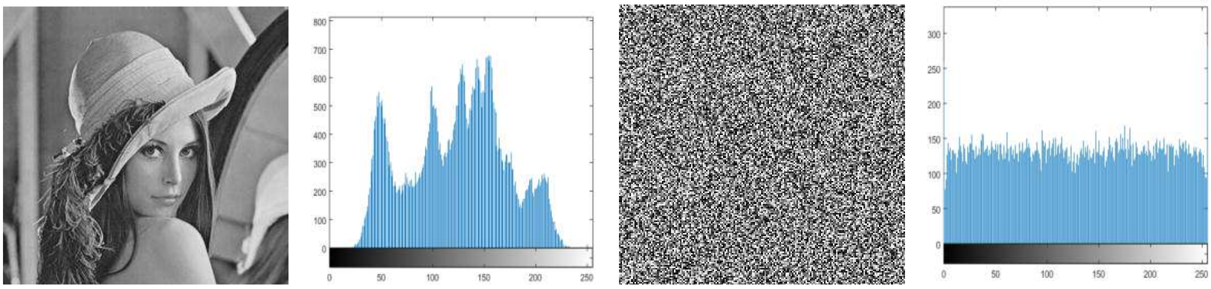


Figure 12. The decrypted image.

4.2. **Analysis of encryption results.** The general feature of the image can be described through gray histogram of the image [15], that is the number of occurrences of different pixel values. If a image with a low contrast, then the histogram is narrow and focused on the middle of the gray scale. If the pixel of an image occupies all possible gray scale and it is uniform distribution, then the image has high contrast and various gray color. Thus it can analyze the effect of image encryption through the contrast of the digital image histogram. The analysis of the contrast of the histogram of the original image and the encrypted image are shown as Figure 13.

From the histogram we can see that there is obvious change between the encrypted image histogram and the original image histogram. There are great changes from the distribution of pixels and the pixels. And the histogram pixel values of encrypted image are more evenly distributed. Then the encrypted image approximation for a picture of a random noise image. From this result we can see that the Lorenz algorithm has good effect for image encryption. It also suggests that this kind of algorithm had a high security. In the process of the image transmission it will be not susceptible to tampering or eavesdropping.

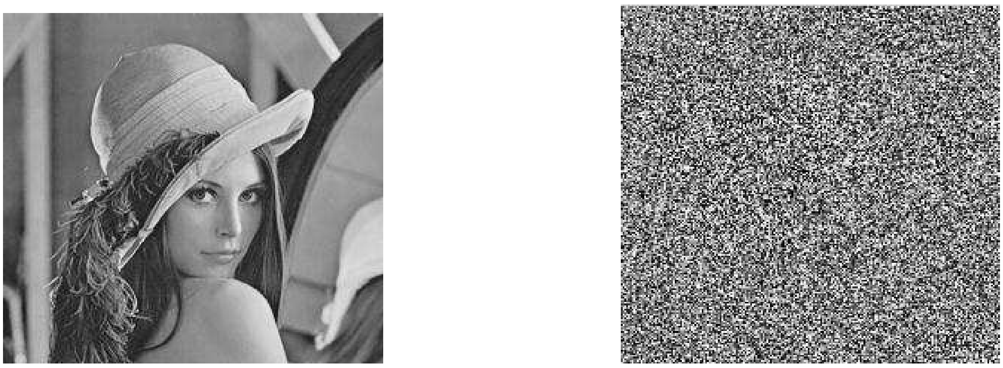
A good encryption algorithm should be sensitive to plaintext, and also be sensitive to the key. Here we choose the encryption method of the key is the initial value of the Lorenz chaotic system $x = 0.02$, $y = 0.01$, $z = 0.03$, in theory the key space is infinite, so it is



(a) The original image (b) Histogram of original image (c) The encrypted image (d) Histogram of the encrypted image

Figure 13. Histogram analysis of image encryption.

enough to resist the brute force attacks. In order to test the sensitivity of the key, we select the correct key: $x = 0.02$, $y = 0.01$, $z = 0.03$ and the wrong key: $x = 0.0201$, $y = 0.01$, $z = 0.03$, decrypt the encrypted image respectively. Decryption results as shown below:



(a) The decrypted image with correct key (b) The decrypted image with wrong key

Figure 14. Key sensitive text.

The results show that even if we use the wrong key with a litte difference with the correct key, at the time of decryption. There is a big difference between the original image and encrypted image, that is the wrong image, it has been unable to restore the original image, lead to complete failure to decryption. This shows that the encryption method based on Lorenz chaotic sequence is sensitive to the key.

5. **Conclusion.** In this paper, a method of image encryption based on discrete Lorenz chaotic sequences is proposed. The key point is that we choose a sequence of the best encryption properties after the Lorenz chaotic system is discretized. Before the sequence quantization, through the test of the power spectrum and the autocorrelation test, it is concluded that the encryption characteristics of X and Y sequences are relatively good. In this paper, a quantitative method of Lorenz chaotic series is proposed. After quantization and standard NIST test, it is concluded that the sequence of X direction is the best sequence of relative encryption and randomness. So choose this sequence as the image encryption sequence cipher code, simulation verification in MATLAB environment, from the above experimental results and analysis, coupled histogram analysis, this method can achieve very good image encryption effect. And the decryption essentially and encryption has the same structure, it can conveniently to restore the original image, because this

method is easily implemented in software, this is a good foundation for the future on hardware implementation. We have reason to believe that the Euler method has a broader space for development in the future of the discrete chaos, Lorenz chaotic system has a bright future in image encryption.

Acknowledgment. This paper is supported by Innovated Team Project in colleges and universities of Heilongjiang Province (No. 2012TD007), Institutions of Higher Learning by the Specialized Research Fund for the Doctoral Degree (No. 20132301110004). National Natural Science Foundation of China: 'detection and resistance of chaos sequence in a variety of periodic phenomena' (No. 61471158).

REFERENCES

[1] J. Pan, N. Qi, B. B. Xue, Q. Ding, 201 Filed Programmable Gate Array-Based Chaotic Encription Systerm Design and Hardware Realization of Cell Phone Short Message, *J. Acta Electronica Sinica,* vol. 61, no. 18, pp.180-194, 2012.

[2] L. O. Chua, T. Lin, Chaos in Digital Filters, *J. IEEE Transactions on Circuits and Systems*, vol. 35, no. 6, pp. 648-658, 2002

[3] K. J. Persohn, R. J. Poxinelli, Analyzing Logistic Map Pseudorandom Number Genearators for Preiodicity Induced by Finite Precision Floating-Point Representation, Chaos Solitons & *Fractals*, vol. 45, no. 3, pp.238-245, 2012.

[4] Y. B. Zheng, J. Pan, Y. Song, H. Cheng, Q. Ding, Research on the quantifications of chaotic random number generator, *International Journal of Sensor Networks*, vol. 15, no. 1, pp.139-143, 2014.

[5] R. J. Mattliews, On the derivation of a cliaotic encryption algoritlim, *J. Cryptologia*, vol. 13, no. 1, pp.29-42, 2012.

[6] Y. C. Zhou, L. Bao, C. L. P Chen, Image Encryption Using a New Parametirc Switching Chaotic System, *J. Signal Processing,* vol. 93, no. 11, pp.3039-3052, 2013.

[7] G. C. Wu, D. Baleanu, Jacobian Matrix Algorithm for Lyapunov Exponents of the Discrete Fractional Maps, *Communications in Nonlinear Science and Numerical Simulation*, vol. 22, no. 3, pp.95-100, 2015.

[8] Q. Ding, Y. Zu, F. Y. Zang, X. Y. Peng, Discrete Chaotic Circuit and The Property Analysis of Output Sequence, *International Symposium on Communications and Information Technologies*, pp. 1009-1012, 2005.

[9] Y. S. Liu, A video conference solution and achievement based on chaotic encryption algorithms, Computer & Digital Engineering, vol. 39, no. 1, pp.104-109, 2011.

[10] Q. Ding, J. Pan, The research of optimization parameter based on Lorenz chaotic masking secure communication, *Proc. of First International Conference on Pervasive Computing, Signal Processing and Applications*, pp.1136-1139, 2010.

[11] J. H. Lu, G. R. Chen, A new chaotic attractor coined, Bifurc Chaos, vol. 12, no. 3, pp.659-661, 2002.

[12] X. Y. Wang, Y. X. Xie, Cryptanalysis of a chaos based on cryptosystem with an embedded adaptive arithmetic coder, *J. Chin Phys*, vol. 20, no. 8, pp.80-85, 2011.

[13] L. Mohamed, S. Abhinav, Generalized Hardware Post-Processing Technique for Chaos-Based Pseudorandom Number Generators, *ETRI Journal*, vol. 35, no. 3, pp.448-458, 2013.

[14] T. Andrew, M. Kevin, Reconstructing the Key Stream from a Chaotic Encryption Scheme, *IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications*, vol. 48, no. 5, pp.124-130, 2001.

[15] H. Yang, H. Xia, Histogram modification using gray-level co-occurrence matrix for image contrast enhancemen, *J. Image Processing*, pp.782-793, 2014.