Image Encryption Algorithm Based on Wavelet Transforms and Dual Chaotic Maps

Shucong Liu
Department of Instrument, Institute of Disaster Prevention, Sanhe,Hebei Province, China
Email:fzxylsc@sina.com

Yanxing Song
Department of Instrument, Institute of Disaster Prevention, Sanhe,Hebei Province, China

Jingsong Yang
Department of Instrument, Institute of Disaster Prevention, Sanhe,Hebei Province, China

Abstract—In view of characteristics of digital image,such as bulk data capacity,high redundancy and poor security, a new image encryption algorithm was put forward by combining chaotic maps with wavelet transform. Mallat algorithm in wavelet transform firstly was used to decompose the original image, leaving only the low-frequency information, and then oversampled Chebyshev chaotic maps were used to achieve space chaos of compressed image, oversampled Logistic chaotic maps were used for encryption. Finally, security analysis of the encryption algorithm are analyzed from the perspective of key space, statistical analysis, key sensitivity analysis and so on. Simulation results show that the method can effectively compress image, the amount of information transmission is low and the key space is large enough to resist the brute-force attack and with good encryption effect.

Index Terms—**Chaotic Maps, Image Encryption, Wavelet Transform,Image Transmission**

I. Introduction

With the rapid development of Internet technology and multimedia technology, more and more information are transmitted over the network, and the digital image has become an important information carrier for the exchange of information, the security issues of the digital image are especially prominent, and the security and confidentiality transmission of the image signals in the channel are also increasing. Chaotic system is a highly complex nonlinear dynamic system, and is very sensitive to initial conditions. Because the chaotic sequences are with extreme sensitivity and unpredictability to initial conditions, and chaotic encryption with the characteristic of high-speed, high-fidelity, large amount of key, high-security, chaotic encryption technology have got extensive research in the field of image encryption[1-3]. In recent years, many encryption algorithms based on discrete chaotic sequences have been proposed, however most of the encryption algorithms are based on a single chaotic map, which with some fundamental shortcomings, such as the key space is small, the speed is slow and with weak security features. In order to improve the security of image transmission, a new method was put forward, wavelet transform decomposition compression was firstly done to the original digital image, over-sampled algorithm was applied to Chebyshev and Logistic chaotic sequences, oversampled sequences by iterations act as the encryption key, oversampled Chebyshev chaotic maps were used to achieve space chaos of compressed image, oversampled Logistic chaotic maps were used for encryption. Finally, security analysis of the encryption algorithm are analyzed from the perspective of key space, statistical analysis, key sensitivity analysis. Simulation results show that the method not only has a large enough key space to resist brute-force attack and greater sensitivity to small changes in key encryption performance, but also improves the speed and efficiency of the image, and is a suitable method for application in image encryption.

II. Wavelet transform and Mllat algorithm

$\forall f(t) \in L^2(R), \psi(t)$ is mother wavelet,if $\psi(t)$ satisfy the admissibility conditions:

$$C_\psi = \int_{-\infty}^{\infty} \frac{|\hat{\psi}(\omega)|^2}{|\omega|} d\omega < \infty \tag{1}$$

Then the continuous wavelet transform of $f(t)$ (sometimes referred to as integral wavelet transform) is defined as:

$$WT_f(a,b) = |a|^{-1/2} \int_{-\infty}^{\infty} f(t) \overline{\psi\left(\frac{t-b}{a}\right)} dt, \qquad a \neq 0 \tag{2}$$

Manuscript received May 1, 2013; revised June 1, 2013; accepted July 1, 2013.

Corresponding author：Shucong Liu, fzxylsc@sina.com

doi:10.4304/jsw.9.2.458-465

or with the inner product form

$$WT_f(a,b) = \left\langle f, \psi_{a,b} \right\rangle \quad (3)$$

where $\psi_{a,b}(t) = |a|^{-1/2}\psi\left(\frac{t-b}{a}\right)$, a is scale factor, b is displacement factor.

Mallat unified the specific structure of the wavelet basis, using the concept of multi-resolution analysis and thus put forward Mallat fast wavelet decomposition and reconstruction algorithm widely used today, which in wavelet analysis is equivalent to fast Fourier transform in Fourier analysis. Mallat algorithm can be extended to a two-dimensional image. Using Mallat algorithm, the signal can be decomposed layer by layer, each layer results of the decomposition are the low-frequency and high-frequency two parts by further decomposition to the low-frequency signals obtained by the last decomposition, such as the Eq. (4).

$$S=A_N+D_N+\ldots+D_2+D_l \quad (4)$$

A_N is the low-frequency signal obtained by the Nth layer of decomposition (appoximation signal); D_1, D_2 ,…,D_N are respectively the high-frequency signals (details of the signal) obtained by decomposition of the first layer and second layer to the Nth layer[4-6].The image compression based on wavelet transform increased the image compression ratio and compression speed, and was able to maintain the same characteristics of signal, with anti-interference in the transmission process.

III. Oversampled Chaotic Sequences

A. Oversampled Chebyshev and Logistic Chaoti cSequences.

Chaos (Chaos) system is a complex nonlinear process, the structure is complex and difficult to analyze and predict, but can provide sequences with good randomness and complexity random. Chaotic systems with a high degree of sensitivity to its initial parameters, only small differences in the initial state after a relatively short period of time will produce two completely different and unrelated chaotic sequences. The initial value has a decisive role on iterative sequence of chaotic systems. Chaotic thinking after the introduction have extensive research in the area of encryption field, the digital image encryption based on the chaos become a hot research field of information security. In recent years, many encryption algorithms based on discrete chaotic sequence are proposed, however, most of the encryption algorithms are based on the form of simple one-dimensional chaotic maps, such as one-dimensional Chebyshev map, one-dimensional Logistic chaotic map, two-dimensional Smale map, but the analysis pointed out that the security of low-dimensional chaotic system is not high enough.

Chebyshev and Logistic chaotic sequence are both one-dimensional chaotic maps commonly used in encrypted chaotic systems, their iteration equation is simple and easy to implement encryption. The iteration equation of Chebyshev and Logistic chaotic sequence are shown as Eq.(5) and Eq.(6).

$$x_{n+1} = \cos(2^k \cos^{-1} x_n) \quad x_n \in (-1,1)$$
$$k = 1,2,3\ldots$$

(5)

$$x_{n+1} = x_n \cdot \mu \cdot (1 - x_n)$$
$$\mu \in [0,4] \qquad x \in [0,1] \quad (6)$$

The oversampled operation of communication theory are introduced to the nonlinear mapping[7-8], so that the following transformation will be done on chaotic map to get another new mapping relationship ,named as oversampled chaotic map.

$$x_{n+1} = \underbrace{f(f\cdots(f(x_{n,k})))}_{p} = f^{(p)}(x_n,k) \quad (7)$$

Where $x_{n+1} = f(x_n)$ is first-order source map, p is a natural number not less than three. For a first-order chaotic map $x_{n+1} = f(x_n)$, assuming that the error point x_n is the d_n of the track,then

$$dx_{n+1} = f(x_n + dx_n) - f(x_n) \approx f'(x_n) \bullet dx_n \quad (8)$$

Assuming error dx_0 has been given in the formula, Error x_n can be expressed as

$$|dx_n| = dx_0 \prod_{i=0}^{n-1} \left| f'(x_i) \right| \quad (9)$$

If $\left| f'(x_i) \right| > 1$, systematic errors will increase over time.We assume that this extension is the exponential form:

$$dx_n = 2^{\lambda n} dx_0, or \qquad dx_n = e^{\lambda n} dx_0 \quad (10)$$

Among λ is Lyapunov exponent

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \log 2 \left\{ \prod_{i=0}^{n-1} \left| f'(x_i) \right| \right\} = \lim_{n\to\infty} \sum_{i=0}^{n-1} \log 2 \left| f'(x_i) \right| \quad (11)$$

Assume $y = g(x)$ can generate a new mapping which is $y_{n+1} = gfg'(y_n)$, similarly as shown below:

$$\frac{dy_n}{dy_1} = \frac{dy_n}{dx_n} \frac{dx_n}{dx_{n-1}} \frac{dx_{n-1}}{dx_{n-2}} \bullet\bullet\bullet \frac{dx_2}{dx_1} \frac{dx_1}{dy_1} = g'(x_n) \prod_{i=1}^{n-1} \frac{f'(x_i)}{g'(x_1)} \quad (12)$$

So Lyapunov exponent become

$$\lambda^1 = \lim_{n\to\infty} \frac{1}{n} [\ln(\prod_{i=1}^{n-1} f'(x_i))] + \ln \left| \frac{g'(x_n)}{g'(x_i)} \right|$$

(13)

Because by linear conversion, the second part of Eq.(13) equal to zero. However, for oversampled maps, the second definition of Eq.(13) is positive, and the Lyapunov exponent value is increasing. In the case of the sampling rate are four, the value of the Lyapunov exponent are as four times as source maps.Therefore, k-class Chebyshev polynomial is an map with invariant density function $p(x)=\pi^{-1}(1-x^2)^{-\frac{1}{2}}$, and its track exhibit "chaos"[9]. Two-dimensional sequences generated by the Chebyshev polynomials(k=3,p=4) are over-sampled chaotic sequences (OSCM). From this we can know oversampled sequences are new sequences realized by sampling to the source mapping sequences in every $p-1$ point. It can be seen that reference parameter p greatly increased the number of sequences generated by mapping iterating. It should be considered that the OSCM sequences generation process was extraction process to discrete-time digital signal sequences from the essence. Oversampling is the re-sampling to time-discrete digital signals, and reschedule the new sampling points to form new sequences according to the original sequence,and the new sequences are with stronger sensitivity to initial values than the source map sequences. Oversampled sequence, the performance of its track is "Chaos", is also chaotic sequence and chaotic invariant measure did not change.

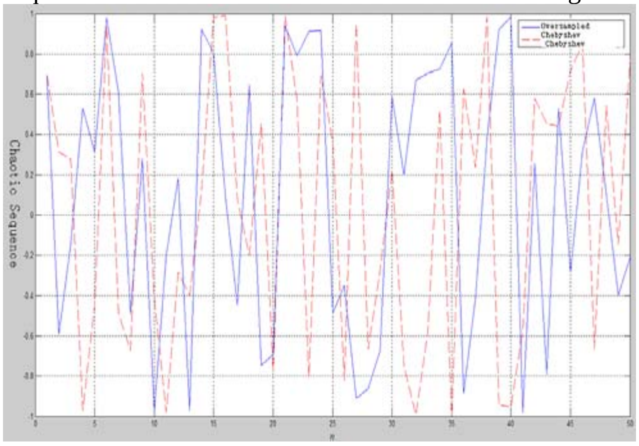


Figure 1. Chebyshev chaotic sequence and oversampled chaotic sequence

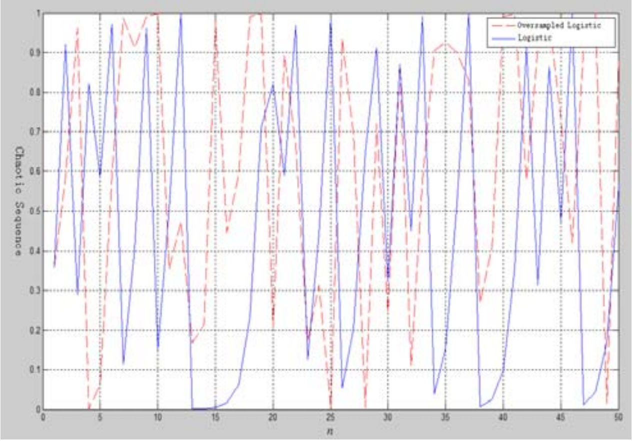


Figure 2. Logistic chaotic sequence and oversampled chaotic sequence

According to the oversampling method, the original Chebyshev and Logistic sequence are processed, Fig.1 and Fig.2 are respectively the new sequences after sampling. As can be seen from the figure, the oversampled chaotic sequences and the original sequences are with great distinction.

B. Chaotic Sequence Confidentiality.

Chebyshev sequences have great initial value sensitivity. When the initial values were taken x_{10} = 0.1 and x_{20} = 0.1000001, Chebyshev sequence generated are shown in Fig.3. The initial value of the Chebyshev sequence have only a difference of 10^{-7} , but calculation results are completely inconsistent. Likewise,the Logistic chaotic sequences are also very sensitive to the initial value. When the initial values were taken x_{11} = 0.1, μ_1 =4, x_{21} = 0.1000001, Logistic sequence generated are shown in Fig.4. It can be seen that Chebyshev and Logistic chaotic sequences are extremely sensitive to initial values,and can provide larger number, random and renewable determine signals which can be used as the encryption sequences.

In the chaotic image encryption process, Chebyshev and Logistic chaotic sequences , due to its extremely sensitive dependence on initial values and parameters , are often as chaotic encryption key. If more parameters chaotic signal generation depends on, the better the system confidentiality. The original chaotic sequence was sampled so that the original sequence changed from the one-dimensional sequence into a two-dimensional sequence, increasing the complexity of the chaotic sequence. Increasing a sampling rate force decrypters must master one more parameter by truncated analysis in the decryption process. However, the variation range of the sampling rate can be very large, which changes every one value will cause a great change of the entire sequence, as shown in Fig.5.This make it is difficult to through truncated analysis to OSCM sequence to find out the mapping function prototype for the decrypter, and grasping the laws of this sequence for eavesdropper is almost impossible. It can be seen that the complexity of chaotic mapping upgrading by sampling will further enhance the confidentiality of the system.

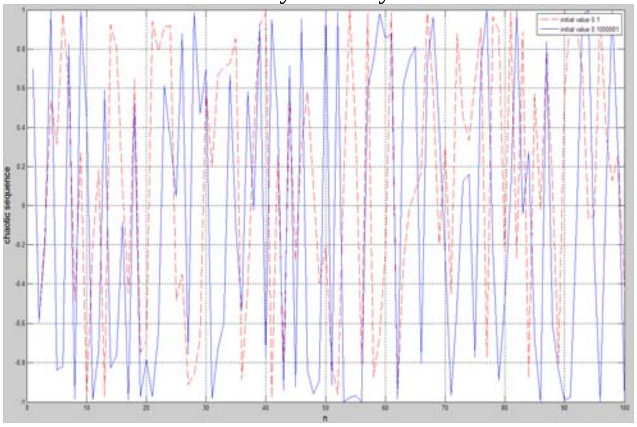


Figure 3. Eight-order Chebyshev function values with the initial value of 0.1 and 0.1000001

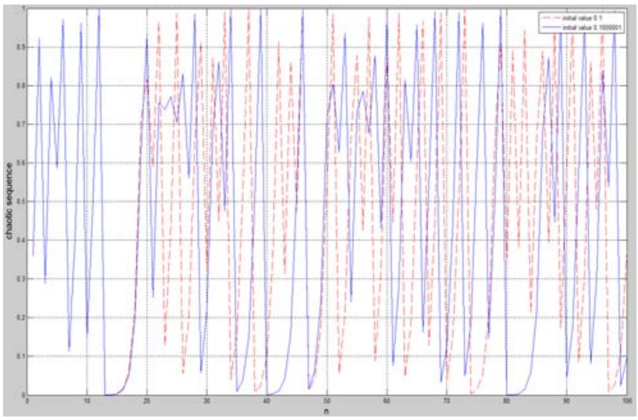


Figure 4. Logistic chaotic sequences with the initial value of 0.1 and 0.1000001

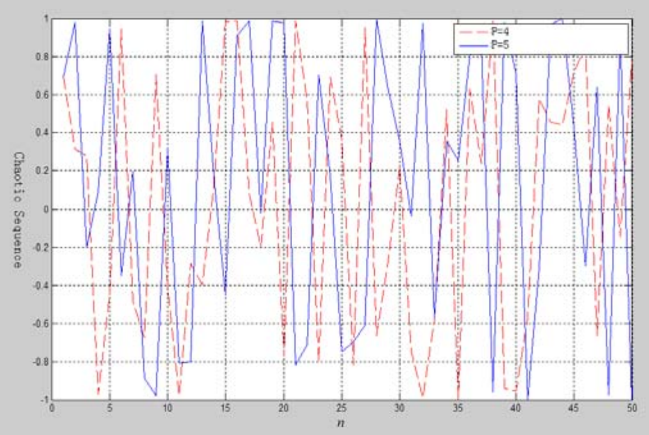
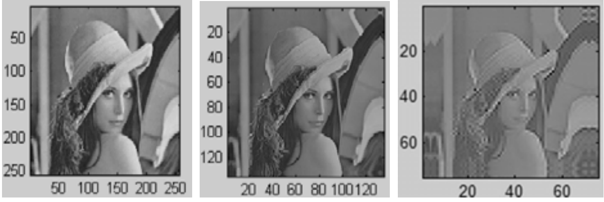


Figure 5. Chaotic sequences with different sampling parameters and initial value of 0.1

IV. Image Encryption Algorithm

A. Wavelet Transform of Image

The wavelet analysis method is a time-frequency localization analysis method which the window size is fixed but its shape can be changed and the time window and the frequency window (i.e., the window size) can be changed, having a higher frequency resolution and lower time resolution in low-frequency parts, having a higher time resolution and a lower frequency resolution in the high-frequency parts. By the wavelet transform, the original data is transformed into the frequency domain, and is decomposed into four subbands image: horizontal and vertical low-frequency sub-band image LL1; horizontal low-frequency and vertical high-frequency sub-band image LH1 ; horizontal high-frequency and vertical low-frequency sub-band image HL1; horizontal and vertical high-frequency sub-band image HH1. The subband image LL1 focuses on the most information of the original map. If the low-frequency sub-band image LL1 are encrypted by encryption algorithm, not only obtain a good effect of encryption, the key sequences required greatly reduced, increasing the algorithm speed greatly. Because the image data itself have a high degree of redundancy, so it is available to use layers of low-frequency sub-band image substitute the original image in the occasions of not high demand for image.The low-frequency part is very similar to the original two-dimensional image after wavelet decomposition, while the information performanced by the other three components are not much, which are the details of the image parts.



(a)Original image (b)First compressed image (c)Second compressed image

Figure 6. Original image and compressed image after wavelet transform

TABLE 1

CAPACITY COMPARISON OF ORIGINAL IMAGE AND DIFFERENT COMPRESSED IMAGE

	Name	Size	Bytes	Class
The size of image before compression	X	256x256	65536	uint8 array
The size of first compressed image	ca1	135x135	145800	double array
The size of second compressed image	ca2	75x75	45000	double array

Bior3.7 was used to do wavelet decomposition to the image, the two-dimensional image was decomposed by wavelet transform and low frequency parts were obtained, thus reducing the image data, according to the visual characteristics of human beings. As can be seen from Fig.6 and Tab.1, the first compression extracted the low-frequency information of the first layer wavelet decomposition of image, compression effect is better and the ratio is relatively small about one third, the second compression extracted the low frequency part of the low-frequency information obtained from the first layer by the decomposition (i.e., the low frequency part of the wavelet decomposition second layer), the compression ratio is relatively large and approximately one twelfth, the compression effect is good in visual.

B. Chaotic Encryption

Chaotic encryption are using chaotic systems to generate chaotic sequences as key sequences, which are used to encrypt the plaintext. Ciphertext by channel transmission, the receiver extract plaintext information to decryption with the chaos synchronization. One-dimensional Chebyshev maps and Logistic maps for image encryption algorithm are simple and fast for computation, but the algorithm's key space is small because only an initial value parameters affect the chaotic sequences, with poor confidentiality and security[10-13]. Based on original encryption method, The oversampled

Chebyshev sequences were used for image chaotic, and then the oversampled Logistic chaotic sequences were used to generate the encryption matrix for the image encryption, combining space chaotic with pixel value encryption. Decryption is the inverse of encryption, the encryption of the image transmission system was shown in Fig.7.

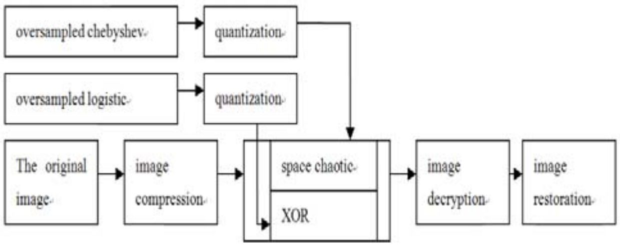


Figure 7. Image encryption and decryption system

Image space chaos:(1) Read the image pixel matrix $I_{M\times N}$, iteration was done by Chebyshev chaotic system, with different initial value x_{10} , x_{20} and sampling parameters $p1$, $p2$, and do oversample processing to Chebyshev sequences to producing two one-dimensional chaotic sequence respectively, take some value after several values to generate a chaotic sequence C1={C_{11},C_{12},C_{13}…C_{1M}} , C2={C_{21},C_{22},C_{23}…C_{2N}}.

(2) The generated chaotic were rearranged in a order from small to large, sequences sorted are X1= {X_{11}, X_{12}, X_{13} … X_{1M}}and X2={X_{21}, X_{22}, X_{23} … X_{2N}}. Each element of the original sequence C1 was identified the location in the sorted sequence X1 successively, at the same time generating a position sequence Xh1={h1,h1,h3,…h_M}, elements of the original sequence C2 were identified the location in the sorted sequence X2, generating a position sequence Xh2={k1,k2,k3, …k_N}. h1, h1, h3, ... hM are positive integers in the interval [1, M], k1,k2,k3, …k_N are positive integers in the interval [1, N]. According to the elements [hi] (i = 1, 2, 3, ..., M) of position sequences ,the entire ith row of the image matrix were moved to the [hi]th line. After the completion of all the rows mobiling , then the same moving was done to all the columns, according to the elements [kj] (j = 1,2,3, ..., N) of position sequences, the jth entire column was moved to the [kj]th column to obtain chaotic matrix after $I_{M\times N}$, so the rows and columns chaos of the image were completed to achieve the first encryption of image.

The pixel value encryption: The simple pixel position encryption does not alter the original image pixel statistics information, therefore, the images need for further pixel encryption after the position encryption. Pixel gray value encryption was using pixel value disturb vector generated by chaotic maps to disturb the pixel gray value of original image to hide the information of the original image.

(3) Iteration with the initial value x_{11} , μ_1 , x_{21} , μ_2 and sampling parameters $p3$, $p4$, by the Logistic chaotic sequences, some numbers after several numbers were selected for chaotic sequences generated, and then the remainder, rounding, quantization of each iteration value was achieved successively, respectively producing two chaotic sequences L1={L_{11},L_{12},L_{13}…L_{1M}},L2={ L_{21},L_{22},L_{23}…L_{2N}}. L1 bit XOR the row of $I^r_{M\times N}$, encryption was done to L2 and the column of $I^r_{M\times N}$ to achieve final image encryption. The transformed image matrix have been completely chaotic, as shown in Fig.8 (b), it can effectively improve the ability to anti-exhaustive.

(4) The decryption process is the inverse of encryption and need the key (x_{10} , x_{20} , x_{11} , μ_1 , x_{21} , μ_2 , $p1$, $p2$, $p3$, $p4$).

V. Simulation Results and Analysis.

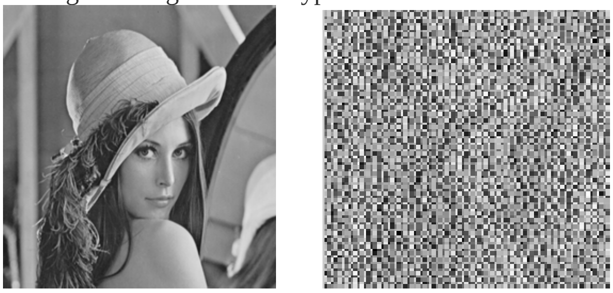
A. The Key Space Analysis

In the encryption scheme, the key were (x_{10} , x_{20} , x_{11} , μ_1 , x_{21} , μ_2 , $p1$, $p2$, $p3$, $p4$), $p1$, $p2$, $p3$ and $p4$ are integers, each parameter of the rest was double-precision real numbers with fifteen bit, so the possible values were 10^{15} for each parameter, the key space were at least about 10^{90} , and encrypted image had a sufficiently large key space to resist exhaustive attack.

B. The Key Sensitivity Test

(1) The experiment use pictures Lena (256 * 256), the initial value of the Chebyshev chaotic sequences were selected as x_{10} = 0.4, x_{20} =0.6, $p1$ =3, $p2$ =4,the initial value of Logistic chaotic sequences were x_{11} =0.4, μ_1 =3.26, $p3$ =3, x_{21} =0.6, μ_2 =4. 0, $p4$ =4.Fig. 8(a) is the original image, Fig.8(b) is the encrypted image.

Fig.9(a) is the decryption image when the key is correct, decrypting with the correct key would recover the original image. When the decryption using the wrong key x_{10} =0.4000001, x_{20} =0.6, x_{11} =0.4, μ_1 =3.26, x_{21} =0.6, μ_2 =4. 0, $p1$ =3, $p2$ =4, $p3$ =3, $p4$ =4,the decryption image was completely invisible, as shown in Fig.9(b). It can be seen that the key have a slight change, it also could not see the outline of the original image after decryption.

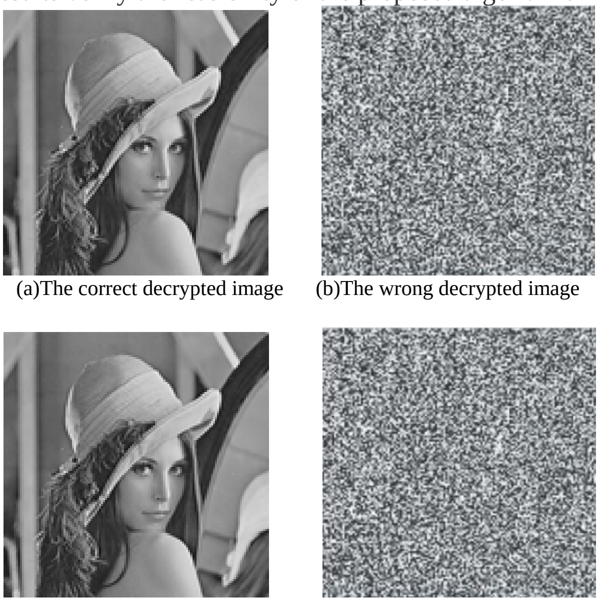


(a)The original image (b)The encrypted image

Figure 8. Original and encrypted image

(2) When select the wrong decryption sampling parameter p1,and the other parameter unchange, x_{10} =

0.4, x_{20} =0.6, x_{11} =0.4, μ_1 =3.26, x_{21} =0.6, μ_2 =4. 0, $p1$ =4, $p2$ =4, $p3$ =3, $p4$ =4, it samely will not get the original image,as shown in Fig.9(d) . The same operation is performed to other sampling parameter($p2$, $p3$, $p4$), the result is still the same. Add sampling parameters makes the confidentiality of image transmission encryption further improve. Therefore, the algorithm is fully sensitive to initial values, has good ability to resist attack. The encrypted image have a sufficiently large key space to resist brute-force attacks, the experimental results verify the feasibility of the proposed algorithm.



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

(c)The correct decrypted image (d)The wrong decrypted image(p1=4)

Figure 9. Decrypted image

C. The Pixels Correlation Coefficient Analysis

The original image have a relatively high correlation coefficient of adjacent pixels, in order to prevent the theft of illegally obtaining image information, the encrypted images should have a relatively low correlation coefficient of adjacent pixels. In order to analyze the pixels correlation coefficient of the image and the encryption image, the level, the vertical and the diagonal directions of plaintext image and the encryption image, respectively, were randomly selected 7680 pairs of adjacent pixels and were calculated according to the following formula[14-17].

Statistical mean: $$E(x)=\frac{1}{n}\sum_{i=1}^{n}x_i \tag{14}$$

Statistical variance: $$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{15}$$

Statistical covariance:

$$COV(x,y)=\frac{1}{N}\sum_{i=1}^{N}E(x_i-E(x))(y_i-E(y)) \tag{16}$$

correlation coefficient: $$r_{xy}=\frac{COV(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{17}$$

The correlation coefficients of the adjacent pixels in the horizontal, vertical and diagonal directions were respectively calculated according to Eq.(14)~ Eq.(17) .The simulation results are shown in Tab.2.

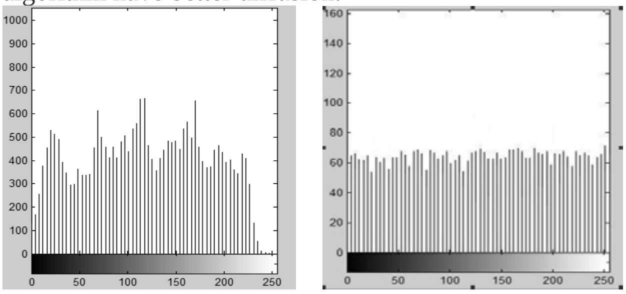
TABLE 2
ADJACENT PIXELS CORRELATION COEFFICIENT BEFORE AND AFTER ENCRYPTION

Correlation coefficient	The level	The vertical	The diagonal
The original image	0.9231	0.8254	0.8721
The encrypted image	0.0082	0.0053	0.0081

As can be seen from Tab.2, the adjacent pixel correlation coefficients of the encrypted image on the horizontal, vertical and diagonal directions are much smaller than the plaintext image, which achieved the purpose of the encryption.

D. Statistical Analysis

Fig.10 (a) is the histogram of the original image and Fig.10 (b) is the histogram of encryption image. As can be seen, the image encrypted by the chaotic system tend to be uniform distributed (pixel values tend to more uniform distribution), and the statistical characteristics are complete different from the original image, it can be seen that ciphertext generated by the encryption algorithm have better diffusion.

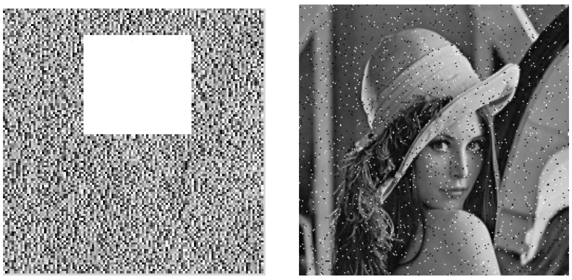


(a) Histogram of original image (b) Histogram of encrypted image

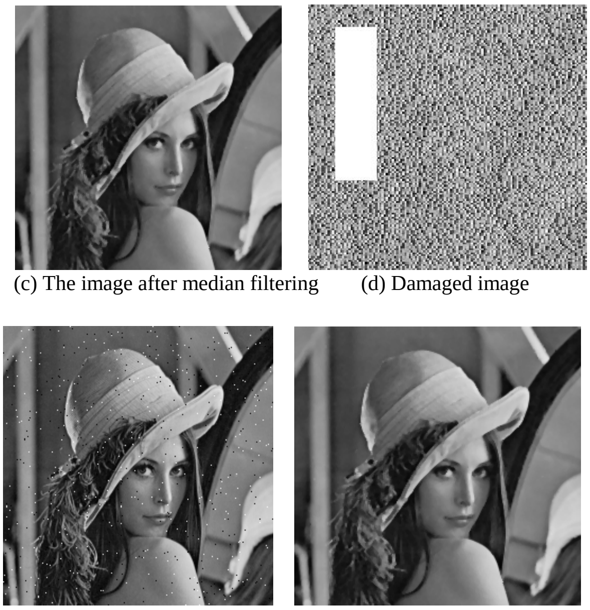
Figure 10. Histogram

E. Shear Test Analysis

Image may be damaged during transmission, resulting in the image information missing. In this case, encrypted image lack of information can restore the original image information by decryption method. As shown in Fig.11, the image is cut and with noise in the recovery image, but not affect understanding of information image, the algorithm can restore the vandalism damaged image to some extent.



(a)Damaged image (b) Restored image



(c) The image after median filtering (d) Damaged image

(e) Restored image (f) The image after median filtering

Figure 11. Demaged image and restored image

The restored image is relatively clear, although appeared small points in the recovery, uniformly distributed in the whole image, similar to the effect of the salt and pepper noise, but it could be very close to the original image after median filtering in which those small point could be eliminated. From the simulation results, the encryption algorithm have resistance to damage attack and could restore decrypted image patches by median filtering, and get a satisfactory result.

VI. Conclusions

The digital images encryption and decryption algorithm by oversampled Chebyshev and oversampled Logistic dual chaotic maps based on wavelet transform was put forward. Two-dimensional discrete wavelet transform was firstly used for image decomposition and compression, the compressed images are then further encrypted by oversampled Chebyshev and oversampled Logistic dual chaotic sequences. Simulation results show that this algorithm can increase the transmission speed of the image, the generated sequences have a very large key space, with high operation efficiency and good encryption effect, and enhance the image of confidentiality and security.

Acknowledgments

This work was financially supported by Special Fund of Fundamental Scientific Research Business Expense for Higher School of Central Government (Projects for creation teams ZY20120101).

References

[1] Feng Huang, Xilong Qu. Design of Image Encryption Algorithm Based on Compound Two-dimensional Maps. Journal of Software, Vol.6, No.10 (2011), pp.1953-1960

[2] *Yongqiang Chen, Yanqing Zhang, Hanping Hu, Hefei Ling.* A Novel Gray Image Watermarking Scheme. Journal of Software, Vol 6, No.5 (2011), 849-856, May 2011

[3] *Jun He, Zhi-bin Li, Hai-feng Qian.* Cryptography based on Spatiotemporal Chaos System and Multiple Maps. Journal of Software, Vol 5, No 4 (2010), 421-428, Apr 2010

[4] Sun Kehui, Shang Fang,Zhong Ke. New image encryption scheme based on OCML and TD-ERCS map [J]. Computer Applications Studies, Vol. 2, No. 25, 2008, pp.518-520.

[5] Li Mingwei, Feng Yong, Li Linjing. An Image Encryption Approach Based on a Two-dimensional Reversible Map[J]. Computer Simulation, Vol. 2, No. 25, 2008, pp. 227-331.

[6] Hyung Suk, Chong Koo An. A Study on the Improvement of Wavelet Packet Algorithm for Image Compression[J] . IEEE Audio Engineering, Electronics, Communication, 2002, 4(2): 379-382.

[7] Yu.Yinhui. Wang. shuxun. Han Yan. Analysis of the performance of balance of digital multivalue based on Chebyshev chaotic sequence [J]. Second International Symposium,ISICA 2007.Proceedings,2007.568-574.

[8] Hongtao Zhang.Jiehang Guo,Huiyun Wang.Runtao Ding.Oversampled Chaotic Map Binary Sequences Definition Performance and Realization.The 2000 IEEE Asia-pacific conference on circuit and system Tianiin 2000.618-621.

[9] Liu Wei. Design of 4-phase Chaotic Map of Oversampled and its Applications in Spreading Spectrum Communication[J] Mathematics in Practice and Theory, Vol. 11, No. 39, 2009, pp.98-103.

[10] MATFHEWS R.On the derivmion of a chaotic encryption algorithm [J].Cryptologia, 1989, 13(1):29-42.

[11] FRIDRICH J.Symmetric ciphers based on two-dimensional chaotic maps [J].Int J Bifurcation and Chaos, 1998, 8(6):1259-1284.

[12] Gao Fei, Li Xinghua. Bit Image Encryption Research Based on Chaotic Sequence [J]. Journal of Beijing Institute of Technology, Vol. 5, No. 25, 2005, pp. 447-450.

[13] GUAN Z H, HUANG F J,GUAN W J.Chaos-based image encryption algorithm[J].Physics Letter A,2005,346:153-157

[14] RenHonge,ShangZhenwei,WangYtmnzahi,et a1.A Chaotic Algorithm of Image Encryption Based on Dispersion Sampling[A].The 2007 IEEE Eighth International Conference on Electronic Measurement and Instruments [C] 2007.2-836~2-839

[15] Tong Xiaojun,Cui Minggen.A New Chaos Encryption Algodthm Based on Parameter RandomlyChanging[A].The 2007 IFIP International Conference on Network and Parallel ComputingWorkshops[C].2007.303~307

[16] XiaoHuangpei,ZhangGuoji.An Image Encryption Scheme Based on Chaotic Systems[A].Proceedings of the 2006 IEEE Fifth International Conference on Machine Learning And Cybernetics[C].2006.2707~2711

[17] Pareek N K,Vinod Patidar,Sud K K.Image Encryption Using Chaotic Logistic Map[J].Image and Vision Computing ,2006,24:926~934

Shucong Liu, Hebei, China. Birthdate: November, 1983, received her master degree in Measuring Testing Technology and Instruments from Jilin University of China. She is currently working as a full-time lecture in Institute of Disaster Prevention. She has published six journal papers. Her research field is image signal processing and computer, database theory. Postal address: Department of Instrument, Institute of Disaster Prevention, Yanjiao District, San he City, Hebei Province. China 065201.

Yanxing Song Ph.D, Hebei, China. Birthdate: March, 1980, graduated from Harbin Institute of Technology of China. She is a lecturer of Institute of Disaster Prevention. She has published twenty journal papers. Her research direction is Image measurement and signal processing.Postal address: Department of Instrument, Institute of Disaster Prevention, Yanjiao District , San he City, Hebei Province. China 065201.

Jingsong Yang, Ph.D, Hebei, China. Birthdate: May, 1975, graduated from Jilin University of China. She is a lecturer of Institute of Disaster Prevention. She has published twenty journal papers. Her research direction is Embeded System Development and network engineering.