ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 11, November 2017

A new image encryption algorithm based on logistic chaotic map

DHANALAXMI BANAVATH, SRINIVASULU TADISETTY
Department of Electronics and communications,
KU College of Engineering and Technology, Kakatiya University, Waranagal-506009.
Telanagana, INDIA.

Abstract: A new self-adaptive image encryption algorithm is proposed to improve its robustness. Under this algorithm, a gray image or color image was divided into 2×2 size blocks. A corresponding size of matrix in the top right corner was created by the pixel gray-scale value of the top left corner under Chebyshev mapping. The gray-scale value of the top right corner block was then replaced by the matrix created before. The remaining blocks were encrypted in the same manner in clockwise until the top left corner block was finally encrypted. This algorithm is not restricted to the size of image and it is suitable to gray images and color images, which leads to better robustness. Meanwhile, the introduction of gray-scale value diffusion system equips this algorithm with powerful function of diffusion and disturbance.

Key words: Image encryption, colour image, Chaotic algorithm, Decryption.

1. Introduction

There are many different image encryption schemes, such as spatial domain encryption [1-6], frequency domain encryption [7], and adaptive encryption [9-11]. As the chaotic map has the sensitivity to the initial value and the parameter, the image encryption algorithm based on the chaotic map is more efficient and the high security. The high-dimensional chaotic map can be used to discretize the pixel values of the image, such as the use of only one-dimensional cat mapping, two cat mapping, Discrete index chaotic mapping and other technologies to achieve image encryption.In addition, based on the look-up table technology, switching technology [4] and a variety of mapping combinations [1] program is also presented. [7] based on the frequency domain to encrypt the image, the basic idea (Discrete Wavelet Transform (DWT)), and then scrambled the resulting low-frequency and vertical low-frequency (LL) matrix. Finally, the inverse discrete wavelet transform is used to obtain the encrypted image. But this does not change the statistical information of the image pixels.

In the paper, a new adaptive image scrambling algorithm is proposed. Compared with the traditional image-based encryption technology based on airspace or frequency domain, the algorithm scrambles and encrypts the other part of the data according to the part of the data of the image white body. After the image can effectively prevent the known plain attack. '10' pointed out that the algorithm's three defects: do not change the original image pixel statistics; select the plain attack can reduce the complexity of the encryption algorithm; use 128 options The key of the algorithm can be completely

restored and the improved method is put forward: In the process of one round encryption, the S-box and the adaptive scrambling are used in the round key and / The improved algorithm can solve the above three defects

The '11' clever use of wave propagation to achieve image encryption. In the encrypted image, the image can be seen as a lake, through the analog wave on which to spread for encryption, and the wave can be superimposed, the effect of superposition is equal to the effect of the superposition of each wave. The wave propagation replaces the pixel values of the image pixels, and the adaptive structure will spread quickly to the entire ciphertext for any minor changes. Because of its use of modulo and XOR operation, the execution speed of the algorithm is improved. The document fills the input image so that it becomes a matrix of rows and columns that are multiples of four. But the literature did not explain how to restore the original image after decryption.

Based on the analysis of the characteristics of chaotic sequences, this paper proposes a new adaptive structure and gray value diffusion mechanism. The algorithm can achieve the performance requirements by two rounds of encryption.

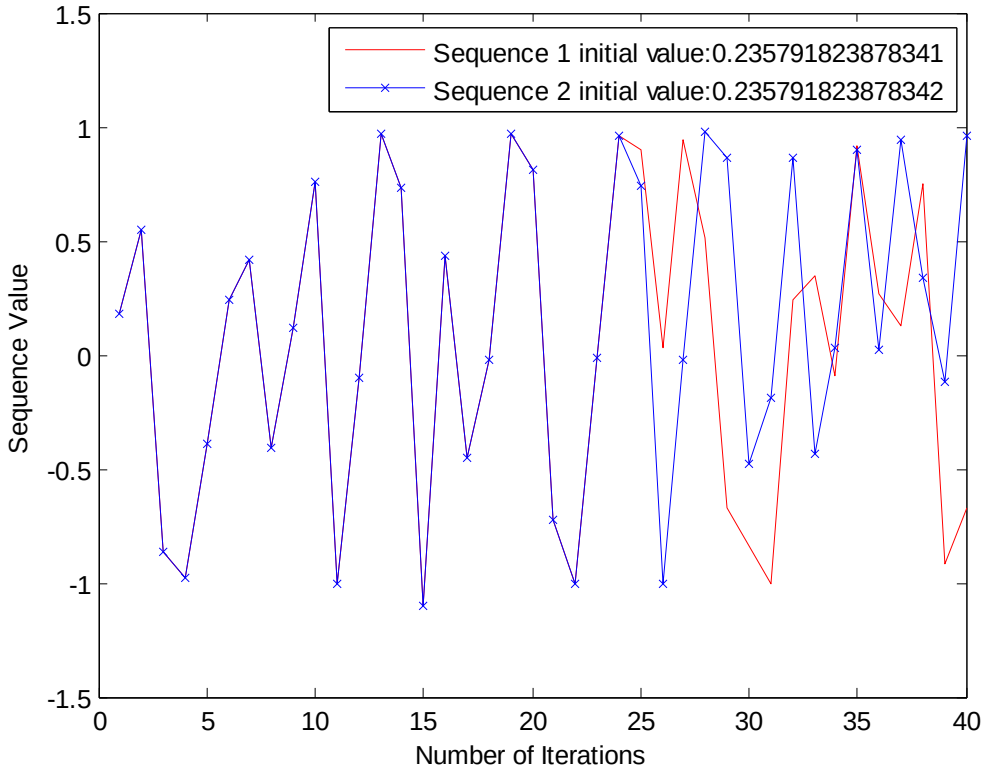


Figure 1 Chehyshev mapping of the two sequences of the initial difference of 10^{-15} chaotic orbit separation

2. Chebyshev mapping and grayscale diffusion mechanism

2.1. Chebyshev mapping

It is generally believed that chaos is a seemingly random, similar random phenomenon in the deterministic system, with the overall stability of local instability, sensitive dependence on the initial conditions, long-term unpredictability and other characteristics [8]. Commonly used one-dimensional chaotic maps are Logistic, Kent., Chebyshev mapping. In this paper, Chebyshev mapping is used. The discrete form is defined as follows:

$$x(n+1)=\cos\left(k\ \arccos\left(x(n)\right)\right);\quad -1\le x(n)\le 1 \tag{1}$$

When k is the value of 4, the mapping produces the sequence x_0. In the interval $[-1,1]$ traversal, autocorrelation for the δ function, cross-correlation is 0. The small changes in the parameters or initial conditions of the chaotic system will affect the chaotic trajectory to a large extent. As shown in Fig. 1, the two chaotic sequences with initial values differ by 10^{-15} are rapidly separated after 24 iterations. The number of iterations n_0. And the initial value x_0. Can be used as the encryption algorithm key.

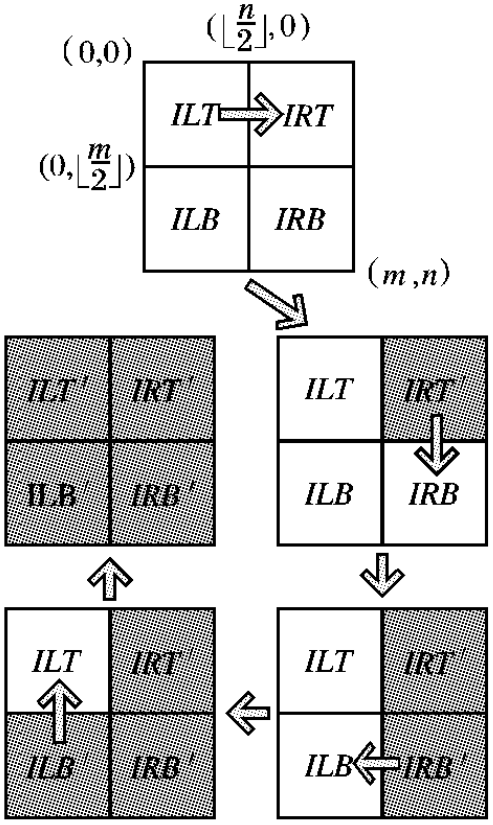


Figure 2 2x2 block structure of Adaptive image encryption

2.2. Gray-level Diffusion Mechanism

Gray-level Diffusion Function is defined:

$$I_b^{'}(i,j)=\left(\left(I_b(i,j)+A(i,j)\right)\bmod\ N\right)\oplus I_0 \tag{2}$$

where i and j are the image block matrix I_b, respectively. Row and column of the index ; $I_b(i, j)$ for the replacement before the gray value; $I_b^{'}(i, j)$ is the gray value after the replacement; I_0 is the gray value of the last replacement, the initial value takes the same value of all gray values of the previous block matrix; *N* is The gray scale is 256 for the 256 gray scale image. The mode is to keep the replaced gray value in the gray scale. In order to make the tiny changes to the plaintext quickly spread to the entire ciphertext, the initial value of the Chebyshev mapping x_0. To transform:

$$x_0 = \frac{I_0}{256} \times x_0 \tag{3}$$

Preference of the equation (1). To make the chaotic orbit separate and continue iterations $i \times j$ times with the structure I_b. Such as the large matrix A, makes:

$$A(i, j) = \lfloor x_n \times N \rfloor \tag{4}$$

Where $\lfloor \bullet \rfloor$ round operator

The inverse transformation of (2) is:

$$I_b^{'}(i, j) = \left(\left(I_b^{'}(i, j) \oplus I_0 + N - A(i, j) \right) \bmod N \right) \tag{5}$$

3. Adaptive image encryption algorithm based on chaotic mapping

This paper proposes a new structure of Adaptive image encryption, as shown in Figure 2. Adaptive image encryption and decryption required to divide the input image. Image classification method is commonly used to fill the image first and then divided into blocks of equal size, the decryption process also needs to be removed to fill part of the image in the end. This article without using the fill method, block size may be different. The first block encryption and decryption process does not depend on the 2nd block size depends only on the 2nd block of pixel-by-pixel values.

First, let the size of the input image I be $m \times n$, m and n . Pair I clockwise into 4 pieces, *ILT*-left corner, right corner of *IRB*, ILB_0 on the lower left.

3.1. Encryption Process

Combining the Chebyshev mapping and the gray scale diffusion function introduced in Chapter 1, the encryption process is:

1) The input image I is divided into four sub-blocks.
2) Encrypt each sub-block clockwise. If *ILT* is used to encrypt *IRT*, the *IRT* value of the gray value of each pixel of I_o is calculated first:

$$I_0 = \bigoplus_{(i,j) \in I_b} ILT(i, j) \tag{6}$$

Obviously, I_0 the values do not depend on the size of the *ILT*, depending only on the pixel values of the *ILT* pixels.

3) According to equation (3) initial value x_0 for the Chehyshev map transformation and iterative n_0. According to equation (4) constructing matrices A.
4) In the order of behavior, the *IRT* is traversed in ascending order, and the gray value of each pixel is replaced by the equation (2), and the value of I_0 is updated once every other time, which is equal to the pixel value after replacement. After the traversal, get encrypted $IRT_0^{'}$.
5) Use the encrypted IRT 'application $2)\ \square\ 4)$ to encrypt the *IRB* to get *IRB'*. Similarly, *IRB* 'encrypts *ILB* to get *ILB'*, *ILB* 'encrypts *ILT* to get *ILT'*, and combines *ILT '*, *IRT'* , *IRB '*, *ILB'* to get the encrypted image *I'*, and the end of the round of the encryption operation.

3.2. Decryption Process

1) Is consistent with the encryption process 1).
2) Decrypt each sub-block counterclockwise. *ILB* 'is used to decrypt *ILT'*, and the exclusive-OR value of [LB gray value of each pixel] is calculated I_0:

$$I_0 = \underset{(i,j)\in I_b}{\oplus} ILB^{'}(i,j) \qquad (7)$$

Likewise, the value of I_0 does not depend on the size of *ILB '*, depending only on the pixel values of each pixel *ILB'*.

3) Consistent with encryption process 3).
4) To the main sequence, ascending traverse *ILB'*, formula (5) to replace the pixel gray value, update the I_0 value after each traversal, which is equal to the replacement value. end of the traverse are decrypted *ILT*.
5) Use *IRB* 'Apply 2) – 4) Ground, IRT' Decrypt IRB 'Get IRB, ILT. Step Decrypt IRB' Get ILB. Similar to 'decrypted IRT" to get IRT, combined with ILT, IRT, IRB, ILB to get the decrypted image I, the end of a decryption operation.

3.3. Color image encryption and decryption

The color image consists of three color components, namely red (R), green (G) and blue (B). The encryption and decryption process of the gray image can be transplanted to the color image, the three components are independently encrypted / decrypted, and the final encryption / decryption result is combined into an encrypted / decrypted color image.

Table 1: Correlation Coefficent of adjacent pixels in plain text and ciphertext images

Direction	Lena		Qing Ming Shang hetu					
	Clear Text	Ciphertext	Cleartext			Ciphertext		
			R	G	B	R	G	B
Level	0.98	0.05	0.85	0.80	0.78	-0.04	0.06	-0.01
Vertical	0.97	0.04	0.89	0.86	0.82	-0.08	0.00	0.17
Diagonal	0.95	0.02	0.77	0.72	0.66	-0.04	-0.01	-0.016

4. Experimental results and safety analysis

In the experiment, the plaintext is a 512 x 512 Lena grayscale image and a 511x 229 fresco color picture; key. For 128, x_0 . For O.3453.

4.1. Statistical analysis

4.1.1. Histogram

Figure 3 shows the comparison of histograms before and after Lena image encryption. Figure 4 shows the comparison of the histogram before and after the encryption of the river. It can be seen from the figure that the encrypted histogram is relatively uniform, effectively masking the distribution of the pixels in the plaintext image, making the statistical analysis more difficult.

4.1.2. pixel correlation

A good encryption algorithm key space should be large enough to resist brute force attack. This key,. Range of values 1024, iteration count n. Values for the positive integers. In Matlab, simulation of precision of 101 '5, positive integers are represented by 16-bit binary, the key space is 2x10'5 x2'6zz 1.3107 x102. Thus there is a large enough keyspace to resist brute force attack.

Table 2: Key change sensitivity test

Rounds	LENA	Plainext and Cipher text
1	0.99623	0.99607
2	0.99634	0.99615
3	0.99597	0.99650
4	0.99597	0.99650
5	0.99612	0.99588

4.2. Key sensitivity analysis

Image encryption algorithm is an important measure of the avalanche effect. Strict avalanche effect that, when you change any 1 bit in the plaintext or keys, almost all of the encrypted data will be changed. The experiment, we will be,. From 0.345 3 101 with '5, make it a 0.345300000000001, and compare the encrypted cipher text changes. Table 2 shows that the keys small change in the ciphertext data change rate average is above 99.5%. Figure 4 is a sensitivity test results round of encryption keys.

Table 3: Clear Change after 1NCPR & UACI

Rounds	**Lena**		**Qing Ming Shang he TU**	
	NPCR	**UACT**	**NPCR**	**UACI**
1	0.49780	0.16695	0.49564	0.16646
2	0.99610	0.33521	0.99589	0.33555
3	0.99625	0.33443	0.99626	0.33417
4	0.99594	0.33414	0.99603	0.33467

4.4. Differential analysis

In order to test the effect of a pixel change on the entire ciphertext, two methods are usually used: the Number of Pixels Change Rate (NPCR) and the Unified Change Intensity (UACI). In the experiment, we changed the last 1 bit of the Lena image from 1 to 0, and the last one of the R component of the Qingming River was changed from 1 to 0. Table 3 lists the rounds of NPCR and UACI values. As can be seen from Table 3, after two rounds of encryption, the energy relationship is relatively stable, suitable for embedded robust watermark, and P, B frame suitable for embedded in the motion vector fragile watermark, the next step in the I frame embedded copyright And then the watermark information is embedded in the motion vector of P and B frames, so as to realize copyright authentication and content authentication.

NPCR values were basically stable at around 0.99, UACI also fluctuated around 0.33. The first round of NPCR and UACI values is lower than the theoretical value because the changed 1-bit data is at the end of the plaintext, that is, the last encryption of the adaptive structure, so only affects the IRB and ILB two sub-blocks.

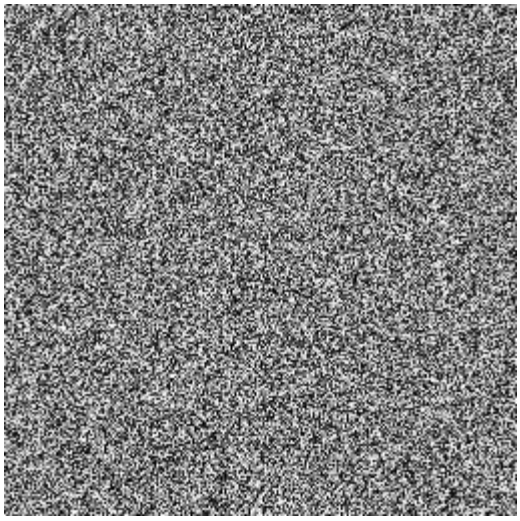
4.5. Performance analysis

In the gray scale diffusion, a simple addition, modulo and exclusive OR operation are used for each gray value of the image, and the time complexity is O (n). In addition, each sub-block encryption only needs to construct an auxiliary matrix A equal to the size of the previous sub-block, and as long as two rounds of encryption can achieve the required performance.

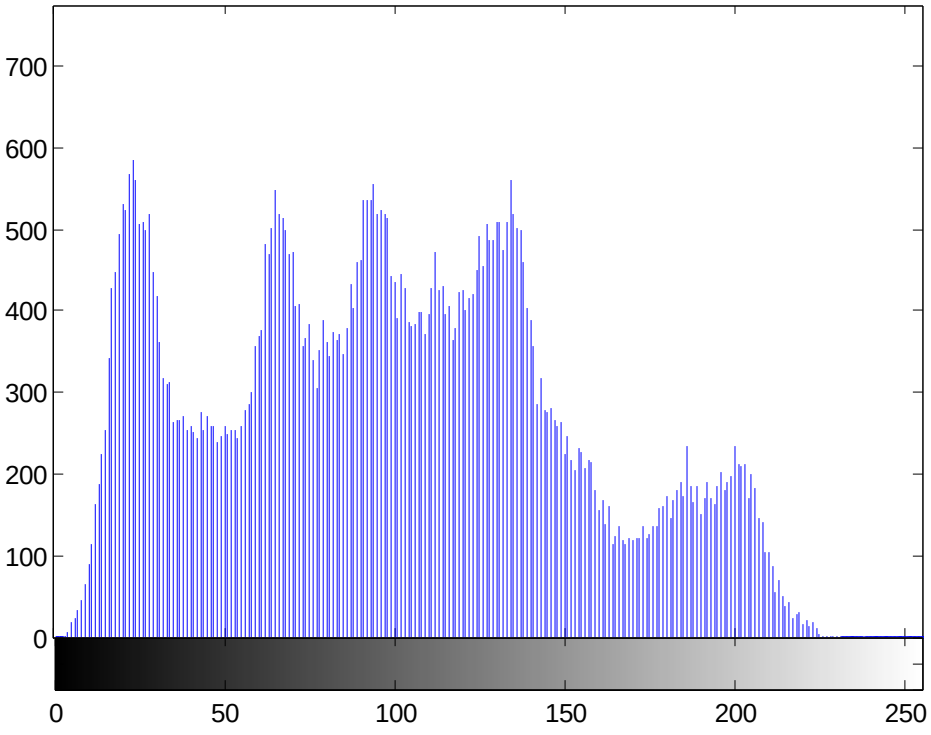
5. Conclusion

This paper presents a new adaptive structure and gray-scale diffusion mechanism. The adaptive structure makes the tiny changes to the plaintext quickly spread throughout the ciphertext. The gray-scale diffusion mechanism makes the statistical information of the plaintext hidden, which can effectively resist the statistical analysis attack. The experimental results show that the algorithm has strong robustness and sensitivity to the key, and can effectively resist statistical analysis, exhaustive attack and differential attack.

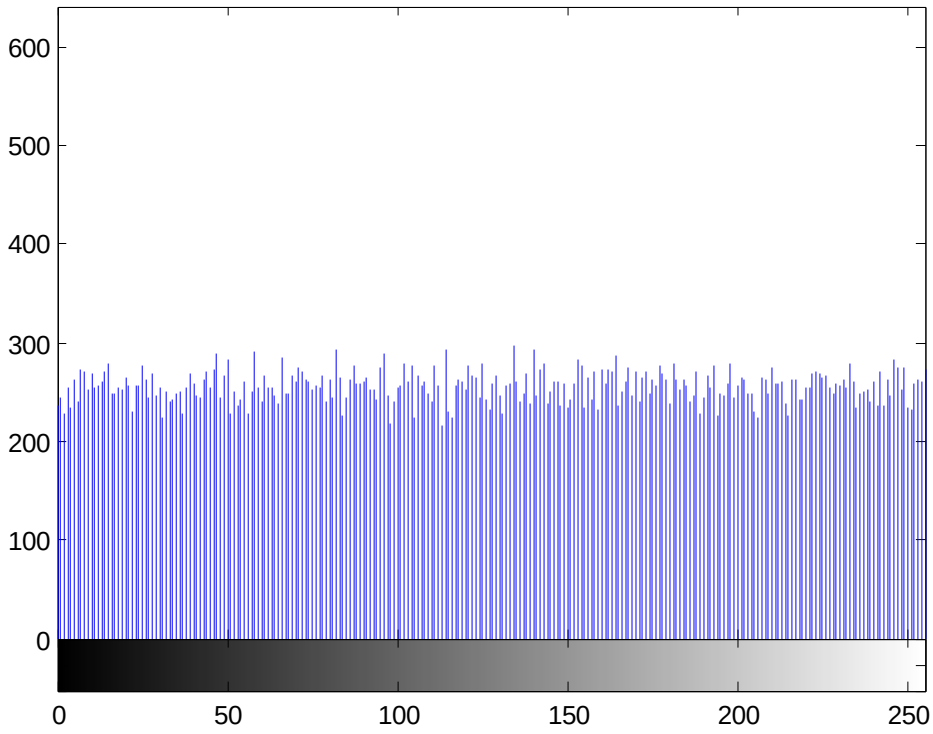
(a) Plain text



(b) Cipher text



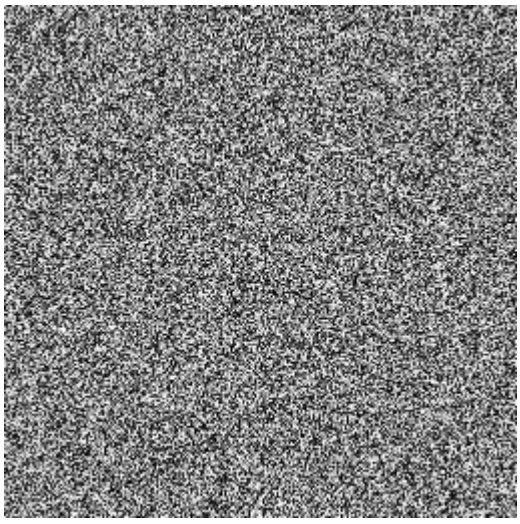
(c) Plain Image Histogram



(d) Ciphertext Histogram

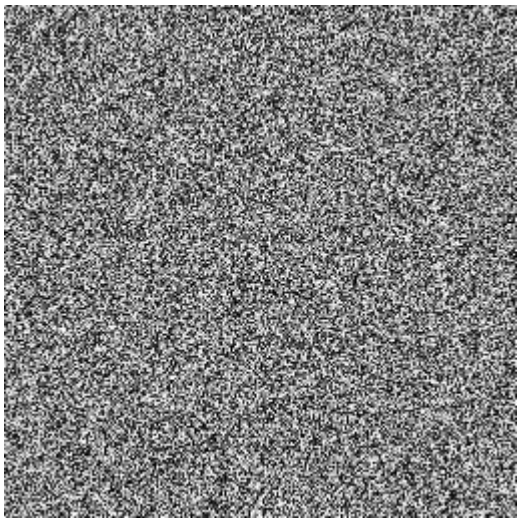
Figure 3 Lena plaintext and ciphertext histogram

(a) Expressly



(b) Ciphertext

(c) Decryption of the original key results



(d) Keys change the 1-bit decryption results

Figure 4 Key sensitivity test results

Acknowledgments

I very much thankfull to UGC India, for providing research fellowship .

References:

[1] Chen Guanrong, Mao Yaobin, Chuick, "A Symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals, 2004, vol.21, no. 3, pp. 749-761.
[2] Guan Zhihong, Huang Fangjun, Guan Wenjie, "chaos based image encryption algorithm," Physics letters A, 2005, vol. 346 , no. 1/2/3, pp. 153-157.
[3] Zhang Linhua, Liao Xiaofeng, Wang Xuebing, "An Image encryption approach based on chaotic Maps," chaos, solitons & Fractals, 2005, vol.24, no. 3, pp. 759-765.
[4] Wong K W, Kwok B S H, Yuanch, "An efficient diffusion approach for chaos-based image encryption,". Chaos, Solitions & Fractals, 2009, vol. 41, no. 5, pp. 2652-2663.
[5] Huang C K, Nien H H, "Multi chaotic systems based pixel shuffle for image encryption," Optics Communications, 2009, vol.282, no.11, pp. 2123-2127.
[6] Chen Gang, Zhao Xiaoyu, Li Junll. "A self adaptive algorithm on image encryption," Journal of software, 2005, vol.19, no.11, pp.1975-1974.
[7] Xiao F, Gao XP, "An approach for short-term prediction on time series from parameter-varying systems," J Softw, vol.17, pp.1042–1050, 2006.
[8] Ye G, Wong KW, "An image encryption scheme based on time-delay and hyperchaotic system." Nonlinear Dyn, 2013, vol. 71, pp.259–267.
[9] Zhang G, Liu Q, "A novel image encryption method based on total shuffling scheme," Opt Commun, 2011, vol. 284, pp.2775–2780.
[10] Zhang XP, Zhao ZM, "Chaos-based image encryption with total shuffling and bidirectional diffusion," Nonlinear Dyn, 2014, vol. 75, pp.319–330.
[11] Zhou Q, Liao X, "Collision-based flexible image encryption algorithm," J Syst Softw, 2012, vol. 85, pp.400–407.