2014

ISSN : 0974 - 7435 Volume 10 Issue 24

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(24), 2014 [15795-15806]

Design of digital image encryption algorithm based on mixed chaotic sequences

Tao Wang
Department of Computer Science and Technology, Shaoxing University, Zhejiang, (CHINA)
Department of Computer Science and Technology, Shaoxing Vocational & Technical, Zhejiang, (CHINA)
Email: wangtaolt8@yeah.net

ABSTRACT

Digital image scrambling is to transform a digital image, to make it unrecognizable and become another chaos images without obvious meaning. If the operator knows the algorithms, he can reconstruct the original image from the chaos image by using the certain algorithms. Image scrambling encryption technology that based on Chaos Theory encrypts the image data stream through using the chaotic signal. It has the advantage like high security, encryption speed, large key space, and good scrambling effect. This paper studies the "extraordinary Key" and "to be trivial key" that are in the chaotic sequences that is caused by Logistic map, thus presents a image chaotic encryption algorithm that is based on hybrid chaotic sequence. Firstly, the algorithm generate hybrid chaotic sequence through the key; then through generates the corresponding offset matrix and permutation matrix the discrete mapping; finally, do the implementation of wavelet transform to the image, do the digital image scrambling encryption in the transform domain. In order to measure the degree of scrambling, we propose a "scrambling degree" concept. Experiments confirmed that the encryption algorithm has good scrambling in nature, and achieved good encryption effect. It confirmed the degree of scrambling encryption can effectively reflect the effect of scrambling encryption of the algorithm.

KEYWORDS

Chaotic sequence; Images; Scrambling.

INTRODUCTION

Currently, the international Internet technology worldwide has rapidly developed around the world. Many of the activities of people are linked through a variety of information systems. With the computer networks, people can easily perform various multimedia information exchanges. Digital image is a kind of media that can be adapt to the development needs of computer network, and contains a wealth of information. However, transmitting data files or images through the network, makes malicious individuals or groups transmit and copy the copyrighted content without obtaining the owner's permission. So encrypting the digital image has become an important research direction. Although traditional cryptography encryption algorithm has a strong security, the result of encrypting image is not necessarily the best. Digital image scrambling is to transform a digital image, to make it unrecognizable and become another chaos images without obvious meaning. If the operator knows the algorithms he can reconstruct the original image from the chaos image by using the certain algorithms. Theory encrypts the image data stream through using the chaotic signal, and it has the advantage like high security, encryption speed, large key space, and good scrambling effect. The scrambling process of digital image is essentially a process of coding and decoding of a class of image. When the third capture confusing image, since the parameters of scrambling algorithm are confidential, even in the case that the algorithm is known it is also difficult to decipher. The image scrambling requires that the image has a lower intelligibility after scrambling; the scrambling image should have a certain degree of security after scrambling, and can withstand a certain degree of attack. Digital image scrambling cannot change the resolution of images, the images that remove the scrambling have undifferentiated or little difference with original image, and can be able to accurately express the content or meaning of the original image. Compared with traditional cryptography, digital image has a large amount of data, thus it has a lot of clear space, and also has a great ciphertext space, the most important is the autocorrelation of the digital image visually manifested direction of perpendicular and direction of various tilt angles, it is difficult for such one-dimensional signal sequence in this paper to talk autocorrelation, Therefore, when considering the scrambling algorithm we should fully consider the impact of algorithm on the image autocorrelation, the worse the autocorrelation the better the scrambling, the poorer the intelligibility of the image after scrambling. Therefore, the conventional cryptography encryption algorithm has a strong security, but the effect of encrypting image is not necessarily the best.

THEORY OF DIGITAL IMAGE ENCRYPTION

Digital image scrambling technology extended from a one-dimensional single-table password, applied to the two-dimensional image plane, even the three-dimensional image color space, disrupted the component of the image, damaged autocorrelation of the image, even if the computer uses the "exhaustive" to calculate various combinations, and also consumes a lot of time, to a certain extent, the digital image scrambling technology protects the image information. Commonly used digital image scrambling methods are mainly based on a number of ways that transform from Arnold; and use the pixels on the image to do the Hilbert curve methods that can traverse change the sorting scrambling; and methods that use other mathematical knowledge and peculiar phenomenon to do the digital image scrambling and methods that are based on chaotic sequence scrambling. These methods have advantages and disadvantages on security scrambling and effect of removing scrambling.

The image can be viewed as a binary function F (x, y), (x, y) $\in$ Ron a plane region R, in general, the region R is a matrix form, to any point (x, y) on the R, F (x, y) represents the image information (such as the gray value, RGB component values, etc.), it shows that the binary function of the image has its particularity. After the image is digitized Z = F (x, y) is corresponding to a matrix, the rows and columns where the elements of the matrix are in, are the coordinates of all pixel of the image displayed on the computer screen, values of the element are the pixel gray (typically 256 levels, an integer from 0 to 255), the color image can be taken into the mixing matrix, the gray level of each pixel has relationship with the red, green, blue, the color images can be represented as three matrices, and also can be

represented as a three-dimensional vector matrix, digital image scrambling transformation can happen in the position space, color space, and on the frequency space, however, in order to restore the original image, we must ensure that the original image and the converted image are maintained between the correspondence.

IMAGE ENCRYPTION ALGORITHM BASED ON MIXED CHAOTIC SEQUENCES

Algorithm design

With the improvement of emphasis on the multimedia information security, the development of image encryption technology in China is imminent. For multimedia information, especially picture and audio information, see the traditional password encryption as a normal data traffic and encrypt it, without considering the characteristics of multimedia data, it will have some limitations. Image scrambling encryption methods, such as the classic Arnold transform, Hilbert curve transformation, E curve transformation, geometric transformations, and Knight Parade scrambling transformation, etc., effect of each methods are not the same after image scrambling, but they all have a certain certainty, while during the scrambling process what are changed are only the position of the pixel, the size can not be changed, so the image scrambling still have a certain regularity. Literature[1] proposed encryption algorithm based on chaotic sequence, it do not only change the position of pixel and also change its size. The algorithm belongs to the spatial domain algorithms. The achievement of ordering encryption algorithm in the spatial domain is simple, the calculation of the ordering encryption algorithm is less. However, the local random scrambling effect of spatial domain is not very good. The algorithm proposed in literature[2] is DCT domain algorithms. The advantage of frequency domain algorithm is, the changes of each point in the frequency domain have some impact on the entire data set. Relative to the spatial domain algorithm, frequency domain encryption algorithm has more efficiency. In this paper, we propose the wavelet image scrambling encryption algorithm that are based on hybrid chaotic sequence.

(a) Chaotic system

Chaos is a process during which deterministic and liking a random appear in nonlinear dynamical systems, this process is neither cycle nor convergence, and has extremely sensitive dependence on the initial values.

A one-dimensional discrete-time nonlinear dynamical system is defined as follows:

$$x_{k+1} = \tau(x_k) \quad \textbf{(1)}$$

In the formular, $x_k \in V, k = 0,1,2,3,\cdots,$ we call them state; And $\tau : V \to V$ is a mapping, the current state x_k is mapped to the next state x_{k+1}. If we start from the initial x_0, repeated the application of τ, we can get a sequence of $\{x_k, k = 0,1,2,3,\cdots\}$. This sequence is called a trajectory of the discrete-time dynamical systems. A class of very simple dynamical systems but has been extensively studied is the Logistic mapping, which is defined as follows:

$$x_{k+1} = \mu x_k (1 - x_k) \quad \textbf{(2)}$$

Wherein, $0 < \mu \le 4$ is called the branch parameter, $x_k \in (0,1)$ and it is defined as above. The research of Chaotic dynamical systems pointed out that, when $3.5699456\cdots \le \mu \le 4$, logistic mapping work in the chaotic state. That is to say, the sequence $\{x_k, k = 0,1,2,3,\cdots\}$ generated by the Logistic mapping from the initial condition x_0 is non-periodic, not converge, and is very sensitive to the initial value.

Without the lost of generality, for simplicity, we mainly consider the case when $\mu = 4$, namely:

$$x_{k+1} = 4x_k(1-x_k) \quad \textbf{(3)}$$

The inputs and outputs of Logistic mapping are located in (0,1), you can use the probabilistic method to quantitatively analyze the features of the sequence, Schuster H.G proved that the probability distribution density function $\rho(x)$ of chaotic sequence $\{x_k, k = 0,1,2,3,\cdots\}$ that generated from the formula (3), and the function is shown as the following formula:

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{x(1-x)}} & 0 < x < 1 \\ 0 & x \le 0; x \ge 1 \end{cases} \quad \textbf{(4)}$$

What can be seen from Equation (4) is, chaotic sequence generated from Logistic mapping is ergodic, and it also has the cross-correlation function between autocorrelation function and zero, so it can be used as a good generator of image scrambling sequence.

In literature[3,4], and[5], etc. we all use Logistic mapping in formular (3) to generate chaotic sequence, and use it for encryption scrambling. When the initial value is $x_0 = 0.75$, the chaotic sequence generated from formular (3) is $\{x_k = 0.75, k = 0,1,2,3,\cdots\}$; When the initial value is $x_0 = 0.25$, the chaotic sequence generated from formular (3) is $\{x_0 = 0.25, x_k = 0.75, k = 1,2,3,\cdots\}$.

Obviously the sequence in both cases are not available for scrambling. We called these two cases ordinary keys and extraordinary keys.

(A) Ordinary keys

Mark

$$f(x) = \mu x(1-x)$$

Logistic mapping

$$x_{n+1} = f(x_n), \quad (n = 0,1,2,\cdots). \quad \textbf{(5)}$$

If there is a point $x_0 \in (0,1)$ and it can make $x_n = x_0 (n = 1,2,\cdots)$, This key is called an ordinary key that cycle is 1. Similarly, for some positive integer k, it can make $x_k = x_0$, so we can get that $x_{n+k} = x_n (n = 0,1,2,\cdots)$, This key is called an ordinary key that cycle is k, Obviously, when x_0 is equal to ordinary keys that the cycle is k, Logistic mapping in the formular (5) take only has k number of value. $x_0, x_1, \cdots, x_{k-1}$,

It does not generate chaotic sequence.

(B) Extraordinary keys

Suppose $x^{<k>}$ is ordinary key that the cycle is k, that it can get that:

$$x^{<k>} = f^{om}(x)$$

x is extraordinary key that the cycle is k, this extraordinary key that the cycle is k is existing. Solving the ordinary key is solving the following equation

$$x^{<k>} = \mu x(1-x) = \mu x - \mu x^2$$

When $\mu^2 - 4\mu x^{<k>} \ge 0$, There exists real solutions in the above equation. If is an ordinary key that the cycle is 1. After solving we can get that $1 - x^{<1>}$ is an ordinary key that the cycle is 1.

(C) Existence of ordinary key and the extraordinary key

Ordinary key that the cycle is 1 will meet the equation

$$x = \mu x(1-x)$$

After solving we can get that

$$x = 1 - \frac{1}{\mu} \tag{6}$$

Ordinary key that the cycle is 2 will meet the equation

$$x = \mu(\mu x(1-x))(1-\mu x(1-x)).$$

After x was eliminated, a cubic equation we can get that

$$1 = \mu(\mu(1-x))(1-\mu x(1-x)).$$

That is

$$x^3 - 2x^2 + (1+\frac{1}{\mu})x + (\frac{1}{\mu^3} - \frac{1}{\mu}) = 0. \tag{7}$$

Because ordinary key that the cycle is 1 is ordinary key that the cycle is 2, So (6) will be the roots for the cubic equation (7), use the division to solve it, we can get that

$$x^2 - (1+\frac{1}{\mu})x + (\frac{1}{\mu} + \frac{1}{\mu^2}) = 0.$$

$$\Delta = (1+\frac{1}{\mu})^2 - 4(\frac{1}{\mu} + \frac{1}{\mu^2}) = \frac{(\mu-3)(\mu+1)}{\mu^2}$$

So when $3 < \mu \le 4$, equation (7) has two roots. That is there are two ordinary keys that the cycle is 1.

$$x_{1,2} = \frac{(1+\frac{1}{\mu}) \pm \sqrt{\Delta}}{2}$$

When $\mu = 4$,

$$x_{1,2} = \frac{5 \pm \sqrt{5}}{8}.$$

Use MATLAB to solve the ordinary key that the cycle is 3, we can get that when $3.8284271\cdots < \mu \le 4$, there exists ordinary keys $\delta_i^{<3>} \in (0,1), (i = 0,1,\cdots,7)$ that the cycle is 3, and also there exists extraordinary keys $\delta_i^{'<3>} \in (0,1), (i = 0,1,\cdots,7)$ that the cycle is 3.

Lee - York Theorem: if there is $3-$ periodic point of continuous mapping f in interval I, then for any positive integers n, f has n- periodic points.

So when $3.8284271\cdots < \mu \le 4$, there must exist the ordinary key $x^{<k>}$ that the cycle is k, and the extraordinary key $x^{'<k>}$ that the cycle is k. And when $k \to \infty$, there exists countable ordinary keys $x^{<k>}$ and

extraordinary keys $x'^{<k>}$ in (0,1). These points are "sparse" relative to the entire (0,1) interval, but they are not negligible for scrambling encryption algorithm. Suppose that $\{x_k, k = 0,1,2,3,\cdots\}$ is chaotic sequence that generated by the Logistic mapping, when x_k is equal to the ordinary key $x^{<l>}$ that the cycle is l or is equal to the extraordinary key $x'^{<l>}$ that the cycle is l, so the sequence after x_k necessarily hasve cyclical, and the cycle is l. This is not consistent with our requirements for chaotic scrambling encryption algorithm, for example, from the formula (6) we can know that, when $x = 1 - \frac{1}{\mu}$, the sequences generated from Logistic map is $\{x_k = 1 - \frac{1}{\mu}, k = 0,1,2,3,\cdots\}$, Such sequences cannot reach the scrambling effect.

(b) Wavelet transform processing of the image

Since the late 1980s Wavelet analysis theory has become internationally very active area of research, it has been widely used in image processing, oil exploration, data compression, CT imaging, fractal geometry, and many other fields.

(A) Definition of wavelet transform

Definition: Suppose $\psi \in L^2 \cap L^1$, and $\hat{\psi}(0) = 0$, if it satisfies the allowing conditions:

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

We call ϕ allowing wavelet or basic wavelet.

Expanding and translating the function as the following methods will generate the function $\psi_{u,s}$

$$\psi_{u,s}(t) = \frac{1}{\sqrt{s}} \psi(\frac{t-u}{s})$$

It is called continuous wavelet function. In the formulas s is the scaling function, u is the translation parameters. The wavelet transform of function $f(t) \in L^2(R)$ is defined as:

$$Wf(u,s) = \int_{-\infty}^{+\infty} f(t) \frac{1}{\sqrt{s}} \psi^*(\frac{t-u}{s}) dt$$

Wavelet transform can be written as the form of the convolution:

$$Wf(u,s) = f * \overline{\psi_s}(u),$$

In the formular,

$$\overline{\psi_s}(t) = \frac{1}{\sqrt{s}} \psi^*(\frac{-t}{s})$$

Thus, the wavelet transform can be regarded as the filter that is a band-pass filter which the impulse response is $\overline{\psi_s}(t)$ to f (x). Since the introduction of wavelet scale parameter s, so that resolution varies with s in the time domain and frequency domain. Thus, the most prominent advantage of wavelet transform is the ability to well carve mutation signal.

(B) Mallat algorithm

Inspired by Burt and Abelson's tower algorithm of image decomposition and reconstruction, based on the framework of multi-scale analysis, Mallet proposed a pyramid decomposition algorithm, called the Mallet algorithm, which plays an important role in wavelet analysis.

Suppose Vj is the given multi-scale analysis, ϕ and ϕ are the corresponding scaling function and wavelet function, for a given discrete signal {Sk, k ∈ Z} ∈ V0 (here the corresponding resolution is j = 0), the expansion translation system of V0 space is { ϕ j, k, k ∈ Z}, we can construct a function f (u) ∈ V0 inV0 space,

$$f(u) = \sum_{k \in Z} S_k^0 \varphi_{0,k}(u)$$

Since V0 = V1 ⊕ W1, so that f (u) can be decomposed as follows:

$$f(u) = \sum_{k \in Z} S_k^1 \varphi_{1,k}(u) + \sum_{k \in Z} d_k^1 \psi_{1,k}(u)$$

In the formular the first part is the projection that f (u) on V1, the second part is the projection that f (u) on W1. Since V1 = V2 ⊕ W2, in the formula the first portion may be further decomposed, respectively projected onto the space V2 and W2,

Solve the formular like this way, we can get pyramid decomposition of the signal. The decomposition recursive formula is:

$$S_k^{j+1} = \sum_{n \in Z} h_{n-2k} S_n^j$$

$$d_k^{j+1} = \sum_{n \in Z} g_{n-2k} S_n^j$$

We referred S_k^{j+1} as the discrete approximation of f (u) with 2j resolution, that calls low-frequency components; referred d_k^{j+1} as the discrete detail of f (u) with 2j resolution, that calls high-frequency components.

$$f(u) = \sum_{k \in Z} S_k^1 \varphi_{1,k}(u) + \sum_{k \in Z} d_k^1 \psi_{1,k}(u)$$

The first term in the formula can be understood as the ingredients of function f (u) in the frequency of not more than j ; the second term in the formula can be understood as the ingredients of function f (u) in the frequency between j to j+1. Thus, according to the above pyramid decomposition algorithm function f (u) can be decomposed into components of different frequency channels.
Synthesis is the reverse process, the synthetic formula is:

$$S_k^{j-1} = \sum_{n \in Z} h_{k-2n} S_n^j + \sum_{n \in Z} g_{k-2n} d_n^j$$

This pyramid decomposition algorithm is also suitable for two-dimensional case.

(C) Applications of wavelet transform in image processing

(1) Image decomposition

For a finite set of orthogonal wavelet, the function ϕ (x) satisfies two-scale difference equation that is limited form.

$$\varphi(x) = \sqrt{2} \sum_{k=0}^{N-1} h_k \varphi(2x - k)$$

$$g_k = (-1)^{k-1} h_{2N-k-1} \qquad k = 0,1,2,\cdots 2N-1$$

The decomposition and synthesis formular of discrete signal are limited transformation formula. Take N = 3 or N = 5 we can get the corresponding recursive formula and synthetic formulas of limited form. The selected size of N has relationship with the smoothness of wavelet function, the size of N is small, the smoothness of wavelet function is poor, but the operation is small; the size of N is large, the smoothness of wavelet function is good, but the operation is large. Experiments show choose N = 3 or N = 5 has almost no difference in image recovery quality, so we choose N = 3 that can meet the requirements.

The coefficient image obtained after decomposition, the total amount of data is equal to the amount of data of the original image, the data of coefficient image of each level reflects the frequency components of the image in different frequency bands, with certain characteristics. Since the original image of each color has 5 bits, a total of 32 gray levels, if the gray level changes, although it increases 1 or decreases 1, it is sensitive to visual, The coefficient values after the decomposition and the pixel values of the low frequency image are real numbers, which will cause the quantization error. Therefore, in order to ensure the quality of the decoded image, we must consider as possible to reduce quantization errors.

(2) Denoising treatment

Denoising treatment is more important work in image processing. For example several small pieces of an image are stained by noise points, if directly remove the dust, it will leave traces. Using wavelet transfo the characteristics of the signal itself from these different levels of wavelet components, and then to extract the edge points.

Wavelet analysis is constantly evolving in theory, see from the theory of wavelet analysis, application of wavelet packet has its obvious advantages, It can complete more finer image orthogonal decomposition, that is: based on the tower decomposition, and then decompose the coefficients image that got the high frequency, Makes the band of the high frequency system image after the final decomposition can be put into more sophisticated way. Then do the optimal combination of the resultant series of coefficient images, This allows the high frequency coefficients image that the band is more finer divided to take corresponding measures, Such as process the high frequency coefficients image which the human eye is not sensitive to, or simply remove certain components of frequency coefficients, it is conducive to the application in image processing.

In summary, the wavelet transform is the time - frequency representation of the image. Compared with the conventional DCT transform, the time frequency of DCT is irrelevant, WT spatial resolution increases with frequency, and it has better adaptability for the edge that dramatic changes; On the other hand, a normal image are energy concentrated in low frequencies, in WT the rate of change of the frequency is inversely proportional to the frequency, allow to decompose low-frequency into the finer subband.

Every time image is decomposed into four sub-graphs by wavelet transform, of which corresponds to a smoothed version, and the other three corresponds to details versions (shown in Figure 1).

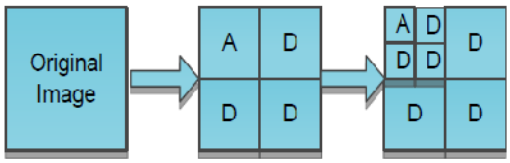


Figure 1: Diagram of wavelet decomposition (A is smooth part of original image, D is details part of original image)

Known from the above picture, the image data is changed to the frequency domain by the wavelet transform, and is decomposed into a smoothed version and details version. If implemented image scrambling algorithm in a smoothed version A of wavelet domain, the changes of each point have

some impact on the entire data set, and it can achieve good scrambling effect; And the required length of the chaotic sequence can be multiply reduced, the speed of the algorithm is greatly improved.

Image scrambling algorithm that based on mixed chaotic sequence

Because there are ordinary keys and extraordinary keys in the Logistic mapping, we propose a image encryption algorithm that based on mixed chaotic sequence, it can avoid generating ordinary keys and extraordinary keys.

(a) Algorithm principle

Order Chebyshev mappings are defined as follows:

$$\tau(x_{k+1}) = \cos(n(\cos^{-1} x_k) \quad \textbf{(8)}$$

In the formular, the defined range is $(-1,1)$, in this article we make the defined range $(0,1)$.

In algorithm that proposed in this paper, first use the Logistic mapping (3) and Chebyshev mapping (8) to alternately generate mixed chaotic sequence, then use mixed chaotic sequence to produce the corresponding permutation matrix and offset matrix. For any image I, suppose the size of I is $n = M \times N$, do the operation in the wavelet domain:

1. do the WT transform to the image, $I_W = WT(I)$, suppose the image of smoothed version in it is I_{WA}

2. use offset matrix to transform the coefficient values in I_{WA}, we can get I_{WAF}

3. use the permutation matrix to do arranged transformation to I_{WAF}, we can get I_{WAFT}

4. Do the inverse wavelet transform to I_{WAFT}, $I_E = WT^{-1}(I_{WAFT})$, and then complete the image encryption.

(b) Algorithm design

(A) Generation of permutation matrix and scrambling operation

For a two-dimensional image $I_{M\times N}$ (for the sake of discussion we assume that $\frac{M\times N}{4}$ is an integer), use Logistic mapping and Chebyshev mapping to generate real numbers mixed chaotic sequence $\{x_k, k = 0,1,2,3,\cdots\}$. Sequence x_k multiplies $\frac{M\times N}{4}$ and rounded up, got a integer mixed chaotic sequence $\{y_k \in [1, \frac{M\times N}{4}], k = 0,1,2,3,\cdots\}$. Orderly put the element values of sequence y_k into the empty matrix $P_{\frac{M\times N}{4}}$, ensure any element $P_{ij} \in [1,2,\cdots,\frac{M\times N}{4}]$, if $P_{ij} = P_{kl}$, If and only if $i = k, j = l$. Because the generated mixed chaotic sequence has ergodic property in the interval (0,1), $P_{\frac{M\times N}{4}}$ must be filled, matrix $P_{\frac{M\times N}{4}}$ is the permutation matrix after being filled. Permutation matrix $P_{\frac{M\times N}{4}}$ equally owns chaotic characteristics.

(B) the generation of the offset matrix

Use the permutation matrix $P_{\frac{M\times N}{4}}$ that has been generated, to Divide a pre-set threshold value, we can generate the offset matrix $R_{\frac{M\times N}{4}}$. Use the values in the offset matrix to change the wavelet coefficients in smoothed version, similarly offset matrix $R_{\frac{M\times N}{4}}$ also has chaotic characteristics.

(C) the achievement of encryption algorithm

Step 1. Input parameters

* Original image file name InImage;

*The resulting image file name OutImage ;

* keys x_0 。

Step 2. (one) From the key x_0, generate real value mixed chaotic sequence x_k and integer mixed chaotic sequence $y_k, k = 0,1,2,\cdots$;

(two) generate the offset matrix $P_{\frac{M\times N}{4}}$ and permutation matrix $R_{\frac{M\times N}{4}}$;

(three) do the wavelet transform to the image $I_{M\times N}$, suppose that in the process the smoothed version of the image is set as I_{WA}

(four) use $R_{\frac{M\times N}{4}}$ to change the wavelet coefficient values in I_{WA}, and then use $P_{\frac{M\times N}{4}}$ to do scrambling operation to I_{WA}

Step 3. do the inverse wavelet transform to the image data that the scrambling operation has been completed, then output the resulting image.

(D) The achievement of the decryption algorithm

The user must enter the correct key, make the encryption algorithm reverse operation, then we can get decrypted images.

RESULTS AND ANALYSIS

We use Daubechies wavelet transform to achieve the algorithm in this article. Figure 2 is the encrypt results of the algorithm to the Lena image.

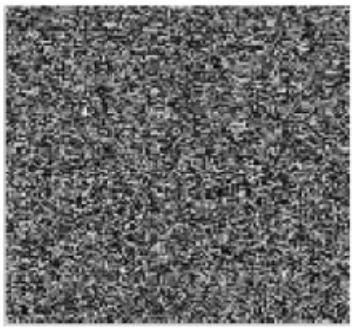
Experimental results show that, when $\mu = 4$, set the ordinary key x_0=0.75 that the circle is 1 and the extraordinary key x_0=0.25 that the circle is 1 in the Logistic mapping as the initial value, the algorithm is able to produce chaotic sequence that can meet the requirements, it is a result that single using Logistic mapping cannot produce. Meanwhile, use this mixed chaotic sequence to do scrambling encryption, but also increase the difficulty of image decryption attacks.

This algorithm change part of (low frequency) values of wavelet coefficients in the wavelet domain, change the quality of original image. Scrambling encryption algorithm for the general spatial domain changes the position of pixel, and does not change its value, therefore, the encrypted image and the original image has the same histogram. And in the algorithm, the position and values of the pixel have been changed, thereby it improved the quality of the encryption. This can be seen from the change of histogram of the images that are before encryption as Figure 3 (a) and after encryption as Figure 3 (b). Figure 2 (c) is the encrypted image that the key is x_0= 0.7, Figure 2 (d) is the image that uses the correct key to decrypt. Figure 2 (e) is the image that is decrypted with the wrong key, We can see that, as the chaotic sequence is very sensitive to the initial value, even small changes in key value will get a completely different results of decryption, so there offers a large number of room keys for us to choose, greatly improve the security of encryption.

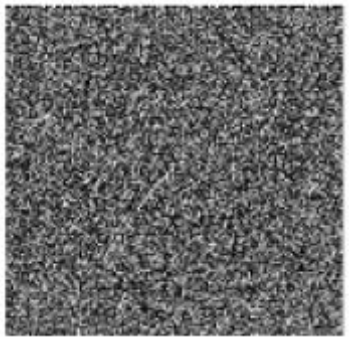
(a) Original image

(b) Wavelet decomposition

(c) Encrypt images

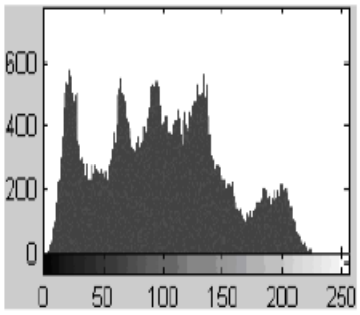


(d) Correct decrypted

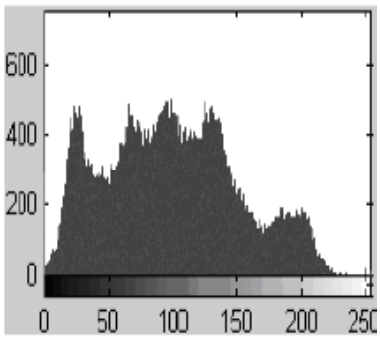


(e) Error decrypted image

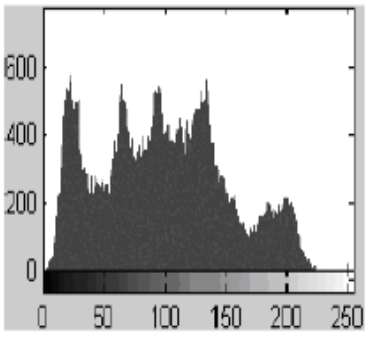
Figure 2: Results of image encryption and decryption



(a) Histogram of original image



(b) Histogram of encrypt image



(c) Histogram of decrypted image

Figure 3: Histogram of the image

CONCLUSIONS

In order to study digital image scrambling, this paper discusses the chaotic sequence images study that is based on the Logistic mapping. Propose a images encryption algorithm that are based on chaotic sequence, improved the performance of digital image scrambling encryption. Chosen the wavelet transform as the time-frequency conversion tool, full use of the images characteristics that the images are wavelet decomposed, choose to do scrambling encryption for images in smoothed version after the images are decomposed. Because changes of each point in the frequency domain will have some impact on the entire data set, so the algorithm can achieve good scrambling encryption effect. Experimental results show that, even small changes in key value will get completely different results of decryption, so there offers a large number of room keys for us to choose, greatly improve the security of encryption.

CONFLICT OF INTERESTS

The authors declare that there is no conflict of interests regarding the publication of this article.

REFERENCES

[1] Ding Wei, Dong Xu; Digital image transformation and information hiding and camouflage techniques [J], Journal of Computers, **21(9)**, 838-843 **(2012)**.

[2] Dong Xu, Zou Jiancheng, Han Xiao Yu; A new class of scrambling transformation and its application in image information hiding, Science in China (E Series), **30(5)**, 440-447 **(2012)**.

[3] Ding Wei, Yan Wei Qi, Qi Dongxu; Based on Scrambling and the integration of digital image hiding technology and its applications, Chinese Journal of Image and Graphics, **5(8)**, 644-649 **(2012)**.

[4] Ding Wei, Yan Wei Qi, Qi Dongxu; Based on Arnold transform digital image scrambling technology, Computer Aided Design and Computer Graphics, **13(4)**, 338-341 **(2012)**.

[5] Sen, Cao Xiu; Affine transform digital image scrambling technology, Computer Engineering and Applications, **10**, 74-76 **(2012)**.

[6] J.C.Yen, J.L.Guo; A New Chaostic Mirror-Like Image Encryption Algorithm and Its VLSI Architecture[J], Pattern Recognition and Image Analysis, **10(2)**, 236-247 **(2000)**.

[7] M.R.Speigel; Theory and problems of complex variables, New York: McFraw-Hill, 35-36 **(1972)**.

[8] Conrad Bessant; Computers and Chaos, SIGMA PRESS **(1992)**.

[9] Clifford A.Pickover; Computers, Pattern, Chaos and Beauty, ST. Martin's Press, New York **(1990)**.

[10] B.L.Hao; Elementary symbolic dynamics and chaos in dissipative systems[M], Singapore: World Scientific Publishing Co Ltd **(1989)**.

[11] H.Sakai, H.Tokumaru; Auto correlation of a certain chaos[J], IEEE Trans ASSP, **289(5)**, 588-590 **(1980)**.

[12] S.Boccaletti, C.Grebogi, Y.C.Lai et al.; The control of chaos: theory and applications [J], Physics report, **329**, 103-197 **(2000)**.

[13] Josef Scharinger; Fast encryption of image data using chaotic Kolmogorov flows, In: Proceedings of the International Society for Optical Engineering, San Jose, California, **3022**, 278-289 **(1997)**.

[14] P.Collet, J.P.Eckmann; Iterated maps on the interval as dynamical system [M], Boston: Birkhauser **(1980)**.

[15] Yen Juicheng, Guo Jiunin; A new chaotic key-based design for image encryption and decryption [Z], ISCAS 2000 IEEE-International Symposium on Circuits and Systems, Geneva, Switzerland **(2000)**.

[16] **(a)** S.Mallat; A theory for multi-resolution signal decomposition: the wavelet representation [J], IEEE Trans. On Pattern Analysis and Machine Intelligence, **11**, 674-693 **(1989)**; **(b)** J.Scharinger; Fast encryption of image datas using chaotic Kolmogorov flows [A], Proceedingd of the International Society for Optical Engineering [C], San Jose, California, **3022**, 278-289 **(1997)**.

[17] P.P.Dang, P.M.Chan; Image encryption for secure internet multimedia applications, IEEE Transactions on Consummer Electronics, **46(3)**, 395-403 **(2000)**.