An Image Scrambling Encryption Algorithm

Ruwang Cai^{1, a} and Bin Wang^{1, b *}

¹Hainan University, Danzhou, Hainan, 570228, China

^a78387729@qq.com, ^b770147433@qq.com

Keywords: Logistic; Divisibility; XOR; Chaos scrambling

Abstract. This paper presents an algorithm that changes the pixel position and the size of pixel values of digital images on the basis of Logistic system, using simple divisibility and XOR operation. The algorithm successfully encrypts the image. Experiments show that the algorithm is simple, crack the secret key space is large, very high security, and can resist a variety of attacks, with excellent practicality.

Introduction

With the development of the network, digital images have become an important medium for people to communicate daily [1]. The security of the image has also become a hotspot in many research scholars. Image scrambling is an important means of encrypting images. The current scrambling algorithm mainly achieves the purpose of encryption by changing the position of the image pixel or changing the size of the image pixel value. Such as Arnold transform, magic square transformation, etc., but these algorithms are only a single image pixel position or pixel values scrambled. And some algorithms exist cyclical, easy to be cracked [2].

Due to the sensitivity of the initial value, the sequence generated is no law, the chaotic system has become the new favorite of scrambling. The use of chaotic system scrambling, you can improve the security of the system to ensure the safety of the image. On the basis of the above, this paper proposes a new algorithm to change the pixel position of image pixels and change the pixel value by using a chaotic sequence pair generated by two coupled chaotic maps. It is proved that the algorithm is simple and easy, and the encryption effect is good, and it can resist a variety of attacks, and the image recovery effect is excellent [3].

Generation of Logistic Chaotic Sequences

Logistic Chaotic Mapping. Chaos refers to seemingly random irregularities that occur in deterministic systems. A chaotic system behavior is uncertain, non-repeatable and unpredictable. Chaos is an inherent characteristic of nonlinear dynamical systems. Its simple structure, sensitive to the initial value and white noise characteristics can improve the security of the encryption system to improve the difficulty of cracking. Chaotic systems play an excellent role in encryption.

Logistic mapping was first proposed by the 1976 mathematical ecologist R. May in the UK's Nature magazine, which originated from the population model. The Logistic map definition sequence is:

$$x_{k+1} = ux_k(1 - x_k) \quad (1)$$

Where u is the branch parameter. When u is in the interval $(3.5699456, 4)$, the sequence it generates is very complicated and there is no rule to follow. At this time, the Logistic system is chaotic and the chaotic sequence is generated. When u is not in this interval, the value will last Approaching a fixed data [4].

Coupled Chaotic Sequences. In order to improve the anti - decipherability of the random sequence and increase the secret key space, two random logistic maps are combined to control the security and randomness of the sequence by interleaving the branching parameters of the other. The coupled chaotic maps are as follows:

$$\begin{cases} x_{k+1} = u_x x_k(1 - x_k) \\ y_{k+1} = u_y y_k(1 - y_k) \end{cases} \quad (2)$$

In order to let the two sequences interfere with each other, according to the literature [3], we define the branch parameters as follows:

$$u_x = \begin{cases} 3.9 & 0 < y_j \leq 0.5 \\ 3.9888 & 0.5 < y_j \end{cases} \quad (3)$$

$$u_y = \begin{cases} 3.9444 & 0 < x_i \leq 0.5 \\ 4.0 & 0.5 < x_i \end{cases} \quad (4)$$

Image Gray Value and '4' Relationship

Grayscale images have a total of 256 gray levels, from 0-255 different represent a different series. When the value of 0-255 on the 4 to be divisible, the business range between 0-63, while the remainder between 0-3. Calculate the maximum value of its quotient multiplied by 4 plus the maximum of the remainder, and its equal to 255 just falls within the gray scale range [5].

In addition, through the ergodic calculation we can find 0-63 between the value of different or 0-63 any value, the results still fall between 0-63. This gives us a very convenient and simple way to change the image gray value.

Image Scrambling Encryption Algorithm

Step 1: Select a digital image to be encrypted matrix I , for each pixel value to do divisible 4 and 4 to take the other operations, the specific calculation is as follows:

$$\text{divi}(i, j) = \text{fix}\left(\frac{I(i, j)}{4}\right) \quad (5)$$

$$\text{residue}(i, j) = \text{mod}(I(i, j), 4) \quad (6)$$

Step 2: Take the initial value as the initial value of the random sequence, using the formula (2) to iterate, thus generating chaotic sequences $x_1, x_2 \dots x_m$ and sequences $y_1, y_2 \dots y_n$. The chaotic sequence is sorted from small to large way to get a new sequence, and save the new array of elements in the original array of the location, get arrX sequence and arrY sequence [6].

Step 3: Use the permutation sequence of the generated double-coupled chaotic sequences to rearrange the resulting matrix of the shuffled 4 of the stored image, each of (i, j) which can correspond to (x_i, y_j) , and (x_i, y_j) can correspond to that, that is, the replacement can be used to complete the storage Divide 4 results to complete the matrix scrambling [7].

Step 4: Take the initial value, use the formula (1) to generate a one-dimensional logistic sequence $z_1, z_2, z_3 \dots z_m$ of length m , in the sequence from small to large order to get a new sequence, save the new array of elements in the original array of the location, ArrZ, and will arrZ the number of 64 to take over, let his range in the interval [0,63] to update the arrZ specific operation as follows:

$$\text{arrZ}(1, j) = \text{mod}(\text{arrZ}(1, j), 64) \quad (7)$$

Step 5: will be different from the XOR, XOR result multiplied by 4, plus, get the final scrambling matrix, the specific operation is as follows:

$$\text{Result}(I, j) = (\text{divi}(I, j) \oplus \text{arrZ}(1, j)) * 4 + \text{residue}(i, j) \quad (8)$$

In the process of image encryption, we introduce four secret keys, the secret search space is large, and each key change will have a great impact on the image, thus ensuring the security of the algorithm.

Image Scrambling Algorithm

The decryption algorithm is just the opposite of the encryption algorithm. First, the corresponding Logistic sequences are calculated, and the sequences are sorted by small to large sequences, and their corresponding position sequences are obtained. And the number of sequences is done by taking the remainder of 64. Then the ciphertext digital matrix H to 4 to take the operation, to obtain the corresponding remainder matrix. The ciphertext matrix minus the remainder matrix, and then

divisible 4, the divisors of the same or on the arrangement of arrZ' , the specific formula is as follows:

$$\text{divi}'(i, j) = \text{fix}\left(\frac{H(i, j) - \text{residue}'(i, j)}{4}\right) \oplus \text{arrZ}''(1, j) \quad (9)$$

And then according to the calculation of the corresponding chaotic sequence, to get the corresponding sequence. Will be replaced with. Restore the original position, and finally multiplied by 4 plus the previously obtained the remainder to find the original image, the specific operation is as follows:

$$I(i, j) = \text{divi}'(i, j) * 4 + \text{residue}'(i, j) \quad (10)$$

Generate the I instantly scrambled before the original image. After comparison, after the chaos decrypted the image and the original encrypted image is not the slightest difference, the reduction effect is excellent [8].

Simulation Experiment and Result Analysis

Histogram Analysis. The grayscale histogram is a function of the gray level, which represents the number of pixels in a gray scale, and can visually embody the statistical properties of the image. Using the histogram, you can get a lot of image features [9].

In the simulation experiment, this paper uses Matlab R2016a on the liftingbody image to scrambling encryption, encryption before and after the histogram, such as Fig. 1 is the original image of the histogram, Fig. 2 is scrambled encrypted histogram.

Figure 1. Original histogram

Figure 2. Scratch image histogram

It can be seen that the encrypted histogram is more evenly distributed than the histogram before the encryption, successfully masking the pixel information of the original image, and the encryption effect is good, which can effectively resist the anti-plain attack and statistical analysis [10].

Secret Key Sensitivity Analysis. The liftingbody image is scrambled and encrypted as an initial key set. Its encryption effect as shown below, Fig. 3 for the original image, Fig. 4 for the scrambling image:

Figure 3. The original picture

Figure 4. Scratch the image

From the encrypted image, we almost do not see any information about the original image, we can see that the algorithm encryption effect is good. Now the initial secret key to do a small modification, and its decrypted images are as Fig. 5, Fig. 6 and Fig. 7.

Figure 5. X The initial value is modified after decrypting the image

Figure 6. Z The initialized decrypted image is modified

Figure 7. Z The array of branch parameters is modified after decrypting the image

From the above figure we can see that even if we use the secret key which is very different from the original secret key to decrypt the scrambled image, we can not decrypt the correct image or image contour. The image still has a good scrambling effect. Therefore, this method of ciphertext search space is great, can effectively resist a certain exhaustive attack [11].

Anti-noise Analysis. Image collection, processing, storage, transmission and a series of processes often introduce image noise, which has an indelible impact on the quality of the image. Therefore, the noise has a certain resistance is very important.

In the simulation experiment, we use different noise pollution after scrambling images, and observe the image effect after the restoration. As shown in the figure, Figure 8 uses the salt and pepper noise, Figure 9 is used Poisson noise. In the contaminated image after the decryption, the decrypted picture is as Fig. 8 and Fig. 9.

Figure 8. Scratch the image by the salt and pepper noise after the decrypted image

Figure 9. Scratch the image by Poisson noise after decrypting the image

As can be seen from the above figure, the image of the chaos after a different noise attack, the scrambling method can still be better to retain the basic contours of the image and information. It can be seen that the method is more resistant to attack. Can resist the general noise pollution, is a relatively good effect of the scrambling way.

6.4 Related calculation of scavenging evaluation index

The correlation coefficients of the two images are related to the statistics of the degree of image correlation, which is the statistical parameter which reflects whether the two pairs of images are closely related. The value is in the range [0,1], the closer the value is to 1, the closer the linearity of the image is, the closer the value is to 0, the less the linear correlation is

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (11)$$

According to the above formula, we calculate the correlation coefficient of the scrambling graph and the original graph, the correlation coefficient of the scrambling graph and the decrypted graph, the correlation coefficient of the decrypted graph and the original image. The calculated values are as Table 1.

Table 1 The correlation coefficient between images

	The original image	Encrypted image	Restore image
The original image		0.0048	1
Encrypted image	0.0048		0.0048
Restore image	1	0.0048	

It can be seen from the above chart that the correlation coefficient between the encrypted image and the original image is very small, and there is almost no linear correlation between the two, indicating that the correlation between the original image and the scrambled image is very weak, and the effect of the scrambling method is very good. In addition, the restored image and the original picture correlation is 1, indicating that the decrypted image and the original picture no difference.

Conclusion

In this paper, we propose a scrambling method based on 4-rounding and 4-ary operations. This method introduces a coupled chaotic sequence and a one-dimensional logistic sequence. The position of the pixel is changed by using the coupled sequence, and the pixel size The This algorithm introduces four secret keys, secret key search space, and secret key sensitivity is very high, easy to be cracked. In addition, the algorithm can still recover the image before the noise. Simulation results show that the algorithm is simple and easy to implement, and it can resist various kinds of pollution.

References

- [1] Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: Survey and analysis of current methods, *Signal Processing*. 90 (2010) 727-752.
- [2] N. Hamid, A. Yahya, R. B. Ahmad, O. M. Al-Qershi, Image steganography techniques, *International Journal of Computer Science and Security* 6 (2012) 168-187.
- [3] N. Provos.: Defending against statistical steganalysis. *Proc. unix Security Symposium*, 10 (2001) 323-336.
- [4] E. Dunk., R.S. Black, *The Elements of Image*, first ed., Macmillan, New York, 2013.
- [5] J. Y. Hsiao, K. F. Chan, J. Morris Chang.: Block-based reversible data embedding. *Signal Processing*, 89 (2009) 556-569.
- [6] Pareek N K, Patida V, Sud K K.: Image encryption using chaotic logistic map. *Image and Vision Computation* 24 (2006) 926-934.
- [7] Mathews R, Goel A, Saxena P.: Image encryption based on explosive inter-pixel displacement of the RGB attributes of a pixel. In: *Proceeding of the World Congress on Engineering and Computer Science*, 2011, London, pp. 19-21.
- [8] T. Frunk., S.D. Green, *Image Communication*, First ed., Springer, German, 2012.
- [9] Lee Y S, Lee Y J.: Performance Improvement of Power Analysis on AES with Encryption-Related Signals. In: *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, 2012, New York, pp. 1091-1094.
- [10] S. Li, C. Li, G. Chen, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, *Image Communication*. 23(2008)212-223.
- [11] Hong K, Jung K.: Partial Encryption of Digital Contents Using Face Detection Algorithm. In: *Berling: Springer-Verlag*, 2006, pp12-20.