2011 International Conference on Information Management and Engineering (ICIME 2011)
IPCSIT vol. 52 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V52.54

Image permutation scheme based on modified Logistic mapping

Cao Guang-hui[1,2] ,Hu Kai[2] and Ding Yi[2]

[1] Electronic & Information Engineering College, Liaoning university of Technology, Jinzhou, China

[2] School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing, China

Abstract— Chaotic systems are extremely sensitive to initial parameters and these systems can be very helpful in the field of image scrambling. However, ordinary chaotic sequence is not uniformly distributed. Transformation which can generate uniformly distributed random variable in the interval [0, 1] based on logistic at μ=4 was studied. Utilizing this generated uniform random variable, random permutation algorithm based on interchange position was obtained. Based on this permutation algorithm, image bit permutation algorithm was described. When applied to image, compared with Rand algorithm and Ye algorithm, the proposed image bit permutation method exhibits large key space, effective ability of dissipating high correlation among pixels and increasing the entropy value. Results showed that this proposed encryption scheme with firmly theoretical foundation can enhance image security significantly.

Keywords-image permutation; chaos sequence; random permutation; permutation strength

1. Introduction

With the increasing maturity of internet on the ground and the speeding up pace of constructing space network together with fast development of digital multimedia technique, transmitting images on the space and on the ground through open network channel utilizing wired and wireless media become an important part of people life and scientific research. High network and digitalization provide us with much convenience, and also bring us some new challenges. Such as how to let authorized people access the valid data, and keep out of unauthorized access, which become the new challenges that network security worker must face.

Conventional encryption approach dedicated to content data cipher. New method adapted to structure data such as image, video, audio with high correlation and huge redundancy must be looked for. Shannon pointed out that diffusion has the property that makes the statistical structure disappear and the redundancy in the statistics of the plaintext is dissipated in the statistics of the ciphertext [1]. Diffusion can be effectively accomplished by using permutation on data, which is a main way for diffusion and was widely used to encrypt data. In particular, bit permutation becomes a new hotspot since it has good scrambling and inherent cipher property. Key early papers of bit permutation have been seen in [2],[3],[4],[5]. The first two bit level permutations called Shi and Lee permutation, respectively, are in fact, permutation instructions developed to efficiently implement arbitrary n-bit permutation in any programmable processors [2],[3]. The third one, called hereafter Socek permutation, is used to implement bit image permutation, which is confined to 8 bits [4]. Important recent paper of implement bit image permutation was Ye algorithm [5]. The main idea was that using Logistic map generates a sequence of floating point number which were sorted to get the index order which then were used to permute every bit in every row. However, probability density function of Logistic and the sequences generated by this map were not uniform. There is no theoretical guarantee that random permutation derived from logistic sequence can satisfy cipher security requirements. Of course, there existed

E-mail address: caoguanghuineu@163.com

other papers that also didn't discuss weather random sequence generated by chaos obeys uniform distribution such as [6]. Some papers [4],[7],[8] pointed out this problem but solved it by indirect methods. Paper [8] made the 0, 1 random sequence approximate uniform by setting the threshold as 0.6 and the threshold depended on initial value and parameter of chaos. Paper [4] replaced Logistic map with the piecewise linear chaotic map.

This paper dedicated to directly solve the problem of Logistic sequence non-uniformity on the condition that probability density function has been known for Logistic map at μ=4 and proposed a scheme of position based random permutation based on this uniform sequence. Further more, image scrambling based on Logistic map uniform distribution was presented.

2. GENERATION OF POSITION BASED RANDOM PERMUTATION

The most common random permutation algorithm is based on sorting chaos sequence [5],[9]. The difficulty with this approach, however, is that sorting chaos sequence typically requires on the order of *n*log(*n*) comparisons. A new random permutation algorithm based on position interchange was proposed that can reduce comparison numbers.

Proposition 1: Suppose *U* is uniformly distributed over the interval (0, 1), then $X = Int(nU) + 1$ (1) will be equally likely to take on any of the values 1,2,…n.

Proof: *U* is uniformly distributed over the interval (0, 1),

and set $X = i,\ \text{if}\ ((i-1)/n) \le U < i/n \quad (i = 1,...,n)$

Since, for $0 < a < b < 1$, $p\{a \le U < b\} = b - a,$

we have that $p\{X = j\} = p\{j-1/n \le U < j/n\} = 1/n$.

Therefore, *X* will be equal to *j* if $j - 1 \le nU < j$; or , in other words, $X = Int(nU) + 1$ .So *X* is uniformly distributed over (1, *n*).

QED

2.1. Generation of uniform random variable

1) Uniform random variable generating by rand() function in matlab (rand random method)

The rand function in matlab generates arrays of random numbers whose elements are uniformly distributed in the interval (0,1). The initial key is the parameter *s* in rand('state', *s*) function. There are two problems utilizing this method.

1: Range of *s* is small. For matlab 6.x version, *s* can only take integer, even if *s* is assigned a decimal fraction, the random sequence induced by the decimal is the same as the sequence induced by rounding the decimal to the nearest integer. And when *s* is larger than 5,000,000,000, the random sequence is always starting from the number 0.6627. Key space is limited and algorithm based on rand can't stand savage attack.

2: According to document [10], rand() function in matlab has a strong nonrandom pattern, which is also a defect for secure problem.

Based on the above reasons, uniform distribution random algorithm based on chaos over the interval [0],[1] was studied.

2)Uniform random variable generating by chaos map (Logistic random method)

Chaotic dynamics started with the work of the French mathematician Poincare who studied the problem of orbits of three celestial bodies experiencing mutual gravitational attraction. It was Li and Yorke who first introduced formally the term chaos into mathematics in 1975 [11]. Meteorologist Lorenz discovered one of the first examples of deterministic chaos in dissipative system [12].

A simple but well known dynamics is Logistic map.

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

When 3.5699457< μ ≤ 4, the Logistic equation enters chaos state. For formula (2), we obtain the natural invariant density for the logistic map at $\mu = 4$ over the interval (0, 1) [13],

$$\rho(x) = \pi^{-1} / [x(1-x)]^{1/2} \tag{3}$$

From formula (3), one can see that the probability density function of Logistic is not uniform, which is not suited for generating random permutation. It is necessary to transform the original chaos sequence into uniformly distributed sequence.

a) Principle of constructing uniform distribution

Suppose that x and y are random variables whose probability density functions are $f(x)$ and $g(y)$ respectively, which are integrable over the interval (a, b) and (c, d), set:

$$\int_a^x f(t)dt = \int_c^y g(t)dt \tag{4}$$

Combing with the meaning of probability density function, formula (4) means that for any x over interval (a, b), there is a y over interval (c, d) corresponding with the given x that make $p(x)$ is equal to $p(y)$. This gave a mapping relationship $y=f(x)$ between x and y, in which domain is (a, b) and value is (c, d).

Suppose x is uniformly distributed random variable, then formula (4) can rewrite as follow:

$$x = \int_c^y g(t)dt \tag{5}$$

Suppose $G(y)$ is the distribution function of random variable y, then formula (5) was changed again to $x=G(y)$. Such is the principle that constructing uniform random variable from ordinary logistic sequence at $\mu = 4$.

Proposition 2: Suppose probability density function of random variable y as follows : $\rho(y) = \begin{cases} \frac{1}{\pi\sqrt{y(1-y)}} & 0 < y < 1 \\ 0 & else \end{cases}$ Then, random variable $x = \frac{2}{\pi}\arcsin(\sqrt{y})$ (6) is uniform (0,1) random variable.

Proof: Let $\rho(t) = \pi^{-1}/\sqrt{t(1-t)}$,

according to formula (5),

$$x = \int_0^y \rho(t)dt = \int_0^y \frac{1}{\pi\sqrt{t(1-t)}}dt = \int_0^y \frac{2\sqrt{t}d\sqrt{t}}{\pi\sqrt{t(1-t)}} = 2\int_0^y \frac{d\sqrt{t}}{\pi\sqrt{1-t}} = 2\int_0^{\sqrt{y}} \frac{dt}{\pi\sqrt{1-t^2}}$$

$$= \int_0^{\sqrt{y}} \frac{2dt}{\pi\sqrt{1-t^2}} = \frac{2}{\pi}\arcsin(\sqrt{y})$$

That is, $x = \frac{2}{\pi}\arcsin(\sqrt{y})$ is uniform (0, 1) random variable. QED

According to proposition 2, formula (6) can transform Logistic sequence at μ=4 into uniform (0,1) random variable.

b) Verification through computer simulation

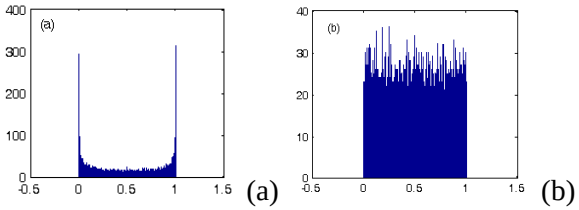


Figure 1

Densities of original Logistic sequence and the transformed Logistic sequence are graphed in Figure 1.

Figure 1(a) showed probability density function of original Logistic sequence, Figure 1(b) showed the probability density function of transformed Logistic sequence. From Figure 1, one can see that the transformed sequence is uniform over the interval (0, 1).

2.2. Random permutation based on position （RPP）

Starting with any initial ordering $P_1, P_2, ..., P_n$, $P_i \in [1, n]$, we pick one of the positions 1,2,…,n at random and then interchange the number in that position with the one in position n. Now we randomly choose one of the position 1,2,…,n-1 and interchange the number in this position with the one in position n-1, and so on.

According to proposition 1, $X = Int(nU)+1$ will be equally likely to take on any of the values 1,2,…,n, we see that the above idea for generating a random permutation can be written as follows:

Step 1. Let $P_1, P_2, ..., P_n$ be any permutation of 1,2,…,*n* (e.g., can choose $P_j = j,\ j = 1, 2, ..., n$).

Step 2. Set $k = n$.

Step 3. Generate a uniformly distributed random variable *U* and let $I = Int(kU) + 1$.

Step 4. Interchange the values of P_I and P_k.

Step 5. Let *k*=*k*-1, and if *k*>1, go to step 3, otherwise, stop.

$P_1, P_2, ..., P_n$ is the desired random permutation.

Algorithm of position based random permutation builted on rand() in matlab was called Rand random permutation and builted on Logistic random uniform distribution was called Logistic random permutation.

3. Image Bit Permutation Based on Rpp

For the purpose of verifying RPP using computer and applying RPP to permute image, image bit permutation scheme was proposed. Of course, one can design any other image scrambling algorithm based on RPP by combing with other rules at the top, this algorithm is a special case for comparison and for clarifying the idea.

3.1. Scheme of image bit permutation

Consider a M*N image with K gray levels.

Step 1. Select an initial value which is associated with the secret key.

Step 2. Generate a random vector V_1 with M elements based on RPP as index array.

Step 3. Rearrange all rows of the image according to V_1.

Step 4. For each row, turn each pixel into bits firstly and get L=N*8 columns.

Step 5. Generate a random vector V_2 with L elements as index array.

Step 6. Rearrange all columns of the current row according to V_2.

Step 7.Repeat step 4-step 7, until the last row of the image.

3.2. Inverse image bit permutation scheme

Decrypting the image is similar to the above process. Image bit permutation scheme built on Rand random permutation was called Rand algorithm and built on Logistic random permutation was called Logistic algorithm.

4. PERMUTATION PERFORMANCE ANALYSIS

4.1. Permutation strength test with simple matrix

For measuring permutation strength of the Logistic permutation algorithm, following algorithm was designed.

Step 1. Generate vector $V = (P_1, P_2, ..., P_n)$,

where $P_j = j,\ j = 1, 2, ..., n$.

Step 2. Permute vector *V* using Logistic random permutation and using sorting permutation of Ye algorithm.

Step 3.Repeat step 1 and step 2 *m* times, get *m*n* permutation matrix.

Step 4.Count the number of different value in every column.

Step 5.Calculate average value and average variance of different elements for all columns.

TABLE I. PERMUTATION STRENGTH TEST RESULTS

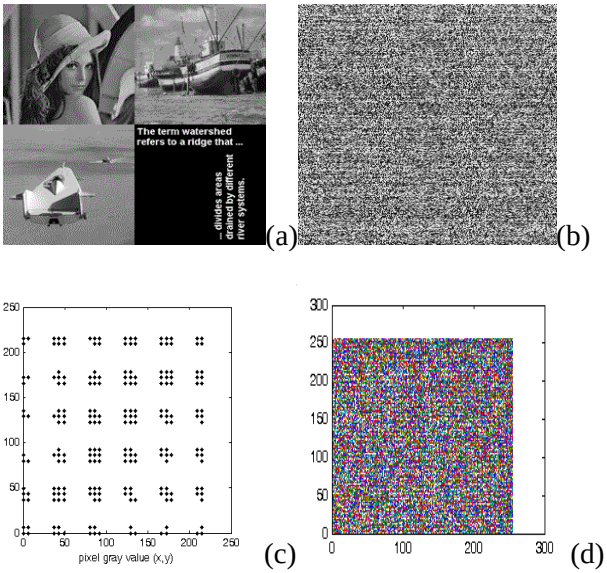
(m, n)	Ye sorting permutation		Logistic random permutation	
	Average	variance	average	variance
(1000,500)	432.0340	37.7083	432.1600	33.8301
(1000,1000)	631.9040	103.1599	632.1780	99.2976
(2000,3000)	1459.5	227.4138	1.459.9	215.4161

From table Ⅰ, although performance of Logistic random permutation is slightly superior to those of Ye sorting permutation [5], it did provide a new effective random permutation scheme which was firmly grounded on mathematical theory.

4.2. Permutation strength test with image permutation algorithm

As far as choosing image is concerned, image (Figure.2. (a)) is a synthesis of four images, including Lena picture, Boat picture, Text picture, Liftingbody picture, which almost concludes all attributes of image. However, there is not smooth transition at the junction among four pictures, this property don't have for natural image, increases the difficulty for image encryption.

Experimental results obtained by the Logistic algorithm can be seen in Figure 1. Figure 1(b) is the cipher-image. Figure 1(c) and (d) show the horizontal direction correlation of the plaintext and cipher-image respectively. From these pictures, one can know that the Logistic scheme has a good cipher effect.



(a) (b) (c) (d)

Figure 2

3)Ddigital characters of permutation image

All kinds of digital characters of permutation image with different algorithms can be seen from Table Ⅱ. From the experiment results, one can see that Logistic algorithm is superior to Rand and Ye algorithm in almost every items. These facts demonstrated that Logistic algorithm has better resistance attack ability.

TABLE II. CIPHER IMAGE DIGITAL CHARACTERS

	Entropy	mean	variance	Histogram variance
Rand algorithm	7.9840	132.0579	75.1712	40.0612
Logistic algorithm	7.9849	132.0050	75.1679	38.8776
Ye algorithm	7.9847	131.8775	75.1665	39.2170

4)Correlation of adjacent pixels

To test the correlation between two adjacent pixels, the following procedures are carried out.

First, randomly selected 10,000 pairs of two horizontal (vertical, diagonal) adjacent pixels from an image and then calculated the correlation coefficient r_{xy} of each pair utilizing the following equations:

$$\mathrm{cov}(x,y) = E(x - E(x))(y - E(y)) \quad r_{xy} = \mathrm{cov}(x,y) / \sqrt{D(x)}\sqrt{D(y)}$$

$$r = mean\,(r_{xy})$$

Where x and y are grey-level values of the two adjacent pixels in the image,

Where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$,

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2\ ,\quad \mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))\ .$$

Repeat the same process 1000 times and get the average value.

TABLE III. AVERAGE CORRELATION COEFFICIENT OF ADJACENT PIXELS

	Horizontal direction	Vertical direction	Diagonal direction
Original image	0.8727	0.7939	0.8518
Rand algorithm	0.0678	-0.0342	0.0576
Logistic algorithm	0.0167	0.0075	-0.0084
Ye algorithm	0.0240	0.1033	0.0592

From table Ⅲ, one can know that the correlation coefficients of original image are approach to 1. Correlation coefficients of image permuted by Logistic, Rand and Ye Algorithm all approach to zero. At the same time, permutation performance of Logistic algorithm is slightly superior to that of the other two.

5. Conclusion

Probability density function of Logistic map at μ=4 is not uniform, which can't be directly used to generate random permutation. To solve this problem, proposition 2 was introduced which can transform non-uniform Logistic sequence into uniformly distributed random sequence. Based on this uniform sequence, random permutation built on position interchange was presented. For measuring permutation strength, an algorithm for this purpose was designed. Utilizing this algorithm, performances of random permutation generated by Ye's algorithm, Baker algorithm and our approach were compared. To verify the effect of the proposed random permutation based on position interchange to image permutation, image bit permutation algorithm was proposed and was compared with Baker and Ye algorithm in statistical analysis, results show that performance of proposed image bit permutation based on Logistic uniform distribution is superior to Ye and Baker methods. And the most importance is Logistic algorithm has firmly theoretical foundation. .

6. Acknowledgment

The work described in this paper was supported by the National Natural Science Foundation of China (Grant No. 61073013), The Key Aeronautic Foundation, china (Grant No. 2010ZA04001).

7. References

[1] C. E. Shannon, "Communication Theory of Screcy Systems," Bell System Technical Journal, Vol. 28(4), pp. 656-715, 1949.

[2] Z. Shi, R. Lee, "Bit Permutation Instructions for Accelerating Software Cryptography," Proc. IEEE ASAP, pp.138-148(2000).

[3] R. Lee, Z. Shi, "Efficient Permutation Instructions for Fast Software Cryptography," IEEE Micro, vol. 21(6), pp. 56-69 (2001).

[4] D. Socek, L. Shujun, et al. "Enhanced 1-D Chaotic Key Based Algorithm for Image Encryption," IEEE, SecureComm2005, pp. 406-407(2005).

[5] Y. Guodong, "Scrambling encryption algorithm of pixel bit based on chaos map," Pattern Recognition Letters, vol. 31(5), pp. 347-354(2010).

[6] Y. Ji Won, K. Hyoungshick, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," Commun Nonlinear Sci Numer Simulat, vol. 15, pp. 3998–4006 (2010).

[7] A. Lasota, M. C. Mackey, Chaos, fractals, and noise– stochastic aspects of dynamics, Springer-Verlag, New York, 2nd Ed, pp. 203-208(1997).

[8] M. Shahram, "Chaotic Image Encryption Design Using Tompkins-Paige Algorithm," Mathematical Problems in Engineering, vol. 2009, pp. 1-22(2009) .

[9] L. Xiangdong, Z. Junxing, et al. "Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation," International Journal of Computer Science and Network Security, vol. 8(1), pp. 64-68(2008).

[10] P. Savicky, "A strong nonrandom pattern in Matlab default random number generator," URL http://www.cs.cas.cz/ savicky/ papers/ rand2006.pdf (2006).

[11] T.Y. Li , J.A. Yorke, “Period three implies chaos,” Amer. Math, Vol. 82, pp. 481-485, 1975

[12] E. Lorenz, “Deterministic nonperiodic flow,” Journal of the Atmospheric Sciences, vol. 20. pp. 130-141,1963.

[13] Edward Ott, Chaos in dynamical systems, Cambridge University Press. 1993, pp.32-38.