A Novel Image Scrambling Algorithm for Digital Watermarking Based on Chaotic Sequences

Zhu Liehuang[†], *Li Wenzhuo*[††], *Liao Lejian*[†], *Li Hong*[††],

[†]School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China
[††]School of Software, Beijing Institute of Technology, Beijing, China

Summary
The main aim of digital image scrambling is to transform a meaningful image into a meaningless or disordered image in order to enhance the power to resist invalid attack and in turn enhance the security. This paper presents a new scheme of digital image scrambling based on the cat chaotic mapping. Firstly we use a cat chaotic mapping to disorder the pixel coordinates of the digital image and then perform exclusive OR operation between certain pixel value of the digital image and a chaotic value that is dependent on the encryption parameters, the iterative time and the coordinates. This is a new diffusion technique to uniform the statistical characteristics of the encrypted digital image. This method is easy to realize, has satisfied scrambling effect, and can be used as pretreatment for digital image hiding and disguising.

Key words:
Image Scrambling, Digital Watermarking, Chaotic Sequences, Cat Mapping.

Introduction

The main aim of digital image scrambling, which is used as the preprocessing or post-processing in image information hiding, is to transform a meaningful image into a meaningless or disordered image in order to enhance the power to resist invalid attack and in turn enhance the security [1].

The encryption permutation of the digital image requires applying "permutation" and "diffusion" mechanism alternately [2]. Permutation is used to transform the pixel coordinate of the graph, while diffusion is used to iterative the pixel value of the graph, in order to uniform the statistical characteristics of the encrypted graph, and complicate the relationship between the plaintext graph and cipher text graph. But all the current methods suffer from some problems to be presented in section 2.

In this paper, we firstly use a cat chaotic mapping to disorder the pixel coordinates of the digital image. Based on the cat chaotic mapping, we use a new diffusion technique to uniform the statistical characteristics of the encrypted digital image. A chaotic value, which is dependent upon the encryption parameters, the iterative time and the coordinates, would be performed exclusive OR operation with certain pixel value of the digital image. Thereby we obtain the encrypted message. In order to restore the information, the disordered digital image should be performed inverse exclusive OR operation and inverse cat mapping.

For the chaotic cat mapping is sensitive to the initial value, which guarantees the uniqueness and unbreakable of the disordering process. The technique which we put forward can be applied directly on digital watermark's making, data encryption technique, information's hiding and so on. In the end we present the scheme, the experimental results have shown that the new diffusion technique can solve the problems, the method is very effective to uniform the statistical characteristics of the encrypted graph, and the efficiency of this method is very high.

2. Related Work and Issues

2.1 The Cat Chaotic Mapping

According to reference [3,4], the cat chaotic mapping is a discrete chaotic modal proposed by Arnold and Avez. The image can be permutated and the mapping is defined as below:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod} 1), \quad A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \qquad (1)$$

In order to apply encryption to the cat map, we need some encryption parameters. Encryption parameters can be introduced by changing the elements of the matrix A. Then, the cat map can be extended to $N \times N$, and be discredited.

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A_d \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\, N),$$

$$A_d = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix}, \quad a, b \in N . \qquad (2)$$

Theorem: the cat map defined by formula (2) has such properties as below:

1. There is a Lyapunov exponent that is over zero;
2. A cat map is a bijective mapping;
3. Parameter a and b have the same period of N.

Lyapunov exponents play an important role in the research of character tics of bifurcation and chaotic motion of dynamics. Property 1 indicates that the mapping defined by formula (2) is a chaotic mapping in [6], and property 3 requires that ‘a’ and ‘b’ must be integers less than N.

2.2 The Diffusion of the Pixel Value

Weiwei Xiao et al [3] presented a method to diffuse pixel value. They generated a chaotic sufficiently long sequence $c_1, c_2, \cdots, c_m$ from a definite chaotic modal, mapped the sequence to another sequence $p_1, p_2, \cdots p_m$ over the pixel domain of the graph, and did certain calculation between the sequence $p_1, p_2, \cdots p_m$ and the pixel values. Since the chaotic sequence presents some kind of random property, the graph after transformation is also some kind random, which can realize the encryption of the graph. The course of decryption is also simple, in which only related inverse calculation between the sequence $p_1, p_2, \cdots p_m$ and the encrypted graph is needed. Actually, this method is a realization of the encryption of the chaotic sequence. For this method, in the course of decryption, $p_1, p_2, \cdots p_m$ is needed. And for most cases, the condition for transporting large amount decryption information is not guaranteed.

Mao Y B et al [5] divided the whole graph into pieces, and then putted the pixel values of the graph into a chaotic map to do the iterative calculation so as to change each pixel value. For this method, the graph should be divided into several small pieces. If the pieces are too small, the pixel value of each point in the same piece will be the same, so the pixel value diffusion effects can not be achieved. On the contrary, if the pieces are too large, the calculation can be very complicated. By using this method, the diffusion effect for the common black letter-white grounding is very bad.

3. A New Diffusion Technique

3.1 Characterization of the Algorithm

In order to solve the problems mentioned above，we deign a new diffusion technique based on the cat chaotic mapping. The experimental results have shown that the new diffusion technique can solve the above cited problems. The method is very effective to uniform the statistical characteristics of the encrypted graph, and its efficiency is very high.

If we only use the cat chaotic mapping to disorder the pixel coordinates of the digital image, it can not uniform the statistical characteristics of the encrypted graph and change the histogram of the digital image. Without change the histogram it can leave the chance for the cryptanalyst to decrypt the ciphertext. So we must iterate the pixel value of the graph to uniform the statistical characteristics of the encrypted digital image.

We use the cat chaotic mapping to transform the pixel coordinate of the digital image，using the formula（2）, we translate the original coordinates (x, y) of the image information into the new coordinate (x', y'). We can get that:

$$\begin{cases} x' = (x + ay) (\mathrm{mod}\, N) \\ y' = (bx + (ab+1)\, y) (\mathrm{mod}\, N) \end{cases} . \quad (3)$$

Firstly with the cat chaotic mapping, we translate (x, y) into $((x+ay)(\mathrm{mod}N),(bx+(ab+1)y)(\mathrm{mod}N))$ and disorder the coordinates of the image information. Secondly in order to diffuse the pixel value, we should calculate $f(x, y, a, b, k)$ which performed exclusive OR operation with certain pixel value P of the coordinates $p(x, y)$ to get a new pixel value P'. k is the iterative time.

$$P' = P \wedge f(x, y, a, b, k). \quad (4)$$

In this paper, we define $f(x, y, a, b, k)$ as follow.

$$f(x, y, a, b, k) = (x' \times y' + k)(\mathrm{mod}\, N) = \left((x + ay) \times (bx + (ab+1)\, y) + k\right)(\mathrm{mod}\, N) . \quad (5)$$

The chaotic mapping is sensitive to the initial value, which guarantees the uniqueness and unbreakable of the disordering process.

This process means that we generate a chaotic sequence $f_{x,y}^{k}$ from the cat chaotic mapping. Here $f_{x,y}^{k}$ is a chaotic value that is dependent on the encryption parameters, the iterative time and the coordinates. And then we do exclusive or operation between the sequence $f_{x,y}^{k}$ and the pixel values. Since the chaotic sequence presents some kind of random property, the graph after transformation is also some kind random, which can realize the encryption of the graph. Actually, this method is a realization of the encryption of the chaotic sequence. And for the different iterative times k, the value of the a chaotic sequence $f_{x,y}^{k}$ is different too, so at every iterative time, we will generate a different chaotic sequence $f_{x,y}^{k}$. So this method is more secure than the first method we introduced in section 2. In the course of decryption, only a, b, k is needed.

3.2 Encryption Algorithm

Figure 1 illustrates the dataflow of our encryption algorithm, where a, b are the encryption parameters of the cat chaotic mapping. We can iterate k times to induce security of encrypted watermark.

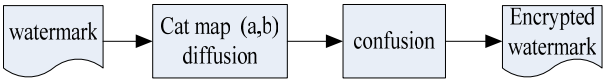
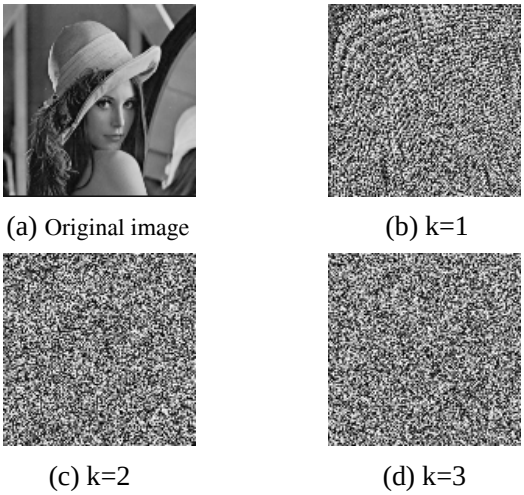


Fig. 1 Chaotic encryption to original watermark signal

Figure 2 shows the scramble results of the digital image Lena after iterating different times our algorithm, when $a = 80, b = 4$.



(a) Original image (b) k=1

(c) k=2 (d) k=3

Fig. 2 Scramble results after iterating different times.

According to figure 2, we can get that our algorithm is very effective to uniform the statistical characteristics of the encrypted graph, and the efficiency of this method is very high. Using the technique presented in this paper, after doing the iterative calculation only twice, we can get very good encrypted image. The encrypted image doesn't seem to have any relevance to the original image in appearance.

3.3 Decryption Algorithm

The procedure for the decryption is similar with encryption, except that the inverse permutation transformation formula can be changed as:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\, N), A^{-1} = \begin{pmatrix} ab+1 & -a \\ -b & 1 \end{pmatrix}. \quad (6)$$

Before every inverse permutation transformation, we should perform exclusive OR operation with the pixel value for each pixel coordinates. When compiling the simulation program, our algorithm will induce error in the course of inverse transformation. The solution is during the course of cat map we construct the look-up table, and in the course of decryption we perform the look up the table and do the calculations.

4 Security Analyses for the Algorithm

4.1 Key Space Analysis

Firstly, the key is main the controlling parameter and encryption parameter for the cat map. Obviously, the more times we encrypt, the larger the key space can be. For example, if we do the encryption only once, for a graph of 64×64, the key space can only be 2^{12}. However, if we do the encryption 4 times, the key space for the system can be $2^{16\times 4}$. Furthermore, the key space is also dependent on the size of the graph, i.e. the larger the graph is, the larger the key space is.

Secondly the confusion sequence $f(x, y, a, b, k)$ is also dependent of both the encryption parameter a, b and the iterative time k.

4.2 Avalanche Effect

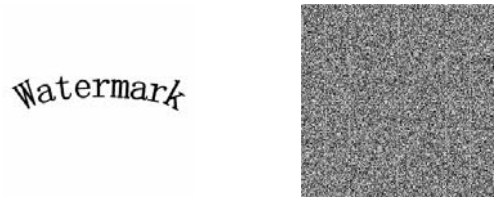
Considering the validity of the key changing, the key grouping algorithm is sensitive to the change of the key, i.e. it has the avalanche effect. According to the strict avalanche effect in the grouping key measurement, changing arbitrary bit of the key can induce almost a half bits to change in the cipher text group.

MSE（Mean Square Error）can directly reflect the differences of the quality between the two digital images. In [9] the emulation uses MSE as the standard to measure the quality of the decoded two digital images. The MSE between the pictures can be defined as:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M} \sum_{j=0}^{N} \left(P_1(i, j) - P_2(i, j) \right)^2 \quad (7)$$

Here, M, N is the width and height of the digital image, $P_1(i, j)$ is the pixel value of the original digital image, and $P_2(i, j)$ is the pixel value of the decoded digital image.

Figure 4 shows altering parameter a very little produces avalanche effect, when $b = 4, k = 3$. MSE between (b) and (c) is 40.46 db.

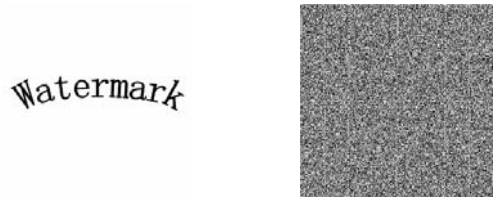


(a) Original image (b) a=80

(c) a=81 (d) different image between (b) and (c)

Fig.3 Altering a produces avalanche effect

Figure 4 shows iterating different times produces avalanche effect, when $a = 80, b = 4$. MSE between (b) and (c) is 41.21 db.



(a) Original image (b) k=2

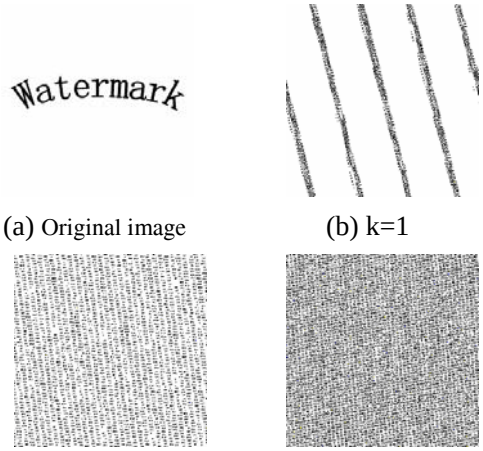
(c) k=3 (d) different image between (b) and (c)

Fig. 4 Iterating different times produces avalanche effect.

Generally if $MSE \geq 30$ db, the quality differences between the two digital images is evident. And using the method in this paper, we get MSE = 40.46 db and MSE = 41.21 db, this result show that out arithmetic is sensitive to the change of the key.

4.3 Statistical Characteristics of the Encrypted Digital image

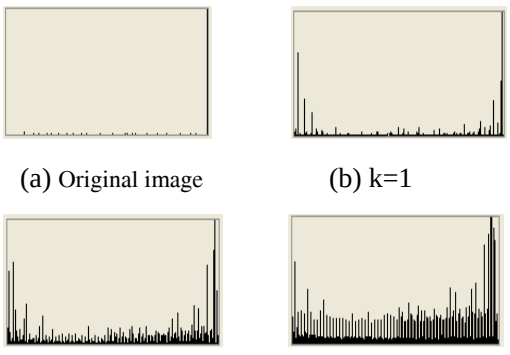
Using some current methods, the diffusion effect for the black-white image is very bad. Figure 5 shows the scramble results of a black-white image after iterating different times the algorithm proposed in [7], when $a = 80, b = 4$. Figure 6 lists the histograms of the image in figure 5.



(a) Original image (b) k=1

(c) k=2 (d) k=3

Fig. 5 Scramble results of a black-white image of the algorithm proposed in [7]



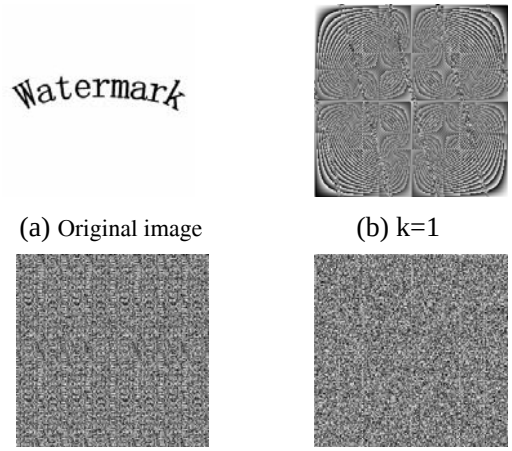
(a) Original image (b) k=1

(c) k=2 (d) k=3

Fig. 6 The histograms of the images in Fig,5.

In [7], author divides the whole digital image into several small pieces, which piece has four pixels. And then the pixel values of the digital image are put into a chaotic map to do the iterative calculation so as to change each pixel value. The pieces are small and the image is the common black letter-white grounding, so the pixel value of each point in the same piece will be the same. As it shows in figure 6, the pixel value diffusion effects can not be achieved. After doing the iterative calculation three times, the result of uniform is bad.

However using the technique presented in this paper, we can get the result as figure 7. Figure 8 lists the histograms of the image in figure 7.



(a) Original image (b) k=1

(c) k=2 (d) k=3

Fig. 7 Scramble results of a black-white image of our algorithm.

(a) k=1 (b) k=2 (c) k=3

Fig. 8 The histograms of the images in Fig,7.

According to figure 8, after doing the iterative calculation only once, the statistical characteristics of the digital image has changed remarkably. Again after doing the iterative calculation only twice, we can get very good pixel value diffusion effects.

5. Conclusion

This paper proposes a new scheme of digital image scrambling based on the cat chaotic mapping. Firstly we used a cat chaotic mapping to disorder the pixel coordinates of the digital image. And then we performed exclusive OR operation between certain pixel value of the digital image and a chaotic value that is dependent on the encryption parameters, the iterative time and the coordinates. Thereby we obtain the encrypted message. This is a new diffusion technique to uniform the statistical characteristics of the encrypted digital image. The experiment results have shown that the new diffusion technique is very effective to uniform the statistical characteristics of the encrypted graph, and the efficiency of this method is very high.

References

[1] Chiou Ting Hsu, and Ja Ling Wu, "Hidden digital watermarks in Image", *IEEE Transactions on Image Processing*, Vol.8, No.1, Jan 1999. 58-68.

[2] Katzenbeisser S, and Petitcolas F. *Information Hiding Techniques for Steganogr by and Digital Watermarking*. Artech House, Boston ,2000.

[3] Weiwei Xiao, Zhen Ji, Xhong Zhang, and Weiying Wu. "Watermarking algorithm based on chaotic encryption", Proceedings of IEEE Region 10 Technical Conference on Computers, Communication, Control and Power Engineering. Beijing, Oct. 2002: 28-31

[4] G. R .Feng, L. G. Jiang, C. He and D. J. Wang, *"A Novel Algorithm for Embedding and Detection Digital Watermarks"*, IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'30), April 6-10, 2003, 549-552.

[5] Y B Mao, and G Chen, *"Chaos-based image encryption"*, In Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics. Springer-Verlag New York, 2005. 231-265.

[6] A. Wolf, J. Swift, H. Swinney, and J. Vastano, "*Determining lyapunov exponents from a time-series*," Physica. D, vol. 16, 1985. 285-317.

[7].I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers,New York, 2002.

[8] Y B Mao. "Research on Chaos-based Image Encryption and Watermarking Technology", PhD thesis, Department of Automatation, Nanjing University of Science & Technology, Nanjing, China, Aug 2003.

Zhu Liehuang received the M.S. degree in Computer Science from Wuhan University in 2001 and Ph.D degree in Computer Science from Beijing Institute of Technology in 2004. He has also worked as a lecturer of Computer Science at Beijing Institute of Technology from 2004. His research interests are in cryptographic algorithms and protocols for cryptography, computer arithmetic, computer and network security.