Digital Watermarking Algorithm Based on DWT and Chaotic Scrambling

Huang Hui-fen

WuHan University of Technology， ShanDong YingCai University

E-mail: shouyu1976@163.com

Abstract: A kind of digital watermarking algorithm based on DWT and chaotic scrambling is realized in this text; firstly, make the scrambling transformation and encryption to watermarking image by using chaotic system. Make the carrier image into blocks by 8*8, transform every block by two-dimension DWT; chose a low frequency coefficient from every block as watermarking information embedment point and embed watermarking image, then make inverse DWT transform. The experiment results show that, the algorithm strength the image robustness, and improve the safety of watermarking, could resist the attack of Salt & Pepper Noise JPEG compression.

Key words: binary watermarking; scrambling sequence; scrambling embedment; wavelet transformation

1. Introduction

As the fast development of multi-media technology, there are growing cases of multi-media data piracy, in order to solve this problem, so comes out the watermarking technology. It is paid much attention and become an effective technology applied in digital products patent protection and data certificate.

Image chaotic scrambling with image scrambling is a usual technology applied technology in image information encryption; it has advantage points in fast speed, good results and so on. Among the common methods used in image scrambling, there are Arnold transformation [1][2], magic squares[3][4], Conway games[5], Cray code[7], Affine Module Transformation. The scrambling image results come from the above methods are different, yet because they have some certainty, there are some rules to follow in the scrambled images, and the calculation scale is big, the safety level is low.

Chaotic phenomena appear in nonlinear dynamical systems, the single is certain while the whole may take the look like a random dynamic process. The process is has no cycle features and not convergence. It has great sensitivity to the initial value and dependency and often used in data encryption. In this text, we want to use it in image scrambling, make wavelet transformation to the carrier image, and embed the scrambled and encrypted binary watermarking image into the wavelet low frequency band and raise the safety of watermarking at certain level.

2. Chaotic scrambling

2.1 The outcomes of chaotic sequence

The current extensively applied chaotic sequence could come out from the Logistic mapping. It is a very simple but very meaningful non linear iterative formula. Though it has specific form, does not include any random factor, yet it could come out totally random and very sensitive sequence to the dynamic transformation and initial value of parametric μ [8]. It takes the usual form like:

$$x_{n+1} = \mu x_n (1 - x_n) \tag{1}$$

Among it, x_n is the mapping alternatives，$0 \le x_n \le 1$； μ is the system parameter，$1 < \mu \le 4$ 。

When $3.569945 \le \mu \le 4$, the mapping comes out real value chaotic sequence. Logistic mapping is in a state of chaotic. Chaotic sequence has the advantages of easily generated, pseudo-random, long-term unpredictability, similar to white noise, as well as sensitive to the initial value.

2.2 Chaotic scrambling

A chaotic random sequence comes from n times of iterative. It chooses μ= 4 here, use the chaotic sequence to process the watermarking image and get the chaotic watermarking image.

(1) Made the initial vale x_0 , y_0 as the key to the sequence，use the chaotic sequence $(x_0, x_1, \cdots, x_{m-1})$, $(y_0, y_1, \cdots, y_{n-1})$ gotten from images， m, n is the row and line No. of watermarking images. These two chaotic sequence is redeemed as row address generator and line address generator.

(2) Renew the orders of the item in chaotic sequence, it should comes from small to big,

and get a new sequence. $(x_0', x_1', \cdots, x_{m-1}')$, $(y_0', y_1', \cdots, y_{n-1}')$。 Because there are no equal spots in chaotic sequence, which is: $(x_0' < x_1' < \cdots < x_{m-1}')$, $(y_0' < y_1' < \cdots < y_{n-1}')$.

(3) Scan the scrambled image in the shape of word "Z", and encode it by 0 and 1, get the binary sequence, thus the watermarking image is secretly pre-processed, increase the data safety and secrecy. And it could also revert to the initial watermarking image. Figure 1 is the initial and scrambled watermarking image.

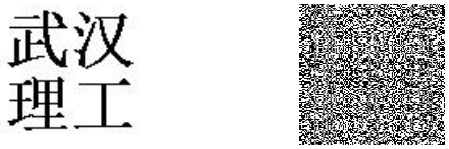

Fig.1 initial watermarking and scrambled watermarking

3. Digital w atermarking based on on DWT and Chaotic Scrambling

Make the carrier image into blocks by 8*8, transform every block by two-dimension DWT; chose a low frequency coefficient from every block as watermarking information embedment point and embed watermarking image, then make inverse DWT transform and get the watermarked image, The watermarking image is binary image, the watermarking should be scrambled in row and line before the watermarking embedment process. The process of drawing watermarking image is to make the inverse calculation of loading watermarking algorithms, draw the scrambled watermarking and revert it.

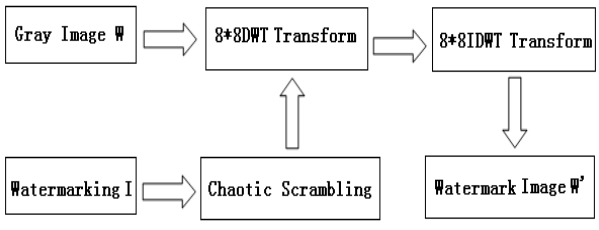

fig.2 Water mark embedding process

3.1 Watermarking embedment

(1) Make carrier image, whose size is $m*n$ into $8*8$ image blocks $g_i (i = 1,2,3,\cdots,t)$

(2) Because when the image is attacked by compression and filter, the high frequency information will lose firstly, in order to make the watermarking information has well anti attack ability, make three level discrete wavelet dissolve to every image block g_i, and get the band $LL3, HL3, LH3, HH3$, detract the low frequency coefficient from the wavelet.

(3) Make it the same size with the dissolved band $LL3$ by extracting the encrypted scrambling watermarking and add up. Make the adjusted watermarking image overload into $LL3$, then comes $LL3' = LL3 + \partial M$, ∂ is the watermarking embedment strength.

(4) Make the watermarking embedded carrier image W by 8*8 DWT reverse transformation, get the watermarking embedded image W', the host image is $131*131$ lena gray image, watermarking embedment strength is 0.34, the embedded result is showed in figure 3. Figure 3 is the embedded image.

Fig. 3 the embedded image

3.2 The extraction of watermarking

In the process of detracting the watermarking, the two keys x_0, y_0 of chaotic scrambling must be known. The watermarking detraction process is similar to the embedment process , the detail process is like below:

(1) Firstly, make the integer wavelet transformation to the watermarking carrier image, detract the low frequency coefficient in wavelet, there is watermarking information.

(2) Make the low frequency coefficient in wavelet into blocks and make DWT

978-1-935068-01-3 © 2009 SciRes.

transformation. Detract from the DWT coefficient matrix 0 and 1 and encode to them, make all the encoding frequency combine together to form a two dimensional encoding matrix.

(3) Use the key x_0, y_0 form chaotic matrix and adjust the sequence of encoding matrix in (2), binary image converted from the newly adjusted 0、1 matrix is watermarking image. Then the decoded two digital watermarking image comes out as figure 4.

Fig. 4 wat ermarking extraction

4. Emulation experiment

4.1 Watermarking embedment experiment

The image takes changes after the embedment process, in order to evaluate the change before the very action of embedment, Peak signal to noise ratio for images is brought in here [9]. The current PSNR=42.1could be gotten from the formula (2).

$$PSDN = -10\log\frac{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(C(i,j)-D(i,j)\right)^2}{A^2} \quad (2)$$

4.2 Anti attack experiment

The common image attack methods include compression, scale, cut and noise and so on. In order to test the performance of this algorithm, the detracted watermarking image is as figure 5.

（a）5% Salt-and-Pepper Noise

（b）JPEG-15compression

（c）5*5 Mid value filter

Fig. 5 watermarking extraction after adding a variety of attacks

The experiment results shows that the digital watermarking algorithm raised in this text has certain resistance to the attacks, especially to the scale attacks. Even the watermarking embedded image is badly damaged after the attacks; competitive complete watermarking information could be detracted, it could be proved from the PSNR.

5. Acknow ledgment

Digital watermarking algorithm is realized by a kind of chaotic mapping in this text, it make the images scramble by using chaotic mapping characteristics. It has following characteristics:

- ✧ It could be got from chaotic mapping parameter and initial background; there is no need to
- ✧ waste unnecessary space to hold the full sequence
- ✧ Large sum of chaotic sequence could be got by using the initial background, usually it is very hard to get the initial background presumed from a limited length, which is very important to information safety.
- ✧ The embedment of watermarking reaches low frequency area of the depth of wavelet transforms, thus strengthen the robustness of algorithm.

References

[1] van Schyndel R G, Trikel A Z, Osborne C F. A digital watermark First IEEE International Image Processing Conference, 1994; 2:86—90

[2] Lumini A， Maio D. A wavelet-based image watermarking scheme，in Proc. Int. Conf. Information Technology，2000: 122-127.

[3] Yen J C, Guo J I. Efficient Hierar-chical Chaotic Image Encryption Algorithm and Its VLSI Realisation [J]. IEEE Proceedings of Visual Image Signal Process, 2000, 147(2): 167-175.

[4] Yen J C, Guo J I. Design of a New Signal Security System [J]. IEEE Proceedings of International Symposium on Circuits and Systems.2002, (4): 121-124.

[5] Chen H C, Yen J C, Guo J I. Design of a New Cryptography System [M]. Berlin, Germany: Springer-Verlag, 2002.

[6] Ferraiolo DF., Sandhu R., Gavrila S. Proposed NIST standard for role- based access control. ACM Transactions on Information and System Security, 2001, 4(3): pp. 224- 274

[7] Weizhong Qiang, Hai Jin, Xuanhua Shi, Deqing Zou. A Novel VO- Based Access Control Model for Grid. Berlin Heidelberg:Springer- Verlag , 2004,3251, pp. 293－300

[8] Francis B., Afinidad, Timothy E., Levin, Cynthia E., Irvine, Thuy D., Nguyen. Foundation for a Time Interval Access Control Model. MMM- ACNS 2005, LNCS 3685: pp. 406- 411

[9] Suroop Mohan Chandran, J.B.D. Joshi. LoT- RBAC: A Location and Time- Based RBAC Model. WISE 2005, LNCS 3806: pp. 361－375