*Sensors & Transducers, Vol. 21, Special Issue, May 2013, pp. 153-158*

www.sensorsportal.com

**Sensors & Transducers**



*http://www.sensorsportal.com*

# Adaptive Watermarking Algorithm in DCT Domain Based on Chaos

**Wenhao Wang**

Computer Engineering Faculty, Huaiyin Institute of Technology,
Huaian, Jiang Su, 223003, China
E-mail: wenhaowang2013@sina.com

*Received: 26 March 2013 /Accepted: 14 May 2013 /Published: 30 May 2013*

**Abstract:** In order to improve the security, robustness and invisibility of the digital watermarking, a new adaptive watermarking algorithm is proposed in this paper. Firstly, this algorithm uses chaos sequence, which Logistic chaotic mapping produces, to encrypt the watermark image. And then the original image is divided into many sub-blocks and discrete cosine transform (DCT).The watermark information is embedded into sub-blocks medium coefficients. With the features of Human Visual System (HVS) and image texture sufficiently taken into account during embedding, the embedding intensity of watermark is able to adaptively adjust according to HVS and texture characteristic. The watermarking is embedded into the different sub-blocks coefficients. Experiment results haven shown that the proposed algorithm is robust against the attacks of general image processing methods, such as noise, cut, filtering and JPEG compression, and receives a good tradeoff between invisible and robustness, and better security. *Copyright © 2013 IFSA.*

**Keywords:** Watermarking, Chaotic encryption and decryption, DCT, Human visual system, Texture, Attack test.

## 1. Introduction

With the rapid development and wide application of the multimedia and network technology, the storage, replication and transmission of digital media become very convenient, which has made a serious social problem of the ownership of products. As the time requires, digital watermarking develops rapidly as a copyright protection technology. At present, there are mainly the space domain algorithms and transform domain algorithms [1, 2]. The spatial domain algorithm is that watermark information is embedded directly into the pixels of the image. This algorithm is simple, but robustness is poor a. As for the transform algorithm, such as discrete wavelet transform (DWT) and discrete cosine transform (DCT), it can make the energy distribute to all the pixel space, so the algorithm has good robustness and application prospect [3, 4].

The key techniques of the watermark algorithm are the degree of image scrambling and the location and intensity of embedding. In scrambling aspects, there is mainly Arnold transform at present. The essence of Arnold shuffling is an iterative process, which needs high time complexity, and this shuffling has periodic. So the algorithm is poor security and easily cracked. Now many scholars study on the chaos systems characteristics. The watermark data encrypted by chaos can ensure the security of the transmission. In the aspect of watermark embedding location, research results have shown that humans' eyes are more sensitive to the parts of the low frequency. If the watermark information should be embedded into the high frequency parts of the image, it will lose information because of the attacks of noise, filter, and compression. So the watermark information is embedded into the intermediate frequency part of the image. In terms of the watermark embedding strength, research results have shown that the higher watermark energy is embedded, the watermark imperceptibility will be worse. But the robust will be better .On the contrary, the lower watermark energy is embedded;

the watermark imperceptibility will be much better. But the robust will be worse. So the embedding strength should be adjusted with the luminance and image texture.

In view of this, this paper presents an adaptive watermarking algorithm based on Chaos in DCT domain. Firstly encrypt the watermark image with the logistic chaos technology, and then make sure embedding strength according to the features of Human Visual System (HVS) and image texture, finally, the watermark is embedded into the DCT intermediate frequency coefficients.

## 2. Encryption Based Chaos

### 2.1. Chaotic Encryption

The Chaos is a kind of complicated dynamics system. Chaos is the process of the determining and random in the nonlinear dynamic system, and the process is neither periodic nor convergence, and it has extremely sensitive dependences to initial value. It is often used to encrypt the image to improve the security performance of image [5, 6]. The chaotic systems mainly include: Logistic Mapping, Tent-Map Mapping, Rosslea System, Lorenz System, Chen System, Lu system and so on. Logistic mapping is the simplest mapping among these mapping. The formula is described as follows:

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

When $3.5699456....<u\leq 4$, the Logistic function will work in a chaotic state, and will generate the neither periodic nor convergence sequence $\{x_k : k = 0,1,2,...\}$. So the security of watermarking information can be greatly improved, if watermark image is encrypted by Logistic chaotic sequence.

### 2.2. Chaotic Encryption Based on Logistic

Suppose that $\{P_n\}$ is a plaintext information sequence, $\{K_n\}$ is the key information sequence, $\{C_n\}$ is the cryptograph information sequence.

The encryption algorithm based on the chaos is described as follows:

$$\{C_n\} = \{P_n\} + \{K_n\} \tag{2}$$

As shown Fig. 1 is the principle of the encryption and decryption based on chaotic:

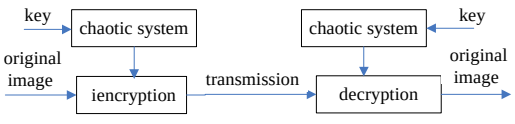



**Fig. 1.** The encryption and decryption based on chaotic.

The key is freely chosen by the user in Fig. 1. It makes decryption more difficult. Besides, so very small initial errors will transmit to the relevant domain space quickly. This feature also increases the difficulty of decryption. The specific algorithm is as follows:

(1) Input the original image, the key $u$ and $Xstart$.

(2) According to Logistic function, calculate $N$ times again and again (The $N$ value is random number), Final function value is referred to y and $Xstart = y$.

(3) Compute chaos byte. Reading each pixels information, Computing 8 times again and again according to the Logistic function, Each times generates a bit of $chaos$ value, which this value rests with the size of $y$ and $u/6$. If $y \geq u/6$, $chaos = 1$. Otherwise $chaos = 0$. Finally, they will be assembled into a byte. The new value will be generated through this chaos value XOR pixel value.

(4) Continue reading the next pixel, computing the next chaos byte, and carrying on XOR operation, such as deals with all the pixels in the image, finally, the encrypted image will be got.

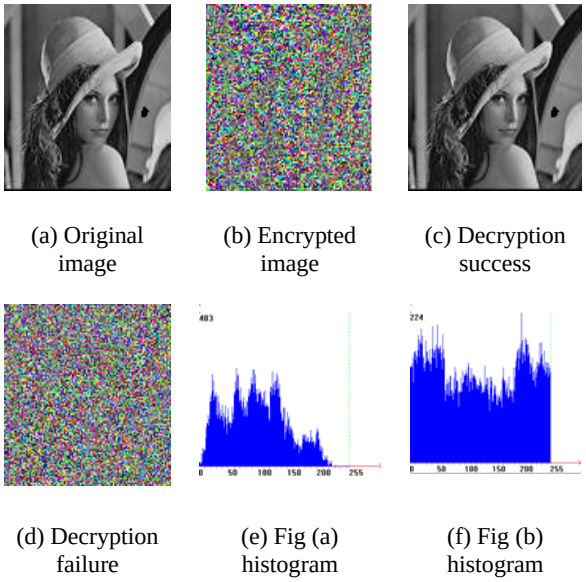
This algorithm is the symmetric algorithm. The decryption is the same key with the encryption. As long as keys are correct, the encrypted image can be correctly decrypted. As shown Fig. 2 is the test results, when $u = 3.9$ and $Xstart = 0.7$; as shown Fig. 2 (a) is the original image; as shown Fig. 2 (b) is the encrypted image; The original image information has been scrambled, which has achieved the better visual effect; as shown Fig. 2(c) is the correctly decrypted result; as shown Fig. 2 (d) is the decrypted result, when $u = 3.9000001$, $Xstart = 0.7$. Although the error is very small, Fig. 2 (b) can be the correctly decrypted. As shown Fig. 2 (e) is the histogram of Fig. 2(a). As shown Fig. 2 (f) is the histogram of Fig. 2 (b); Obviously, the histogram of the watermark image can be changed by chaotic encryption, which makes it uniform distribution and avoids the possibilities that attacker may detect the watermark using statistical methods.

## 3. Adaptive Watermarking Algorithm

### 3.1. DCT Transform

Suppose the image is denoted as $f(x,y)$, $0 \leq x \leq N-1$, $0 \leq y \leq N-1$, $f_m(i,j)$ is a $8\times 8$ sub-block. $0 \leq i \leq 7$, $0 \leq j \leq 7$, $m = 0,1,2,..,(N^2/64)-1$. The formula of DCT transform is as follows:

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{i=0}^{7}\sum_{j=0}^{7} f_m(i,j)\times\cos\left[\frac{(2i+1)u\pi}{16}\right]\cos\left[\frac{(2j+1)v\pi}{16}\right] \tag{3}$$



(a) Original image (b) Encrypted image (c) Decryption success

(d) Decryption failure (e) Fig (a) histogram (f) Fig (b) histogram

**Fig. 2.**The encrypted and decrypted based on Logistic

The formula of IDCT transform is as follows:

$$f_m(i,j)=\frac{1}{4}C(u)C(v)\sum_{u=0}^{7}\sum_{v=0}^{7}F(u,v)\times\cos\left[\frac{(2i+1)u\pi}{16}\right]\cos\left[\frac{(2j+1)v\pi}{16}\right] \tag{4}$$

$$C(u)=C(v)=\begin{cases}\frac{1}{\sqrt{2}} & u=v=0\\ 1 & other\end{cases}, \tag{5}$$

where $f_m(i,j)$ is the grey value of the pixel $(i,j)$, $F(u,v)$ is the DCT coefficient, $F(0,0)$ is the $DC$ coefficient, the other is AC coefficient. Research results have shown that humans' eyes are more sensitive to the low-frequency noise. So the watermark should be embedded into the high frequency part of original image. However, it will lose information because of the attacks of noises, filter, and compression. It will have influence on the robustness of the watermark. In order to solve this contradiction, in this paper, watermark is embedded into the intermediate frequency of the original image.

### 3.2. Adaptive Embedding Strength

The formula, which watermarking is embedded based on DCT, is as follows

$$F'(u,v)=F(u,v)+\alpha_k w_i \tag{6}$$

The higher brightness of the background (The DC coefficient is bigger) becomes, and the higher the watermark embedding strength will be; the more complex image texture is (the greater variance of image is), and the higher watermark embedding strength will be [7]. In this paper, the embedding strength based on the luminance masking and texture characteristic is adaptively adjusted. The calculation of the embedding strength factor is described as follows:

(1) The original image $f(x,y)$ is divided into $K\times8\times8$ sub-blocks, each sub-blocks is denoted as $f_k'(x',y')\ \ 0\le x',y'\le 7$, ( $k=0,1,2...,K-1$ ), where $K$ is the number of sub-blocks. DCT transform is applied to each sub-block. Sub-blocks coefficients through the DCT transform are denoted as $F_k(u,v)$. The calculation formula of the mean value and variance is as follows:

$$u_k=\frac{1}{64}\sum_{i=0}^{8}\sum_{j=0}^{8}F_k(u,v) \tag{7}$$

$$\sigma_k=\frac{1}{64}\sum_{i=0}^{8}\sum_{j=0}^{8}(F_k(u,v)-u_k) \tag{8}$$

(2) Calculate the embedding strength factor of each sub-block. Suppose $min\sigma_k$ is the minimum variance, $max\sigma_k$ is the maximum variance, $minL_{DC}$ is the minimum value of DC coefficient; $maxL_{DC}$ is the maximum value of DC coefficient. The formula is as follows:

$$\alpha_1\frac{\sigma_k-min\sigma_k}{max\sigma_k-min\sigma_k} \tag{9}$$

$$\alpha_2=\frac{L_{Dc}-minL_{DC}}{maxL_{DC}-minL_{DC}} \tag{10}$$

So embedding strength factor is described as follows: $\alpha_k=\alpha_1+\alpha_2$ , $i=0,1,2,...K-1$ .The embedding strength can be changed with the characteristic of the illumination and image texture. Namely, the embedding strength is adaptive.

(3) Calculate the threshold of the embedding factor $\alpha_k$. According to the signal-to-noise ratio (SNR) and formula (6), the formula is as follows:

$$SNR=20\lg\frac{\sqrt{\sum_{k=0}^{K-1}F_k(u,v)^2}}{\sqrt{\sum_{k=0}^{K-1}(F_k'(u,v)-F_k(u,v))^2}}=20\lg\frac{\sqrt{\sum_{k=0}^{K-1}F_k^2(u,v)}}{\alpha_k\sqrt{\sum_i(w_i)^2}} \tag{11}$$

$$\alpha_k=\frac{\sqrt{\sum_{k=0}^{K-1}F_k^2(u,v)}}{\alpha_k\sqrt{\sum_i(w_i)^2}}10^{-\frac{SNR}{20}} \tag{12}$$

The single-to-noise ratio ( *SNR* ), is often in above 20 dB. it will affect the visual effect of image below 20 dB. The *SNR* in the formula (12) was replaced with a 20; the following threshold value is as follows:

$$\bar{\alpha} = \frac{\sqrt{\sum_{k=0}^{K-1} F_k^2(u,v)}}{10\sqrt{\sum_i (w_i)^2}} \tag{13}$$

If $\alpha_k < \bar{\alpha}$ , Revise DCT coefficient with $\alpha_k$ , otherwise revise DCT coefficient with $\bar{\alpha}$

## 4. Watermark Embedding and Extraction

### 4.1. Algorithm of the Watermark Embedding

Suppose the size of the watermark image $W$ is $P \times Q$ . The size of the original image $I$ is $M \times N$ . The embedding procedure is as follows:

(1) Encrypt the watermark image $W$ based on the chaotic encryption algorithm; the watermark sequence which length is $P \times Q \times 8$ bytes will be obtained.

(2) The original image $I(M \times N)$ is divided into 8*8 sub-blocks, each sub-block is denoted as $f_m(x, y), x = 0,1,2...7,\ y = 0,1,2...7$ , k=0, 1. . . $\frac{M \times N}{8 \times 8} - 1$ , DCT transform is performed on each sub-blocks, the result is $F_k(u,v)$ , $u = 0,1,2...7, v = 0,1,2...7$ .

(3) According to formula (7 and formula (8) calculate the mean value and variance of the gray image. Get the DC coefficient ( $F_k(0,0)$ ) of the each sub-block. Calculate $FI_k$ of the sub-block according to $FI_k = F_k(0,0) + \sigma_k$ . The value reflects the comprehensive illumination characteristics and texture characteristics of each sub-block.

(4) Sort $FI_k$ of the all sub-blocks. Select the $l$ sub-blocks that their $FI_k$ values are the biggest. Where $l$ is number of the sub-blocks. Then, sort the intermediate frequency coefficient of each selected sub-blocks, Select the first $q$ biggest intermediate frequency coefficients, where $q$ is number of intermediate frequency which will be modified.

(5) Calculated threshold $\bar{\alpha}$ and the embedding strength $\alpha_k$ . The watermark embedding formula is described as follows: $F_k'(u,v) = F_k(u,v) + \alpha_k w_i$ ; If $\alpha_k < \bar{\alpha}$ , revise DCT coefficient with $\alpha_k$ , otherwise revise DCT coefficient with $\bar{\alpha}$ .

(6) Using IDCT transform to $F_k(u,v)$ , the watermarked image will be abstained.

### 4.2. Algorithm of the Watermark Extraction

The watermark extraction process is the inverse process of watermark embedding. The specific steps are as follows:

(1) The original image and watermarked image are divided into the $8 \times 8$ sub-blocks, and DCT transform is performed on each block. Suppose their Coefficients are respective $F_k(u,v)$ and $F_k'(u,v)$ after DCT transformation

(2) Sort $FI_k$ of the all sub-blocks, Select the $l$ sub-blocks that their $FI_k$ value are the biggest.

(3) Sort the intermediate frequency coefficients of each selected sub-blocks; select the first $q$ biggest intermediate frequency coefficient. Use the inverse process of watermark embedding formula. Watermark ( $W_k''$ ) sequences are got. The method is as follows:

$$W_k' = \frac{F_k'(u,v) - F_k(u,v)}{\alpha_k} \tag{14}$$

$$W_k'' = \begin{cases} 1, \left| W_k' - \lfloor W_k^i \rfloor \right| > 0.5 \\ 0, \left| W_k' - \lfloor W_k^i \rfloor \right| < 0.5 \end{cases} \tag{15}$$

(4) Decrypt the one-dimensional watermark sequence; we can get the watermark image sequence.

(5) The watermark sequences reformulate 2D watermarking matrix. The watermark image can be obtained immediately.

## 5. Experimental Result

The gray image Lena ( $512 \times 512$ ) is used as the original image (Fig. 3(a)). As shown Figure 3(b) is the watermark image ( $32 \times 32$ ), the simulation experiments are tested on the platform of Matlab7.0.

**Fig. 3.** Original image and Watermark image.

As shown in Fig. 4(a) is the encrypted watermark image. As shown Fig. 4(b) is the effect of original image embedded by watermark. As shown Fig. 4(c) is extracted watermark from Fig. 4(b). The peak signal-to-noise ratio ( *PSNR* ) value is 40.25. Obviously, the algorithm ensures the invisibility of watermark embedding.

(a) Encrypted watermark (b) Host image (c) Extract watermark

**Fig. 4.**Watermark embedded and extracted image.

In order to test the robustness of the algorithm, the watermarked image is attacked by added noise, filtered and JPEG compression respectively. The experimental results are as shown in Table 1:

**Table 1.**Test result of some common attacks

| No. | Attack type | PSNR/dB | NC |
|---|---|---|---|
| 1. | No attack | 40.25 | 1.0 |
| 2. | Salt & pepper noise (0.01) | 24.23 | 0.9035 |
| 3. | Gaussian noise (0.01) | 20.63 | 0.9476 |
| 4. | Gaussian low pass filter | 36.53 | 0.9635 |
| 5. | Median filter (3×3) | 30.33 | 0.8248 |
| 6. | JPEG compression (90 %) | 36.82 | 0.9883 |
| 7. | JPEG compression (80 %) | 34.62 | 0.9801 |
| 8. | JPEG compression (70 %) | 33.37 | 0.9712 |
| 9. | JPEG compression (60 %) | 32.40 | 0.9402 |
| 10. | JPEG compression (50 %) | 31.69 | 0.9204 |

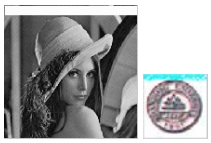
The Table 1 shows that the algorithm is robust against the attacks of general image processing methods such as noise; filtering and JPEG compression. The algorithm in this paper is applied to Peppers, Boat, Balloon, three gray images (512×512) again. after they are suffered from various image attacks, the watermark information is respectively extracted from them. Table 2 gives the correlation coefficient NC.

**Table 2.** Test results of different original image.

| No. | Attack type | Peppers (NC) | Boat (NC) | Baloon (NC) |
|---|---|---|---|---|
| 1. | No attack | 1.0 | 1.0 | 1.0 |
| 2. | Salt & pepper noise (0.01) | 0.8559 | 0.8597 | 0.8587 |
| 3. | Gaussian noise (0.01) | 0.9348 | 0.9367 | 0.9513 |
| 4. | Gaussian low pass filter | 0.9705 | 0.9541 | 0.9642 |
| 5. | Median filter(3×3) | 0.8611 | 0.8309 | 0.8485 |
| 6. | JPEG compression (90 %) | 0.9864 | 0.9813 | 0.9891 |
| 7. | JPEG compression (80 %) | 0.9752 | 0.9810 | 0.9834 |
| 8. | JPEG compression (70 %) | 0.9703 | 0.9638 | 0.9719 |
| 9. | JPEG compression (60 %) | 0.9337 | 0.9315 | 0.9406 |
| 10. | JPEG compression (50 %) | 0.9305 | 0.9286 | 0.9304 |

In order to test algorithm's character of against geometric attack, this paper make a Scaling, cropping and rotation test to the watermarked image. The test results are shown in Fig. 5: The NC and PNSR values are shown in Table 3:

(a) Scale (0.5,2) and extracting watermark.



(b) Cropping attract and extracting watermark.

(c) Rotation 23 angle and extracting watermark.

**Fig. 5.** Geometric attack test.

**Table 3.** Test result on Geometric attack.

| No. | Geometric distortion | PSNR/dB | NC |
|---|---|---|---|
| 1. | Scale (0.5,2) | 25.67 | 0.9298 |
| 2. | Cropping | 29.53 | 0.9593 |
| 3. | Rotation 23 angle | 27.52 | 0.9047 |

## 6. Conclusions

In analyzing the foundation of the characteristic of the Chaos system, the watermark image is encrypted through Logistic mapping to improve the security of the watermark, and then encrypted watermark information is embedded into the sub-blocks DCT medium frequency coefficients Based on the feature of human visual system and image texture. The advantage of this algorithm is simple and easy. Experiments show this algorithm can achieve the desired effect.

## References

[1]. Xuehua Jiang, Digital Watermarking and its Application in Image Copyright Protection, in *Proceedings of the Conference on ' Intelligent Computation Technology and Automation (ICICTA'2010)'*, Changsha, China, 11-12, May, 2010, pp. 114-117.

[2]. Pei-Yu Lin, Jung-San Lee, Chin-Chen Chang, Dual Digital Watermarking for Internet Media Based on

Hybrid, *Circuits and Systems for Video Technology*, Vol. 19, Issue 8, 2009, pp. 1169-1177.
[3]. Geng-Ming Zhu Shao-Bo, Zhang, Research and Implementation of DCT-Based Image Digital Watermarking Algorithm, in *Proceedings of the Conference on Electronic Commerce and Security (ISECS' 2009)*, Nanchang, China, 22-24, May 2009, pp. 195-198.
[4]. Zhi-Yong Meng, Ping-Ping Yu, Guo-Qing Yu, Copyright protection for digital image based on joint DWT-DCT transformation, in *Proceedings of the Conference on Wavelet Analysis and Pattern Recognition (ICWAPR' 2012)*, Xian, China, 15-17 July, 2012, pp. 11-14.
[5]. Zhao Song, Li Hengjian, Yan Xu, A new chaotic algorithm for image encryption, in *Proceedings of the Conference on Young Computer Scientists (ICYCS'2008)*, Zhang Jia Jie, Hunan, China, 18-21, November, 2008, pp. 889-892.
[6]. Zhang Yunpeng, Zuo Fei, Zhai Zhengjun, Cai Xiaobin, A New Image Encryption Algorithm Based on Multiple Chaos System, in *Proceedings of the Conference on Electronic Commerce and Security (ISECS' 2008)*, Guangzhou, China, 3-5, August, 2008, pp. 347-350.
[7]. Zheng, Jiangyong, Dong Hongling, Jiang Zengliang, Milo Jin, A DCT-BASED Digital Watermarking Algorithm for Image, in *Proceedings of the Conference on Industrial Control and Electronics Engineering, (ICICEE' 2012)*, Xian, China, 23-25, August 2012, pp. 1217-1220.
[8]. Xiao-Li Zhang, Xin Lv, A Novel Watermarking Algorithm Resist to Geometrical Attacks, in *Proceedings of the Conference on Electronic Commerce and Business Intelligence, (ECBI' 2009)*, Beijing, China, 6-7, September, 2009, pp. 503-506.
[9]. Lin Yu-Tzu-T, Huang C.-Y, Lee Greg C. Rotation, Scaling and Translation Resilient Watermarking for Images, *Image Processing*, Vol. 5, Issue 4, 2010, pp. 328-340.
[10]. Yin Thu Win, Nitin Afzulpurkar, Chumnarn Punyasai, Hla Thar Htun. Ultrasonic System Approach to Obstacle Detection and Edge Detection, *Sensors & Transducers*, Vol. 127, Issue 4, 2011, pp. 56-68.

---