

Robust Watermarking for Text Images Based on Arnold Scrambling and DWT-DCT

Fan Wu

College of Information Science and Technology
Hainan University
Haikou, China
958889067@qq.com

Jingbing Li*

College of Information Science and Technology
Hainan University
Haikou, China
Jingbingli2008@hotmail.com

Mengxing Huang

College of Information Science and Technology
Hainan University
Haikou, China
huangmx09@163.com

Abstract—With the popularization of Internet and the development at full speed of the multi-media technology, the copyright protection of digital works has already become the hot issue at present. The paper proposes a blind watermarking algorithm for text images' authentication and protection based on DWT-DCT. Firstly, the text image is decomposed into a low frequency, horizontal, vertical and diagonal four components through DWT transformation, then the low frequency component is made the whole DCT transform to get rid of coefficient correlation in order to obtain the visual feature vectors. Based on the studies of the document digital watermarking methods and techniques, this dissertation presents that the problems of existed documents watermarking algorithms can be solved by Arnold Scrambling and DCT technique. The experimental results show that the scheme has strong robustness against common attacks and geometric attacks.

Keywords—Arnold scrambling; Digital Watermarking; DWT; DCT; Zero-watermarking; Text image.

I. INTRODUCTION

With the rapid development of computer science and technology, and multimedia communication technology, digital media is becoming more and more universal. Digital watermarking is an important method for protecting digital media copyright. Most work focuses on audio, video, grayscale, and color images. However, binary images are very useful for security records, insurance information, financial document, fax images, case history, contract, e-business, e-Government, etc. Therefore, it may be very useful to embed and extract watermarking in binary images.

Currently the digital watermarking technique is applied in the transform domain more popular than applied in the spatial domain [2]. DCT is widely used among the transform domain, and DWT based techniques have also been popular applied because of its excellent spatial localization and multi-resolution properties.

In this paper, we have proposed a DWT -DCT based blind watermarking algorithm for copyright protection. The

combination of the two transforms improves the watermarking performance compared to the DWT or DCT only watermarking approach. In addition, the watermarking is scrambled and embedded in a spread spectrum pattern so as to enhance the security and robustness further. Experiment evaluation results show that the proposed algorithm has strong ability in resisting common attacks and geometric attacks.

II. THE FUNDAMENTAL THEORY

A. The Discrete Wavelet Transform

The wavelet transform, proposed by S. Mallat in 1988 firstly, is a new signal analysis theory and a "time-frequency" method. The basic idea is to decompose the signal $f(t)$ based on wavelet function, $\psi_{a,b}(t)$.

$$W_{f(a,b)} = \int_{\mathbb{R}} f(t) \overline{\psi_{a,b}(t)} dt \quad (1)$$

Where, wavelet function $\psi_{a,b}(t)$ is a set of functions which are obtained by translating and stretching of the same base function, $\psi_{a,b}(t)$.

$$\psi_{a,b}(t) = |a|^{-1/2} \psi((t-b)/a) \quad a, b \in \mathbb{R}, a \neq 0 \quad (2)$$

Where, ψ is the basic wavelet, a and b are the dilation factor and the translation factor, respectively. The decomposing equation of Mallat algorithm is defined as follows:

$$c_{j+1,k} = \sum_{n \in \mathbb{Z}} c_{j,n} \overline{h_{n-2k}} \quad k \in \mathbb{R} \quad (3)$$

$$d_{j+1,k} = \sum_{n \in \mathbb{Z}} c_{j,n} \overline{g_{n-2k}} \quad k \in \mathbb{Z} \quad (4)$$

The reconstruction equation of the Mallat algorithm is given by:

$$c_{j,k} = \sum_{n \in \mathbb{Z}} c_{j+1,n} h_{k-2n} + \sum_{n \in \mathbb{Z}} d_{j+1,n} g_{k-2n} \quad k \in \mathbb{Z} \quad (5)$$

By the one-layer wavelet decomposition of the original image, four subband images can be acquired. Where, LL1 is the approximated subband image with low frequency

characteristics that are robust to attacks. The others (LH1, HL1, and HH1) with high frequency characteristics are easily affected by attacks. Therefore, embedding the watermarking into the low frequency subgraph can provide better robustness.

B. The Discrete Cosine Transform

DCT transform is compatible with international data compression standard (JPEG, MPEG) and is widely used. It is well known for the best balance between operation speed and high precision of extracting the feature vector [3]. The $M \times N$ text image's DCT transform is defined by:

$$F(u,v) = c(u)c(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos \frac{\pi(2x+1)u}{2M} \cos \frac{\pi(2y+1)v}{2N} \quad (6)$$

$$u = 0, 1, \dots, M-1; v = 0, 1, \dots, N-1$$

$$c(u) = \begin{cases} \sqrt{1/M} & u=0 \\ \sqrt{2/M} & u=1, 2, \dots, M-1 \end{cases} \quad c(v) = \begin{cases} \sqrt{1/N} & v=0 \\ \sqrt{2/N} & v=1, 2, \dots, N-1 \end{cases}$$

Where x, y is sampled value in the spatial domain sampling; u, v is the frequency domain sampling. Usually digital image is expressed by pixels square, namely $M=N$.

C. Arnold scrambling Transform (AT)

Scrambling transformation as a means of encrypted technology is applied in the pretreatment stage of the watermarking, after scrambling transformation, one meaningful watermarking will become a meaningless, chaotic image. If you do not know the scrambling algorithm and keys, an attacker even got the embedded watermark can't restore it. And thus plays a role of secondary encryption. Additionally, after scrambling transformation, it will upset the relationship between the space locations of pixels and make it evenly distributed in all space of the carrier image. This will improve the robustness of the algorithm. Two-dimensional Arnold scrambling transformation is defined as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad x, y \in \{0, 1, 2, \dots, N-1\} \quad (7)$$

Wherein, x, y is the pixel coordinates of the original space; x', y' is the pixel coordinates after iterative computation

scrambling, N is the size of the rectangular image, also referred to as a step number.

By the above formula the corresponding inverse transform formula can be obtained:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} + \begin{bmatrix} N \\ N \end{bmatrix} \pmod{N} \quad x', y' \in \{0, 1, 2, \dots, N-1\} \quad (8)$$

It is easy to restore the original initial state according to the corresponding iterations. Arnold transformation is cyclical, when iterate to a step, will regain original image. So if you do not know cycle and iterations, you will not be able to restore the image. Therefore, cycle and iterations can exist as a private key. Meanwhile, different image, because the desired effect is different, iterations should also be changed according to your need.

D. A method to obtain the feature vector of text image

Feature extraction means to obtain the feature vector which is used to describe the image content. In literature the common characteristics are usually the following types: gray feature, Shape and location [4], texture features [5] and semantic features.

Firstly, DWT is applied on the original text image to obtain the approximated subband LL1. Then, DCT of the whole LL1 is computed and the DCT coefficient matrix is acquired. We choose 5 low-frequency DWT-DCT coefficients (F(1,1), F(1,2), ,, F(1,5)) for formation of the feature vector, shown in Table I. We find that the value of the low-frequent coefficients may change after the image has undergone an attack, particularly geometric attacks. However, the signs of the coefficients remain unchanged even with strong geometric attacks, as also shown in Table I. Let "1" represents a positive or zero coefficient, and "0" represents a negative coefficient, and then we can obtain the sign sequence of low-frequency coefficients, as shown in the column "Sequence of coefficient signs" in Table I. After attacks, the sign sequence is unchanged, and the normalized cross-correlation (NC) is equal to 1.0.

This means that the signs of the sequence can be regarded as the feature vector of the text image. Furthermore, it proves that the sequence of the DWT-DCT coefficient signs can reflect the main visual characteristics of text images.

TABLE I. CHANGE OF DWT-DCT LOW-FREQUENCY COEFFICIENTS WITH RESPECT TO DIFFERENT ATTACKS.

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14
Image processing	PSNR	F(1,1)	F(1,2)	F(1,3)	F(1,4)	F(1,5)	F(1,6)	F(1,7)	F(1,8)	F(1,9)	F(1,10)	Sequence of coefficient signs	NC
Original image		4.919	-0.025	-0.035	-0.028	-0.123	0.060	-0.190	0.081	-0.248	0.167	1000010101	1.0
Gaussian noise (4%)	13.02dB	4.500	-0.008	-0.031	-0.013	-0.093	0.043	-0.144	0.059	-0.193	0.126	1000010101	1.0
JPEG compression (5%)	17.71dB	4.764	-0.041	0.015	-0.038	-0.087	0.057	-0.164	0.083	-0.239	0.179	1010010101	0.90
Median filter [3×3]	8.535dB	5.775	0.051	-0.307	0.043	-0.312	0.082	-0.303	0.050	-0.288	0.050	1101010101	0.80
Cropping(2%) (fromY direction)	5.439dB	4.895	-0.026	-0.033	-0.028	-0.122	0.059	-0.188	0.081	-0.247	0.166	1000010101	1.0
Rotation (1.5°)	5.598dB	4.737	-0.047	-0.345	-0.039	-0.307	0.022	-0.292	0.024	-0.259	0.052	1000010101	1.0
Scaling(×0.5)		2.442	-0.015	-0.012	-0.015	-0.057	0.029	-0.092	0.040	-0.122	0.085	1000010101	1.0

DCT transform coefficient unit 1.0e+004

III. THE ALGORITHM

Use a meaningful binary image as the watermarking, Represented by W , F represents the original text image, The $W = \{ w(i,j) \mid w(i,j) = 0,1; 1 \leq i \leq M1, 1 \leq j \leq M2 \}$ as digital watermarking, At the same time, we select a paragraph in an article as the original text image. It is describe as: $F = \{ f(i,j) \mid f(i,j) \in R; 1 \leq i \leq N1, 1 \leq j \leq N2 \}$, where $w(i,j)$ and $f(i,j)$ denote the pixel gray values of the watermarking and the original text image, Let $M1 = M2 = M, N1 = N2 = N$.

A. The algorithm of the embedded watermarking.

Step1 the binary watermarking image is scrambled by Arnold scrambling transform, $BW(i,j)$.

$$BW(i,j) = AT(W(i,j)) \quad (9)$$

Step2 L-level decomposition of the wavelet transform to the original text image and obtaining the approximation subgraph FA_L .

The original text image after L level wavelet decomposition, Can get more details sub-graph coefficient $FD_j^k, (k=1,2,3; j=1,2,3 \dots L)$ and an approximation sub-graph coefficient FA_L . Wavelet decomposition level $L \leq \text{floor}(\log(N/M))$, if L level wavelet decomposition series is high, the wavelet coefficient resistance to gaussian, JPEG compression and conventional attack ability will become strong, but wavelet decomposition and the reconstructed time corresponding lengthened. Here take $L = 1$.

$$FA(i,j) = DWT2(F(i,j)) \quad (10)$$

Step3 Full figure DCT transformation on approximation subgraph FA_L , get text image visual feature vector $V(j)$.

Firstly, DCT of the whole approximated subband $LL1, FA_L(i,j)$, is computed and the DCT coefficient matrix, $FF(i,j)$, is acquired. Then, Zig - Zag sort to $FF(i,j)$. Next, the frequency sequence $Y(j)$, from low to high frequency, can be obtained. Finally, the feature vector $V(j)$, $V = \{v(j) \mid v(j) = 0.1; 1 \leq j \leq J\}$ is achieved as the signs sequence of the low-frequency DWT-DCT coefficients, where the value of J can tune the robustness and capability of the embedded watermarking.

$$FF(i,j) = DCT2(FA_L(i,j)) \quad (11)$$

$$Y(j) = \text{Zig} - \text{Zag}(FF(i,j)) \quad (12)$$

$$V(j) = -\text{Sign}(Y(j)) \quad (13)$$

Step4 Use HASH function properties and visual feature vector, Acquire the key sequence.

$$\text{Key}(i,j) = V(j) \oplus BW(i,j) \quad (14)$$

$\text{Key}(i,j)$ is by the image visual feature vector and the embed watermarking $BW(i,j)$, generated by the HASH function of cryptography. $\text{Key}(i,j)$ is used to extract the watermarking, Furthermore, $\text{Key}(i,j)$ can be regarded as a secret key and

registered to the third part to preserve the ownership of the original text image, so as to achieve the purpose of the protection of text images.

C. The algorithm of the extracted watermarking.

Step1 Get the approximation sub-graph of the being tested image by the wavelet transform.

Let the being tested image for Test_F '(i, j), abbreviated as $T_F'(i,j)$, L-level decomposition of the wavelet transform to the being tested image and obtaining the approximation sub-graph $T_FA_L'(i,j)$.

$$FA'(i,j) = DWT2(F'(i,j)) \quad (15)$$

Step2 Full figure DCT transformation on approximation sub-graph $T_FA_L'(i,j)$. get text image visual feature vector $T_V'(j)$.

$$FF'(i,j) = DCT2(FA_L'(i,j)) \quad (16)$$

$$Y'(j) = \text{Zig} - \text{Zag}(FF'(i,j)) \quad (17)$$

$$T_V'(j) = -\text{Sign}(Y'(j)) \quad (18)$$

Step3 Extracting the watermarking $BW'(i,j)$.

According to the key which generated in the embedded watermarking and the visual feature vector $T_V'(j)$ of the being tested image, use HASH function properties to extract the watermarking $BW'(i,j)$. Extracting watermarking doesn't need original image, so it can protect the original image better.

$$BW'(i,j) = \text{Key}(i,j) \oplus T_V'(j) \quad (19)$$

Step4 Using the Arnold scrambling inverse transform to restore the extracted watermarking $BW'(i,j)$, get the watermarking of the being tested image, $W'(i,j)$.

$$W'(i,j) = \text{IAT}(BW'(i,j)) \quad (20)$$

D. Detection algorithm of the watermarking.

Step1 By calculating NC (Normalized Cross-Correlation) to determine whether there is the existence of the watermarking. The larger the value of NC is, the more approximation between $W'(i,j)$ and $W(i,j)$. Defined as:

$$NC = \frac{\sum_i \sum_j W_{(i,j)} W'_{(i,j)}}{\sum_i \sum_j W_{(i,j)}^2} \quad (21)$$

Where, $W(i,j)$ is the original watermarking, $W'(i,j)$ is the extracted watermarking.

Step2 Evaluation of the quality of the text image after Embed watermarking by calculating the peak signal-to-noise ratio PSNR (dB), we often use peak value signal-to-noise ratio PSNR (dB) to reflect the quality of signal, defined as:

$$PSNR = 10 \lg \left[\frac{MN \max_{i,j} (I_{(i,j)})^2}{\sum_i \sum_j (I_{(i,j)} - I'_{(i,j)})^2} \right] \quad (22)$$

where $I(i,j)$, $I'(i,j)$ denote the pixel gray values of the coordinates (i,j) in the original image and the watermarking, respectively; M , N represent the image row and column numbers of pixels, respectively.

IV. EXPERIMENTS

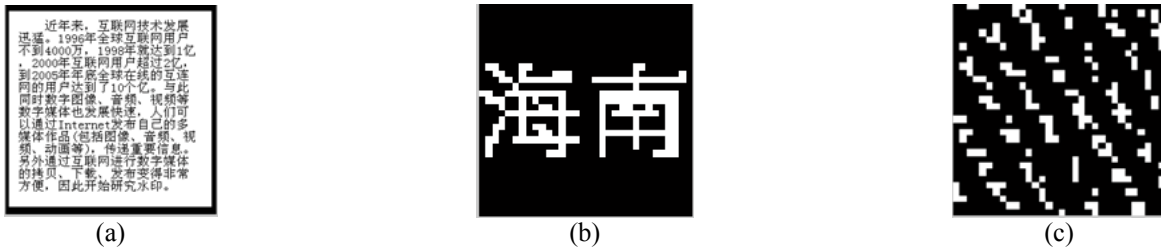


Figure 1. The watermarking is scrambled by Arnold scrambling transform. (a) The watermarked text image without attacks (b) the original binary watermarking. (c) the scrambled watermarking.

In order to investigate this approach of embedding watermarking robust performance, I chose the following verification:

A. Common attacks.

1) Adding Gaussian noise.

In the watermarked text image, Gaussian noise is added by the $imnoise()$ function with different noise level. The text image under the attack of Gaussian noise (10%) with PSNR=13.0Db. At this time, the watermarked text image has been very vague, as shown in Fig. 3(a). The watermarking can obviously be extracted with NC=1.0. As shown in Fig. 3(b). Table II shows the NC values between the extracted and embedded watermarking, and the PSNR of the attacked watermarked image.

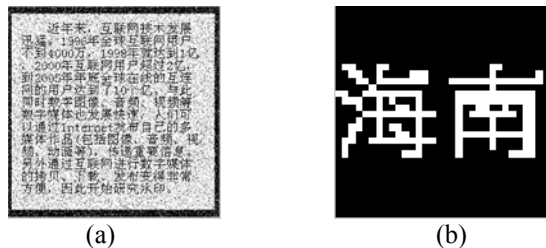


Figure 3. The watermarked text image under Gaussian noise attacks (10%). (a) the watermarked text image under noise attack. (b) the extracted watermarking

To verify the effectiveness of our proposed algorithm, we carried out the simulation in Matlab2010a platform. We choose a significant binary image as the original watermarking and select a paragraph in an article as the original text image. the original watermarking $W = \{w(i,j) \mid w(i,j)=0 \text{ or } 1; 1 \leq i \leq 32, 1 \leq j \leq 32\}$. the original text image $F = \{f(i,j), 1 \leq i \leq 128, 1 \leq j \leq 128\}$.

In the experiment, the parameter values: Arnold scrambling period is 24, and the number of transform times are 8, i.e. $T=24, n=8$.

It can be seen visually from Figure 1 that the quality of the text image embedded has hardly any change. The quality of extracted watermarking is of high-quality with no difference with the original in normal case (no attacking on watermarking).

TABLE II THE PSNR AND NC UNDER GAUSSIAN NOISE ATTACKS

Noise parameters (%)	10	20	30	40	50
PSNR(dB)	13.0	10.2	8.76	7.89	7.34
NC	1.00	0.88	0.86	0.75	0.72

2) JPEG attacks.

JPEG compression process is done by using the percentage of image quality as a parameter to measure. The watermarked text image with PSNR=17.71dB under JPEG attacks (10%) is shown in Fig4 (a). the watermarking can obviously be extracted with NC=0.93. As shown in Fig. 4(b). Table III shows the NC values between the extracted and embedded watermarking, and the PSNR of the attacked watermarked image.

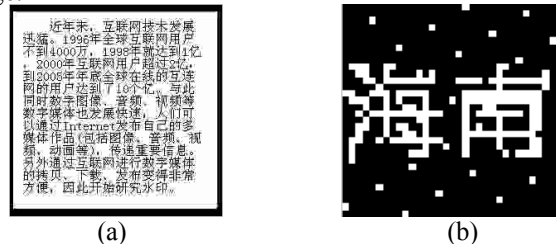


Figure 4. The watermarked text image under JPEG attacks (10%). (a) the watermarked text image under JPEG attacks. (b) the extracted watermarking..

TABLE III THE PSNR AND NC UNDER JPEG

Compression Quality (%)	10	15	20	25	30
PSNR(dB)	17.71	18.80	19.95	21.60	23.07
NC	0.93	0.91	0.91	0.91	1.00

B. Geometrical attacks.

1) Rotation attacks.

We investigate the effectiveness of our proposed watermarking algorithm against rotation angle as the parameter. The watermarked text image under rotation attacks (clockwise by 5°) with PSNR=6.31dB under rotation attacks is shown in Fig. 5(a). The watermarking can obviously be extracted with NC=0.76. As shown in Fig. 5(b). Table IV shows the NC values between the extracted and embedded watermarking, and the PSNR of the attacked watermarked image.



Figure 5. The watermarked text image under rotation attacks. (clockwise by 5°). (a) the watermarked text image under rotation attacks. (b) the extracted watermarking.

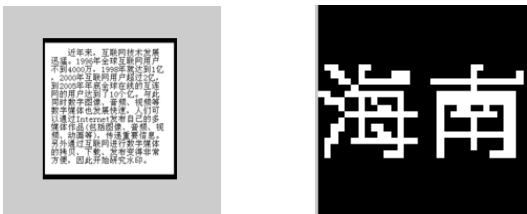
TABLE IV THE PSNR AND NC UNDER ROTATION ATTACKS

Rotation (clockwise)	5°	10°	15°	20°	25°
PSNR(dB)	6.319	5.598	5.239	5.026	4.853
NC	0.76	0.75	0.75	0.69	0.52

Can be seen the extracted watermarking is very similar to the original watermarking.

2) Scaling attacks.

We use the scaling factor as parameter to validate the effectiveness of our proposed algorithm on different scaling attacks. When the watermarked image is scaled 0.5 times, its pixel point has become a quarter of the original. The resolution has sent a lot of. Fig. 6(a) shows that the watermarked image shrunk with a scale factor of 0.5. Moreover, Fig. 6(b) shows that the watermarking can be extracted with NC=1.0. Table V shows the NC values between the extracted and embedded watermarking with scaling attacks on the watermarked image with multiple scale parameters.



(a) (b)

Figure 6. The watermarked text image under scaling attacks. (0.5 times). (a) the watermarked text image under scaling attacks. (b) the extracted watermarking.

TABLE V THE NC UNDER SCALING ATTACKS

Scaling factor	0.4	0.5	0.8	1.00	1.2	2.0
NC	0.72	1.00	0.83	0.92	1.00	1.0

V. CONCLUSION

Many watermarking algorithms exist for the frequency domain using either the DCT or the DWT. In this paper, we propose a new watermarking algorithm using the DWT prior to the DCT to provide better imperceptibility in harmony with the human visual system. Experiments show that its robustness is better than DWT or DCT algorithm alone after applying the same attacks. In addition, it can be used to improve the PSNR and enable to blind extraction.

ACKNOWLEDGEMENT

This work is supported by the National Natural Science Foundation of China (No:61263033) and the Institutions of Higher Learning Scientific Research Special Project of Hainan (Hnkyzx2014-2) and the International Science and Technology Cooperation project of Hainan (No: KJHZ2014-16) and the Key Science and Technology Project of Hainan (No: ZDXM20130078).

REFERENCES

- [1] Alar Kuusik, Enar Reilent, Ivor Loobas, Marko Parve, "Software Architecture for Modern Telehealth Care Systems", AISS, Vol. 3, No. 2, pp. 141 ~ 151, 2011.
- [2] Xueming Li, Guangjun He, "Efficient Audio Zero-Watermarking Algorithm for Copyright Protection Based on BIC and DWCM Matrix", IJACT, Vol. 4, No. 6, pp. 109 ~ 117, 2012.
- [3] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking," Journal of Computer Science 3(9):740-746, 2008
- [4] M. Unoki, R. Miyauchi, "Reversible Watermarking for Digital Audio Based on Cochlear Delay Characteristics," In Proceedings of the 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Oct. 2011, pp. 314-317.
- [5] B. S. Manjunath, "Gabor wavelet transform and application to problems in computer vision," in 26th Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, 1992, pp. 796-800.
- [6] Xia, X. G., Boncelet, C. G. and Arce, G.R., "A multiresolution watermark for digital images," Proc. Int. Conf. on Image Processing 97, Santa Barbara, CA, U. S. A. Vol. I, pp. 548-551, 1997.
- [7] Huang D, Yan H. "Interword distance changes represented by sine waves for watermarking text images," IEEE Trans. Syst. Video Technol., 11(12), pp.1237-1245, 2001.
- [8] Cox I, Kilian J, Leighton T, Shamoon T, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, 6(12), pp.1673-1687, 1997.
- [9] Hsieh, C. T., Lu, Y. L., Luo, C. P. and Kuo, F. J., "A study of enhancing the robustness of watermark," Proc. IEEE Int. Sym. on Multimedia Software Engineering, Taiwan, pp. 325-327, 2000.
- [10] Ester Yen and Li-Hsien Lin, "Rubik's cube watermark technology for grayscale images", Vol 37(6), pp 4033-4039, Jun. 2010.
- [11] GAO Xin-yu, LV Jian-ping. A block-based DCT algorithm of digital image watermarking. JOURNAL OF XI'AN UNIVERSITY OF POSTS AND TELECOMMUNICATIONS. Vol.12, No.5, Sep. 2007.