TELKOMNIKA, Vol.11, No.11, November 2013, pp. 6281~6289
e-ISSN: 2087-278X

A Novel Self-adaptive Discrete Wavelet Transform Digital Watermarking Algorithm

Chi Ma[1,2]*, Yongyong Zhu[3]
[1]College of Software, University of Science and Technology LiaoNing, Anshan, China
[2]Dongling School of Economics and Management, University of Science and Technology Beijing, Beijing, China
[3]Department of Economics and Business Administration, Chongqing University of Education, Chongqing, China
*Corresponding author, e-mail: asmachi@126.com

Abstract

On the basis of the research of wavelet transform and digital watermarking technology, this paper proposed a self-adaptive discrete wavelet transform (DWT) digital watermarking algorithm, which can achieve the purpose of embedding hidden watermarks by decompose three-level wavelet of image and decompose bit-plane of watermarking gray scale image by Arnold scrambling transformation. Layer adaptive threshold and quantizer were referenced in this algorithm, and which adaptive selected coefficient of detail subbands of embedded watermarking to improve the robustness of the watermarking. In testing of semi-blind watermarking, renewing of watermarking based on the embedding sequence of point locations and the quantizer sequence without participation of the original image. Experimental results show that the algorithm is effective to improve the robustness of the cut, adding noise, filtering, and compression image attack treatment.

Keywords: *digital watermarking, DWT, arnold scrambling, bit plan decomposition*

1. Introduction

With the digitization of information and the flourish of Internet, digital products have become greatly enriched and easy to spread, copyright protection and information security issues become more prominent. Due to the defects of traditional information security technology in digital products copyright protection exists, contributed to the development of digital watermarking technology. Digital watermarking technology hides the digital watermark in digital media, in order to provide copyright certificates for copyright owners in copyright disputes. As an effective means to resolve copyright issues of digital products has been widespread concern. Because of the proximity of the wavelet transform and human visual system’s characters, the watermarking technique based on wavelet transform to become a research hotspot [1, 2]. So far, the domestic and foreign scholars have proposed quite a lot of digital watermarking algorithm based on wavelet transform. Through the repeated embedding and use of Reference watermarking method, the reference [3] achieved a higher detection rate. However, due to the reference watermark adding greatly increasing the doping amount, thereby reducing the image quality. Through qualitative and quantitative analysis, the reference [4] proposed the wavelet transform domain image watermark embedding strategy and algorithm. The reference [5] realized watermark adaptive embedding and detection without the original image, the cost is embed the bit is not fixed, and the need to record the embedding position. According to the embedded watermark capacity and the local characteristics of the image, the reference [6] dynamically adjusted the quantization step size, and effectively enhanced the robustness of the algorithm.

On the basis of the research of wavelet transform and digital watermarking technology [7-13], this paper proposes aself-adaptive digital watermarking algorithm based on integer wavelet transformation domain. Algorithm achieved the pretreatment of the watermark information by using multi-scale wavelet transform technology, Arnold scrambling and bit plane decomposition technology, and the watermark has stronger concealment. Also in the algorithm referenced layer adaptive threshold and quantization factor, adaptive selected the coefficients of

Received March 29, 2013; Revised Jul 2, 2013; Accepted Jul 20, 2013

the details sub-band which embedded in watermark adaptively. In recovery detection, watermark recovery can be based on locations sequence of the embedding point and the quantization factor sequence [14-16] without the participation of the original image, and achieved semi-blind watermark detection. Experimental results show that the algorithm is effective to improve the robustness of the cut, adding noise, filtering, and compression image attack treatment

2. Pretreatment of the Digital Watermark

In order to raise the difficulty of being cracked and shear resistance, pretreatment is necessary before the digital watermarking embedding into the host image. In the paper, bit plane decomposition [8] and Arnold scrambling [9] are used in watermarking information pretreatment. Then the quantization algorithm is realized based on that the gray scale image is converted into binary image by Bit plane decomposition. The correlation of watermarking's pixel space can be cleared by Arnold scrambling, and then the watermarking images become meaningless and disorganized, so that the digital watermarking become more hidden.

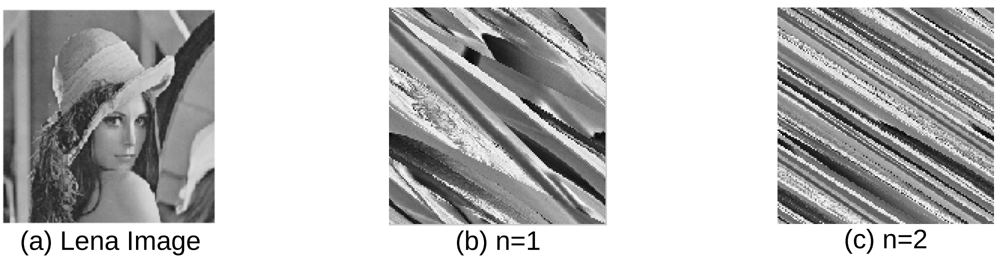
2.1. Arnold Scrambling

Image scrambling is an information encryption technology, and it is also a pretreatment process for information hiding. There are three purposes of scrambling watermark image: Avoiding the block effect, adding a key to ensure the security of watermarking, and enhancing the robustness of watermarking. Arnold transformation is a scrambling technology that commonly used in digital image, commonly known as cat face transformation, the layout of the gray value in the image can be changed by the change of the pixel coordinates. If the digital image is viewed as a matrix, then the image will become "a mess", but if continue to use Arnold transformation, there will be a same image with the original image. A new Arnold transformation for scrambling watermarking image is adopted here, the formulas of transform and inverse transform are.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}^{n} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{1}$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & k+1 \end{bmatrix}^{-n} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N \tag{2}$$

K and N constitute the pairs (K, N) in formula (1), and the pairs can be as the key of scrambling, we can use the common encryption algorithms (such as DES) to encrypt it. Only the person who masters the key can restore the extracted watermarking to the original information, so it enhanced the security of watermarking. In addition, the new cat transformation has many advantages: it is unnecessary to calculate the conversion cycle of restoring the image. If the original image is converted to a state after N steps, then the algorithm can restore the original image from the scrambling state by the same steps. Image can be restored to any times, and the efficiency of recovery is greatly improved compared with the cat transform, it also can save a lot of time. Figure1 is the Lena image scrambling.



(a) Lena Image (b) n=1 (c) n=2

Figure 1. Results of Arnold Scrambling Digital Image (n represents the number of iterations)

2.2. Bit Plane Decomposition

Image bit-plane is common in image coding and image compression. There are many kinds of representations for digital image, take grayscale images as an example, each pixel of digital image is constituted by the way of multi-bit, each pixel is usually 8 bits (i.e., 8 bits planes, each bit is 0 or 1). The meaning of the bit planes is that decomposing the grayscale value of pixel into binary value, then all the bits (0 or 1) with the same value formed the plane. For example, in an image which grayscale value is 256, each pixel represented by a single byte, the 8 binary bits are B7B6B5B4B3B2B1B0 arranged from high to low. In that way, the B0 bit of all the pixels constituting the 0 bit-plane, B0 bit constituting the 1 bit-plane and so on. As is shown in Figure1, the image should contain 8 bit planes..

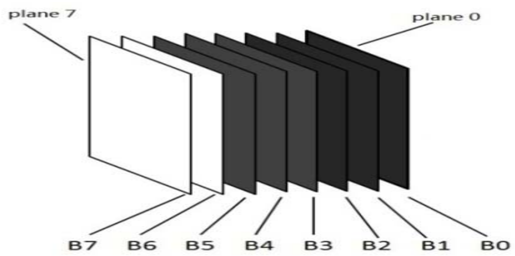


Figure 2. Schematic Diagram of Bit Plane Decomposition

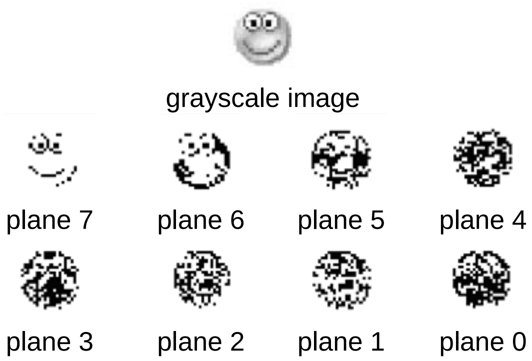


Figure 3. Watermark Image Each Bit-plane after Decomposition

The embedded watermark image is 32×32 grayscale image in this paper. In order to achieve the goal of quantifying the wavelet coefficients of host image through watermark value of 0 and 1 in the embedded algorithm, the grayscale watermark image bit-plane is partitioned into eight binary images, as shown in Figure 3.

3.Watermark Embedding and Extraction Algorithm Description

3.1. Watermark Embedding Algorithm

Let the host image be a $M \times N$ gray scale image, and watermark image be a $m \times n$ gray scale image. This method achieves the purpose of embedding a watermark by quantifying the high-frequency coefficients, and the specific steps are as follows.

1) Achieve three-level wavelet decomposition of the original host image. Let be the L-th layer decomposition of the high-frequency component, $k = h, v, d$ denote horizontal, vertical, diagonal direction component respectively. Conduct one-dimensional scan of the details of sub-band coefficients from the three directions, respectively, from high scale level to low scale level, and generate three one-dimensional sequences of HL, LH, and HH.

2) First conduct Arnold scrambling, generate a two-dimensional watermark image after hashing gray watermark image in order to improve the watermark invisibility. Then conduct bit-plane decomposition, from high level to low level, scan bit-planes at once, thus forming one-dimensional sequence of 0 and 1.

3) According to the characteristics of wavelet coefficients, small low-scale level quantization factor and less segmentation; high-scale level quantization with big factor and more segmentation to generate quantified factor sequence. $Q_1 = 2$, $Q_2 = 3$, $Q_3 = 4$ are the specific values of the three layers. When detecting, due to the small step-size, the change in quantization is not significant and tends to cause deviations, so it is of need to set the threshold value of the step-sizes. Specific step-sizes are: level 1: $step1 = 3.5$; level 2: $step2 = 3.5$; level 3: $step3 = 5$. Generate a threshold value sequence THR with the same step-size as H, V, and D, corresponding to the different levels of the step-size threshold. To reflect the priority principle of important coefficient, it is suggested to try to select a quantitative and meaningful coefficient. Thus, the level embedded threshold value is adaptively set. Decide the threshold value of different levels according to the level in which embedded coefficient is, and the values are as follows respectively:

First level: $thr\_o1 = 2^{|\log_2 C_{xo}|-2}$,

C_{xo}: the maximum in direction o, $thr1 = \min(thr\_h1, thr\_v1, thr\_d1)$;

Second level: $thr\_o2 = 2^{|\log_2 C_{xo}|-2}$,

C_{xo}: the maximum in direction o, $thr2 = \min(thr\_h2, thr\_v2, thr\_d2)$;

Third level: $thr\_o3 = 2^{|\log_2 C_{xo}|-2}$,

C_{xo}: the maximum in direction o, $thr3 = \min(thr\_h3, thr\_v3, thr\_d3)$;

After generating all the threshold values of all level, a coefficient threshold value sequence THR is formed with the length of H, V, and D.

4) All the threshold values are set, in every level, given any (m,n), sort $f_{h,l}(m,n)$, $f_{v,l}(m,n)$, $f_{d,l}(m,n)$ from small to big, $f_{k1,l}(m,n) < f_{k2,l}(m,n) < f_{k3,l}(m,n)$. Compute the value of step-size $\Delta = \dfrac{f_{k3,l}(m,n) - f_{k1,l}(m,n)}{2Q-1}$, and compare Δ with step, if Δ is bigger than step, then go on, or else skip to next point.

5) The specific method for quantizing the middle point is depicted as Figure 4

Partition the distance of $f_{k3,l}(m,n) - f_{k1,l}(m,n)$, the number of intervals is $2Q-1$, and the size of interval is Δ, the coordinate of interval point is $L(j)$, $(j \in [0, 2Q-1])$. Compute the location of $f_{k2,l}(m,n)$, and determine the quantization value of $f_{k2,l}(m,n)$ according to the watermark value.

$$f_{k2,l}(m,n) \in [L(2i), L(2i+1)], (i \in [0, Q]$$

$$f_{k2,l}(m,n) = \begin{cases} L(2i), wm = 0 \\ L(2i+1), wm = 1 \end{cases}$$

In order to extract watermark, store the quantization factor Q of embed point and its location into sequence EQ and IND respectively.

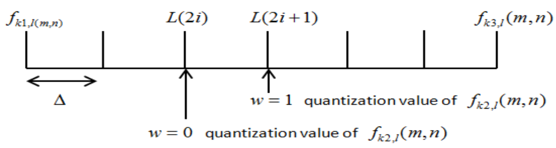


Figure 4. Schematic Diagram of Quantization Process

3.2. Watermark Extraction Algorithm

The algorithm strictly limits the step-size threshold value, coefficient threshold value, and quantization factor in watermark embed algorithm, with the aim to improve the accuracy of the extraction process. Due to limitations of the embedded watermark, the extraction accuracy of this algorithm improves a lot compared with the Kundur algorithm. In addition, this extraction algorithm need only be embedded the location sequence IND and quantized sequence EQ [7], without using the original images.

1) Achieve three-level wavelet decomposition of the detected image, and get the high-frequency components in horizontal, vertical, diagonal direction as embedded algorithm.

2) Conduct an opposite algorithm of embedded watermark to extract embedded watermark. Find the embedded location according to the embedded location sequence IND, sort $f_{h,l}(m,n)$, $f_{v,l}(m,n)$, $f_{d,l}(m,n)$ of this point,then get $f'_{k1,l}(m,n) < f'_{k2,l}(m,n) < f'_{k3,l}(m,n)$.

3) Just as the method when embedding,partition the distance of $f'_{k3,l}(m,n) - f'_{k1,l}(m,n)$, with the interval number of $2Q-1$, and the interval size of $\Delta' = \frac{f'_{k3,l}(m,n) - f'_{k1,l}(m,n)}{2Q-1}$.

4) Find the approximation interval point of $f'_{k2,l}(m,n)$, $ED = round(\frac{f'_{k2,l}(m,n) - f'_{k1,l}(m,n)}{\Delta'})$

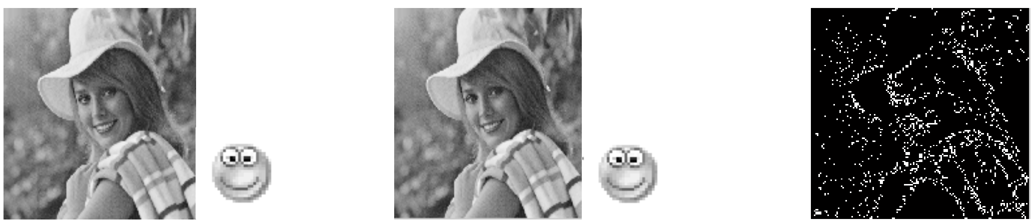
. 5) If ED is even, extract the watermark of this point as 0, or else as 1.

6) Divide the one-dimensional watermark sequence of wm' into eight bit-planes according to $m \times n$ .Then transform this into gray value, recover as $m \times n$ grayscale watermark image.

4. Experimental Results and Analysis

The basic configuration of the computer in experiment is CPU core (TM) 2 Duo/2.5G, memory of 4G, hard disk of 360G. The operating system is Windows 7, and the algorithm is implemented using simulation software Matlab 7. The original host image in experiment is 512×512 grayscale image, and the watermark image is 32×32 grayscale image. Achieve wavelet decomposition on host image and watermark image using db2 wavelet basis. During Arnold hashing processing, take N as 32, K as 1.

Embedding and extracting watermark in the case of normal situation without attack (shown in Figure 3), the experimental result shows that the embedded watermark image is still intact, and the watermark extracted from embedded image is also basically consistent with the original watermark image. From figure (e) we can see the differences between the images before and after the watermark embedding. This figure magnifies the differences of the two images 10 times, depicting the edge, contour outline after embedding watermark into host image using the algorithm, which is in line with human visual system, and could achieve good concealing effect.



a) Original Image and Watermark Image

(b) After Embedding Watermark and Extracting Watermark

(c) The Two Graphs Difference Embedded Watermark before and after NC=0.9994, PSNR=45.3339db

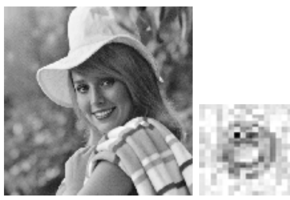
Figure 3. Embedding and Extracting Watermark in the Case of Normal Situation without Attack

(a) White noise processed image (b) Salt and pepper noise processed image
Extracting watermarkand extracting watermark
NC=0.9136, PSNR=39.9466dbNC=0.8620, PSNR=22.3234db

(c) Gaussian filter 3×3 processed image (d) Gaussian filter 5×5 processed image and
extracting watermarkand extracting watermark
NC=0.8626, PSNR=42.5358dbNC=0.8056, PSNR=40.9115db

(e) Median filter processed image (f) Enhance contrast processed image and
extracting watermarkand extracting watermark
NC=0.8376, PSNR=37.1387dbNC=0.9587, PSNR=5.2574db

(g) Cut 1/16 processed image (h) Cut 1/4 processed image and extracting
watermarkextracting watermark
NC=0.9977, PSNR=16.0768dbNC=0.9565, PSNR=10.0637db



(i) Reduced to 1/4 processed image and extracting watermark
NC=0.8759, PSNR=30.2676db

Figure 4. Result of Watermarked Image after Adding All Kinds of Attacks

In order to test the robustness of the algorithm, attack such as noise, filtering, cropping is added into the watermark image. Figure 4 shows the values of PSNR and NC detected after adding all kinds of attacks, and the experimental results demonstrate the strong robustness of the algorithm. Figure 5 shows the Watermark extraction image under different JPEG compression ratio. Figure 6 and Figure 7 show the values of PSNR and NC after JPEG compression attack.

Since this paper first converts grayscale watermark image to a binary sequence, thus it is considerable to further test the extraction effect by calculating the bit error ratio of watermark extraction. Define the bit error ratio (BER) of original watermark wm and the extracted watermark wm' as follows, in which N_w denote watermark sequence length.

$$EBR = \frac{\sum_{i=1}^{N_w} wm(i) \oplus wm'(i)}{N_w} \tag{3}$$

Q=100 Q=90 Q=80 Q=70 Q=60 Q=50 Q=40

Figure 5. Watermark Extraction Image under Different JPEG Compression Ratio
(Q represents the compression ratio)

Table 1 depicts comparison of the extracted watermark bit error ratio of the proposed algorithm and Kunder algorithm after various attacks. It can be seen that the extracted watermark image obtained by the proposed algorithm is closer to the original watermark image than the Kunder algorithm, and with a smaller bit error ratio and a stronger anti-attack capability.

Figure 8 shows the comparison image of extracted watermark bit error ratio of the proposed algorithm and Kunder algorithm after JPEG compression. It shows that there is a significant improvement in the robustness of the proposed algorithm for JPEG compression attack.

4. Conclusion

The proposed algorithm is an improvement of Kundur quantization algorithm. The Kundur algorithm first adaptively selects digital image discrete three level wavelet coefficients, and quantifies corresponding detailed sub-band coefficient according to the watermark value. Due to elaborative selection of quantization interval and embedded location of watermark, the recovery effect of digital watermark is good, and makes the detecting results more intuitive. In addition, it is only of need to embed quantization sequence into the embedded sequence to recover watermark without participation of original image, thus is a kind of semi-blind watermarking. Experimental results show that the algorithm is robust to attack operations such as noise, cut and compression.

Table 1. Comparison of the Extracted Watermark BER of the proposed Algorithm and Kunder Algorithm after Various Attacks

Attacks	proposed algorithm	Kunder algorithm
No Attack	0.0001	0.0000
White Noise	0.1023	0.1102
Salt and pepper noise	0.0745	0.0873
Gaussian filter3×3	0.1769	0.1760
Gaussian filter 5×5	0.1772	0.1767
Median filter	0.2524	0.2881
Enhance contrast	0.1395	0.1501
Cut 1/16	0.0040	0.0051
Cut 1/4	0.0293	0.0311
Reduced to 1/4	0.2497	0.3010

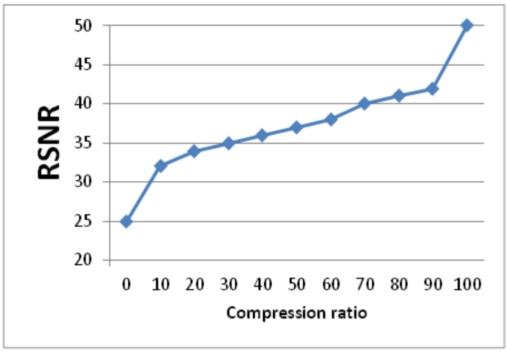


Figure 6. The Values of PSNR after JPEG Compression Attack

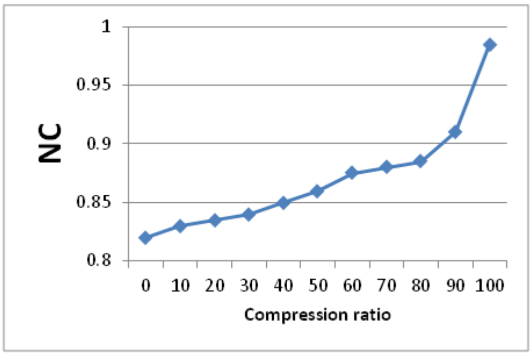


Figure 7. The Values of NC after JPEG Compression Attack

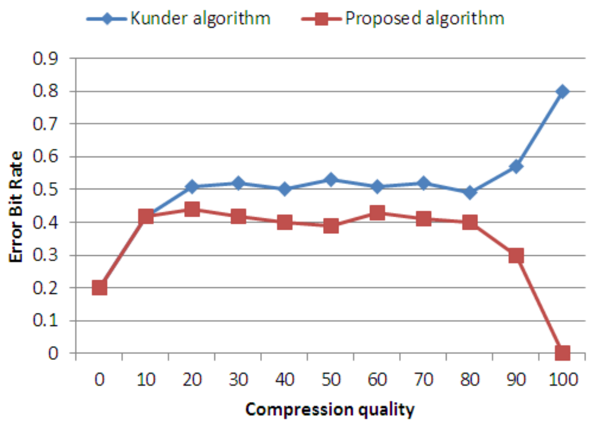


Figure 8. Comparison of Extracted Watermark BER after JPEG Compression

Acknowledgement

This paper is supported by The National Natural Science Foundationof China No. 61202315.

References

[1] XD Zhang, GD Lu, J Feng. The image coding basis and wavelet compression technology - principles, algorithms and standards. Beijing: Tsinghua University Press. 2004.
[2] SG Li, GT Wu. Fractal and Wavelet, Beijing: Science Press. 2002.
[3] D Kundur, D Hatzinakos. *Attack characterization for effective watermarking*. Proc of International Conference Image Processing. 1999; 240-244.
[4] DR Huang, JF Liu, JW Huang. An Embedding Strategy and Algorithm for Image Watermarking in DWT Domain. *Journal of Software.* 2002; 13(7): 1290-1297.
[5] H Inoue, A Miyazaki, A Takashi. *Digital watermark method using the wavelet transform for video data*. Proceedings of the 1999 IEEE International Symposium on. 1999; 4: 247-250.
[6] YF Shao, GW Wu, XG Lin. Quantization-based digital watermarking algorithm. *Journal of Tsinghua University (Science and Technology)*. 2003; 43(1): 20-22.
[7] CW Tang, HM Hang. *A Feature-Based Robust Digital Image Watermarking Scheme*, IEEE Transactions on Processing. 2003; 51(4): 950-959.
[8] CH Fei, D Kundur, RH Kwong. Analysis and design of secure watermark-based authentication systems. *IEEE Trans on Information Forensics Security*. 2006; 1(1): 43-55.
[9] Abduljabbar Shaamala, Shahidan M. Abdullah and Azizah A. Manaf, Study of the effect DCT and DWT domains on the imperceptibility and robustness of Genetic watermarking. *International Journal of Computer Science Issues*. 2011; 8(5): 220-225.

[10] HHe, JP Zhang, Q Wang. Digital Image Watermark Algorithm Based on Wavelet Transform and Compound Chaotic System. J*ournal of harbin university of science and technology*. 2010; 15(4): 15-18.
[11] Y Wu, ZH Guan. A novel digital watermark algorithm based on chaotic maps. *Physics Letters A*. 2007; 365(11): 403-406.
[12] Hu, DQ WANG, F Wan. Wavelet transform watermarking method based on local phase correlation. *Application Research of Computers*,vol.28,no.5,2011,pp1922-1925.
[13] W.Tang, H.M. Hang. A Feature-Based Robust Digital Image Watermarking Scheme, *IEEE Transactions on Processing*. 2003; 51(4): 950-959.
[14] Rusdi CY Chang, HJ Wang, SW Pan. A robust DWT-based copyright verification scheme with Fuzzy ART. *Journal of Systems and Software*. 2009; 82(11): 1906-1915.
[15] DF Chen, YQ Zhang. Blind watermarking algorithm based on lifting scheme wavelet and chaotic mapping. *Computer Engineering and Design*. 2007; 29(20): 5372-5375.
[16] Bao XHMA. Image adaptive watermarking using wavelet domain singular value decomposition. *IEEE Trans on Circuits and Systems for Video Technology*. 2005; 15(1): 96-102.