Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SELF-ADAPTIVE DIGITAL WATERMARKING ALGORITHM BASED ON WAVELET TRANSFORM

[1] ZHANG CHUN NA, [2]ZHU YONG YONG, [1,3]MA CHI,[1]LI YI RAN
[1]College of Software, University of Science and Technology Liaoning, Anshan 114054, China
[2] Department of Economics and Business Administration, Chongqing University of Education, Chongqing 400067, China
[3]Dongling School of Economics and Management, the University of Science and Technology Beijing, Beijing 10083, China
E-mail: [1]zcn1979@yahoo.com.cn

ABSTRACT

This paper proposed a digital watermarking algorithm based on discrete wavelet transform (DWT), 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 Transformation, 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, these algorithms are generally able to resist compression and noise attack.

On the basis of the research of wavelet transform and digital watermarking technology, this paper proposes an adaptive digital watermarking algorithm based on wavelet transform. Algorithm achieved the pretreatment of the watermark information by using multi-scale wavelet transform technology, Arnold scrambling [3] 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 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 [4] 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 improve the crack difficulty and Shear resistance, pretreatment is usually necessary before the digital watermark is embedded into the host image. Arnold scrambling technology and bit-plane decomposition technology are used in the watermark information pretreatment in this paper.

The correlation of the watermark pixel space can be cleared by Arnold scrambling technology, meaningful watermark image becomes meaningless, chaotic, so that the digital watermark has more concealed. Grayscale image is converted to binary image by bit plane decomposition technology, which is the foundation to achieve quantify algorithm later.

2.1 Arnold Scrambling

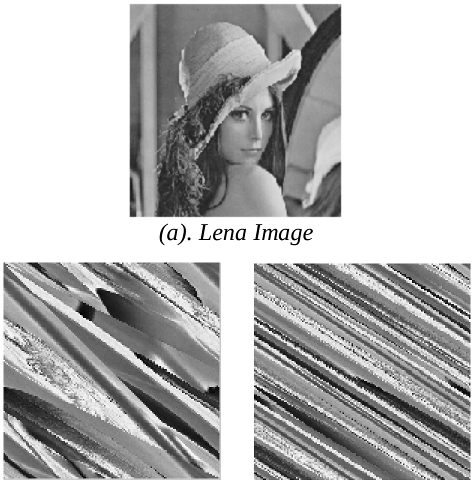
N-order digital image matrix point (x, y) is transformed by the formula (1) to (x', y') :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ K & K+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\, N) \qquad (1)$$

Where $x, y \in \{0,1,2,...,N-1\}$. The transformation is called Arnold scrambling. To do iterative calculation according to the formula (1), through the replacement of discrete points, image information (grayscale, color) is transplanted, while all points of the original image are traversed, a new image is generated. The Arnold scrambling has cyclical characteristics, after iterative cycle it can be changed back to the original image. Further number pairs composed by K and N in equation 1 can be a scrambling key. Some of the commonly used encryption algorithm （such as DES） can be used on its encryption [9], only the master of keys can restore be extracted watermark to the original information, and the security of the watermark is enhanced. In addition, Arnold scrambling process will distract originally damaged bit in the recovery process of the watermark which improved the robustness of digital watermarking. Figure1 is the Lena image scrambling

2.2 Bit Plane Decomposition

Each pixel of a digital image is constituted by a multi-bit way, as shown in Figure 2, each pixel is divided into eight. The size of each pixel value g in the grayscale image can be expressed as $g = \sum_{i=0}^{7} a_i 2^i$, where i represents the position of the pixel, a_i represents the value of the bit i , and $a_i \in \{0,1\}$



(a). Lena Image

(b). n=1 *(c). n=2*

Figure 1: Results of Arnold scrambling digital image (n represents the number of iterations)

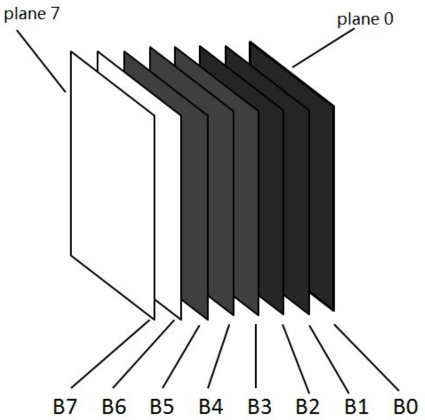
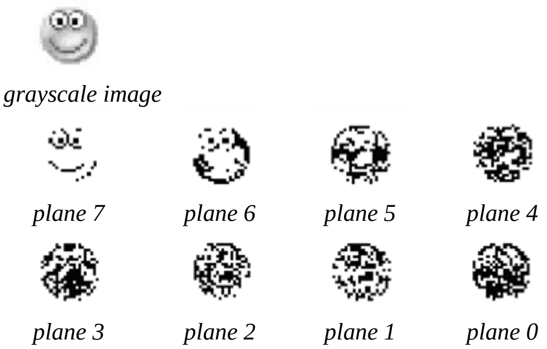


Figure 2:Schematic Diagram Of Bit Plane Decomposition

The distribution characteristics of bit-planes are that from high to low (from plane 7 to plane 0), the details are increasing; the characteristics of bit-plane images are gradually becoming complicated; and the least significant bit-plane are almost random numbers of a uniform distribution. The number of signal energy represented by least significant bit-plane is small, so modification to least significant bit-plane has little effect on the quality of the image. Therefore, after bit-plane decomposition of the watermark image by the proposed algorithm, in accordance with the order from high level to low level, embed the watermark information into the wavelet coefficients of the host images with low resolution to high resolution. The purpose of this is to make sure that the high level value in the grayscale watermark image is embedded into the important wavelet coefficients to enhance its anti-attack capability.

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.



grayscale image

plane 7 *plane 6* *plane 5* *plane 4*

plane 3 *plane 2* *plane 1* *plane 0*

Figure 3: Watermark image each bit-plane after decomposition

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 $f_{k,l}(m,n)$ 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.

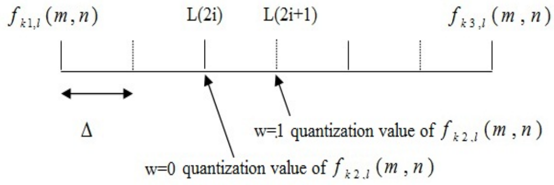

$f_{k1,l}(m,n)$
L(2i)
L(2i+1)
$f_{k3,l}(m,n)$
Δ
w=1 quantization value of $f_{k2,l}(m,n)$
w=0 quantization value of $f_{k2,l}(m,n)$

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 $\Delta' = \dfrac{f'_{k3,l}(m,n) - f'_{k1,l}(m,n)}{2Q-1}$.

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

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

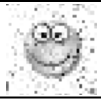
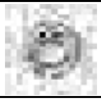
The basic configuration of the computer in experiment is CPU core (TM) 2 Duo/2.5G, memory of 4G, hard disk of 360G. The operating system is Windows 7, and the algorithm is implemented using simulation software Matlab 7. The original host image in experiment is 512×512 grayscale image, and the watermark 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 5), 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.

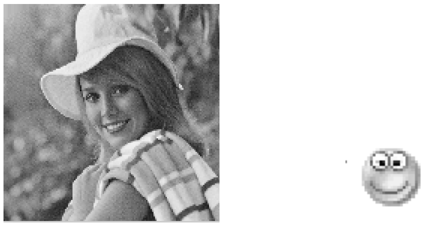
In order to test the robustness of the algorithm, attack such as noise, filtering, cropping is added into the watermark image. Figure 6 shows the result of robustness test. Table 1 shows the values of PSNR and NC detected after adding all kinds of attacks, and the experimental results demonstrate the strong robustness of the algorithm. Figure 7 shows the Watermark extraction image under different JPEG compression ratio. Figure 8 and

Figure 9 show the values of PSNR and NC after JPEG compression attack.

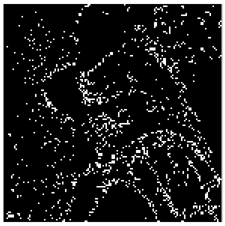
Table 1: The Values Of PSNR And NC Detected After Adding All Kinds Of Attacks

Attacks	***PSNR /db***	***NC***	Watermark extraction
White Noise	39.4225	0.9563	
Salt and pepper noise	22.5745	0.8274	
Gaussian filter 3×3	38.0043	0.8763	
Gaussian filter 5×5	37.9935	0.8756	
Median filter	37.1387	0.8376	
Enhance contrast	5.2574	0.9587	
Cut 1/16	20.2932	0.9981	
Cut 1/4	13.6944	0.9613	
Reduced to 1/4	30.2676	0.8759	

(A).Original Image And Watermark Image



(B). After Embedding Watermark And Extracting Watermark

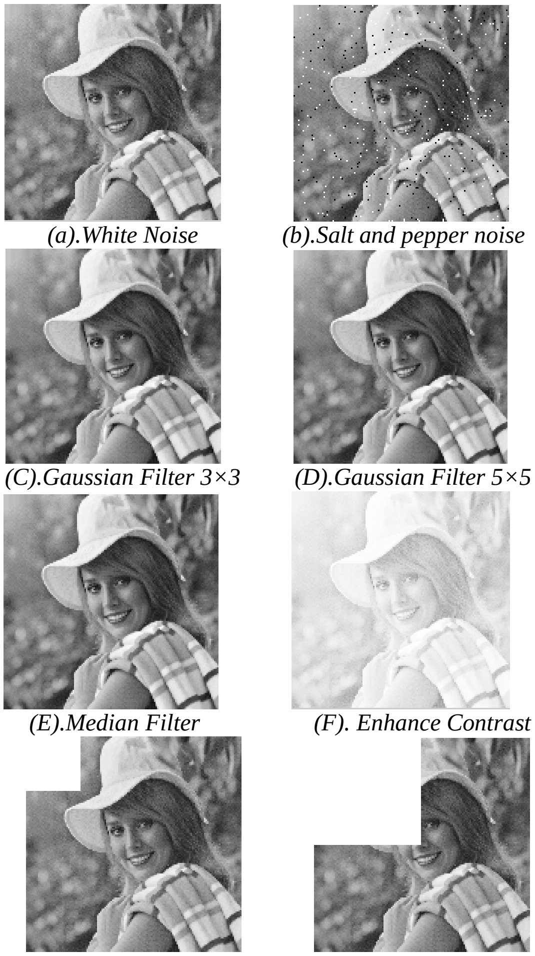


(C). The Two Graphs Difference Embedded Watermark Before And After

Nc=0.9994, Psnr=45.3339db

Figure 5: Embedding And Extracting Watermark In The Case Of Normal Situation Without 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 and the extracted watermark as follows, in which denote watermark sequence length.



(a).White Noise *(b).Salt and pepper noise*

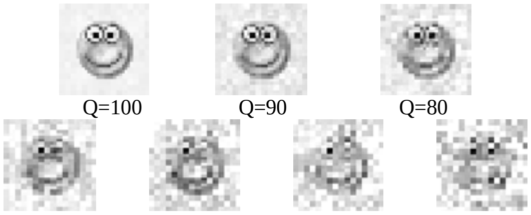
(C).Gaussian Filter 3×3 *(D).Gaussian Filter 5×5*

(E).Median Filter *(F). Enhance Contrast*

(G).Cut 1/16 *(H). Cut 1/4*

(i). Reduced to 1/4

Figure 6: Result Of Watermarked Image After Adding All Kinds Of Attacks



Q=100 Q=90 Q=80

Q=70 Q=60 Q=50 Q=40

Figure 7: Watermark Extraction Image Under Different Jpeg Compression Ratio (Q Represents The Compression Ratio)

Table 2 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.

Table 2: 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 filter 3×3	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 10 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.

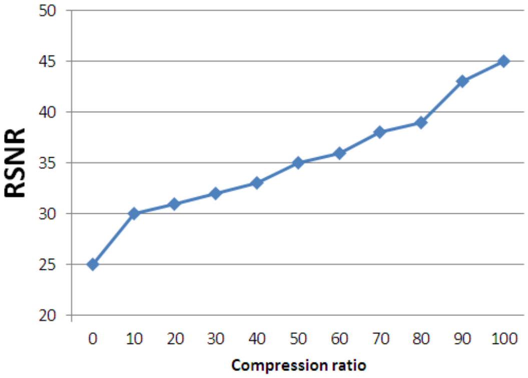


Figure 8: The Values Of PSNR After JPEG Compression Attack

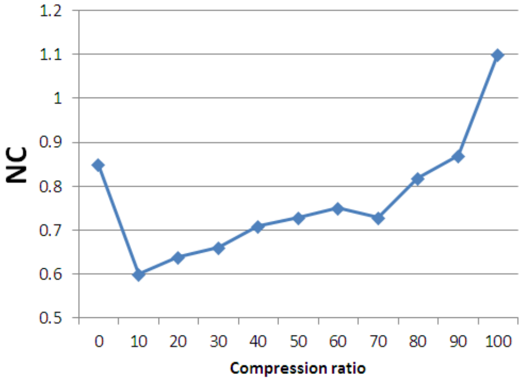


Figure 9: The Values Of NC After JPEG Compression Attack

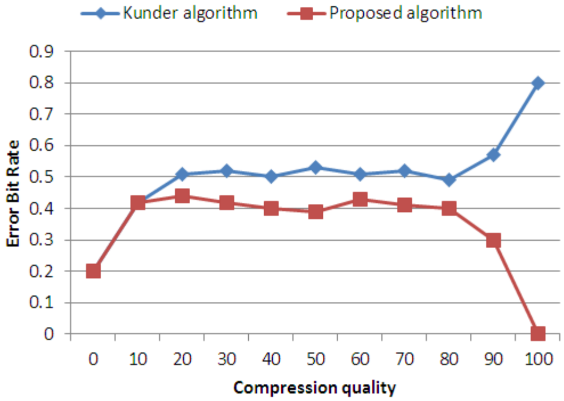


Figure 10: The Comparison Of Extracted Watermark BER After JPEG Compression

5. CONCLUSIONS

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.

REFRENCES:

[1] S.G. Li, and G. T. Wu, Fractal and Wavelet, Beijing: Science Press, 2002.

[2] X. D. Zhang, G. D. Lu, and J. Feng, The image coding basis and wavelet compression technology - principles, algorithms and standards, Beijing: Tsinghua University Press, 2004.

[3] C.W. Tang, H.M. Hang. "A Feature-Based Robust Digital Image Watermarking Scheme", IEEE Transactions on Processing, vol.51 no.4, 2003, pp.950-959.

[4] P. Bao, X.H.MA. "Image adaptive watermarking using wavelet domain singular value decomposition”. IEEE Trans on Circuits and Systems for Video Technology, Vol.15, No.1, 2005, pp. 96-102.

[5] X.Y. Wu, Z.H. Guan. "A novel digital watermark algorithm based on chaotic maps”. Physics Letters A,Vol.365.No.11 2007, pp.403-406.

[6] C.H. Fei, D. Kundur , R.H. Kwong. "Analysis and design of secure watermark-based authentication systems”. IEEE Trans on Information Forensics Security, Vol.1, No.1, 2006, pp.43-55.

[7] K. Maeno, Q. B. Sunn, S.F.Chang, et al. "New semi-fragile image authentication watermarking techniques using random bias and non-uniform quantization”, IEEE Trans on Multimedia, Vol.8,No.1,2006,pp.32-45.

[8] D.F.Chen,Y.Q.Zhang,"Blind watermarking algorithm based on lifting scheme wavelet and chaotic mapping”, Computer Engineering and Design,Vol.29,No.20,2007,pp.5372-5375.

[9] M.Ramkumar,A.N.Akansu."A robust oblivious watermarking scheme”. Vancouver, in IEEE International Conference on Image Processing (ICIP), 2000, pp.450-453.

[10]X.Zhang,G.C.Zhang,"Multi-function Digital Watermark Based on Wavelet Transformation”, Computer Engineering, Vol.34, No.18, 2008, pp.169-173.

[11]B. L. Li, D. C. Xu, "Image Watermark Algorithm for harr Wavelet Transform Based on Lifting Scheme”, Computer Engineering,Vol.35,No.9,2009,pp.155-157.

[12] W. C. Hung, K. Y. Sheng. "An Efficient Contract Signing Protocol Using the Aggregate Signature Scheme to Protect Signers Privacy and Promote Reliability”. ACM SIGOPS Operating Systems Review, Vol.39, No.4, 2005,pp. 66-79.

[13] W.C.Hung,Y.C. Heng , "How to Protect Exchanged Secrets in the Fair Exchange Protocol with Off-line TTP”, Computers and Electrical Engineering, Vol.32, No.5, 2006, pp.364-375.

[14]D.Boneh,C. Gentry, B.Lynn, et al,"Aggregate and Verifiably Encrypted Signatures From Bilinear Maps”,Proc. of EUROCRYPT’03, 2003,pp. 272- 293.