Secure Semi-Fragile Watermarking for Image Authentication Based on Parameterized Integer Wavelet

Xiaoyun Wu[1, 2], Jiwu Huang[1,*], Junquan Hu[1] , and Yun-Qing Shi[3]

[1] School of Information Science and Technology, Sun Yat-Sen University
Guangzhou, 510275, P. R. China
isshjw@mail.sysu.edu.cn

[2] School of Information Science, Guangdong University of Business Studies
Guangzhou, 510320, P. R. China

[3] Department of Electrical and Computer Engineering, New Jersey Institute of Technology
Newark, NJ 07102, USA

Received 28 April 2006; Revised 12 May 2006; Accepted 13 June 2006

Abstract. With the tremendous amount of images distributed over Internet, image authentication has drawn extensive attention for integrity verification. For instance, watermarking fragile to malicious modifications while robust to data compression has been proposed for image authentication. However, the security of watermark has not received enough attention yet. In this paper, we propose a secure semi-fragile watermarking scheme for image authentication based on integer wavelet transform with parameters. The features of the proposed scheme are as follows. Firstly, parameterized integer wavelet transform is adopted. The wavelet base is chosen by a parameter. It is impossible to extract the watermark without the exact parameter and thus the security of the watermark is guaranteed. Secondly, the performance of the generated watermark is improved and the computational complexity is reduced due to the lifting scheme used in the proposed framework of parameterized integer wavelet transform. Thirdly, the proposed watermark can tolerate JPEG lossy compression to a quality factor as low as 40, while being sensitive to malicious attack and able to locate the tampered area accurately. Experimental results demonstrate the merits of the proposed algorithm.

Keywords: semi-fragile watermark, watermark security, image authentication, integer wavelet transform, parameterization

1 Introduction

Digital multimedia has been widely distributed via Internet and broadcasting nowadays. This leads to an acute need for media authentication because the digital contents can be easily edited or modified by using some readily available software tools. As a new tool for content authentication, digital watermarking has been drawing considerable attention and becoming an active research area.

Digital watermark can be classified as robust, fragile and semi-fragile [1]. The robust watermark survives even when the watermarked digital content has been severely attacked and thus can be applied to copyright protection. On the other hand, the fragile watermark will be destroyed even if the change in the marked digital media is minor and thus can be used for data integrity verification. Offering a tradeoff between robustness and fragility, semi-fragile watermark that can resist content-preserving operations (such as data compression within a reasonable extent) while being sensitive to content-altering manipulations (such as feature replacement) is more practicable for content integrity verification.

Many fragile and semi-fragile watermarking schemes based on DWT (discrete wavelet transform) have been reported during the past years. Kundur et al. [2] suggested to embed watermark in the selected wavelet coefficients via quantization. Tamper detection at multi-resolution had been achieved. But it is not consistent with characteristics of the HVS (human visual system) [3] and brings perceptible distortion to the watermarked images. Inoue et al. [4] embedded fragile watermark by thresholding and quantizing wavelet coefficients at the coarser scales and gave a measurement for tamper proofing. Yu et al. [5] modeled the changes of DWT coefficient

[*] Correspondence author

caused by tamper as Gaussian distribution. Malicious tamper has large variance while incidental tamper has small variance. They embedded mark via modulating the mean of some coefficients instead of individual coefficients.

Most of these conventional DWT-based fragile and semi-fragile watermarking schemes reported in literature have the following three shortcomings. i) Vulnerability to attack. The schemes use only one wavelet base to perform the DWT. Once the algorithm is open to public, the hidden information bits may be exposed or modified easily by an attacker. ii) Low robustness to JPEG compression. Almost all of the existing fragile watermark cannot resist JPEG compression with the quality factor lower than 70. iii) High computational complexity. Though the conventional DWT needs less computational cost as compared with DCT (discrete cosine transform), it may be time consuming to perform the DWT on a whole image with large size.

To improve watermark security, Kundur et al. [2] used a random triple to select the embedding region. However, it may weaken the ability to tamper detection and tamper localization. Unfortunately, the security of fragile watermarking techniques has not received sufficient attentions so far. A feasible method to enhance security is to choose a wavelet base from a set of appropriate wavelet bases with parameters. If the parameter space is large enough, then it will be difficult for an attacker to obtain the useful information to attack, thus guaranteeing high security. Based on this idea, Dietl etc. [6-7] proposed to use secret, key-dependent parametric wavelet filters to improve the security of robust watermarking schemes. However, their methods are based on conventional DWT.

Lifting scheme, as the second generation of wavelet transform, has effectively enhanced the processing speed. IWT (Integer wavelet transform) allows constructing reversible wavelet transform to decrease round-off errors which have important impact on the fragile watermark. By using lifting scheme, we can implement IWT efficiently.

In this paper, we propose a secure semi-fragile watermarking scheme for image authentication based on parameterized IWT. It incorporates parameterization and IWT based on lifting scheme to achieve high security and low computational complexity. The semi-fragile watermarking algorithm is presented by applying the parameterized integer wavelets. Analysis and experimental results demonstrate that the proposed watermarking scheme is secure and capable of locating the tampering accurately, while it is robust to JPEG lossy compression as the quality factor low as 40.

This paper is organized as follows. In Section 2, we review the lifting scheme briefly and then adopt a special scheme to parameterize the conventional 9-7 biorthogonal filter bank using lifting scheme, thus constructing the parameterized IWT. Section 3 describes the design of the proposed semi-fragile watermarking algorithm, including preprocessing of a binary image, watermark embedding/extraction and tamper detection. In Section 4, we analyze the security and computational complexity of the proposed scheme. In Section 5, we present the experimental results. Finally, conclusions are drawn in Section 6.

2 Parameterized Integer Wavelet Transform

Cohen et al. [8] proposed a technique named lifting scheme to construct fast and concisely transform steps for wavelet transform. From then on, the lifting scheme has received more and more attention as it can offer not only fast transform, but also “you can construct your owner wavelet at home” [9]. Theoretically, lifting scheme is designed based on the matrix algebra theory and phase filter bank theory such as perfect reconstructed filter bank theory. Generally, lifting scheme includes three steps: splitting, prediction, and update [10].

It has turned out that every FIR (Finite Impulse Response) wavelet or filter bank can be decomposed into lifting steps [10]. The number of lifting steps is bounded by the length of the original filters. It is noted that the lifting factorization is not unique. Depending on the application, one may choose the factorization with the smallest number of steps, or the one that preserves symmetry.

An example of the lifting scheme with CDF 9-7 biorthogonal wavelet [10] is given below. To a prefixed one-dimensional signal $\{x_l\}_{l\in Z}$, the lifting steps are described as following:

$$\begin{cases} s_l^{(0)} = x_{2l} \\ d_l^{(0)} = x_{2l+1} \end{cases} \quad \begin{cases} d_l^{(1)} = d_l^{(0)} + \alpha(s_l^{(0)} + s_{l+1}^{(0)}) \\ s_l^{(1)} = s_l^{(0)} + \beta(d_l^{(1)} + d_{l-1}^{(0)}) \end{cases} \quad \begin{cases} d_l^{(2)} = d_l^{(1)} + \gamma(s_l^{(1)} + s_{l+1}^{(1)}) \\ s_l^{(2)} = s_l^{(1)} + \delta(d_l^{(2)} + d_{l-1}^{(2)}) \end{cases} . \tag{1}$$

$$\begin{cases} s_l = \zeta s_l^{(2)} \\ d_l = d_l^{(2)} / \zeta \end{cases} . \tag{2}$$

$$\alpha\text{=-1.586134342; } \beta\text{=-0.05298011854; } \gamma\text{=0.8829110762;} \\ \delta\text{ =0.4435068522; } \zeta\text{ =1.149604398.} \tag{3}$$

where s_l and d_l are commonly referred to as lower frequency and detail coefficients, respectively, and $s_l^{(i)}$, $d_l^{(i)}$ are called mid-output.

In practical application, it may be more convenient to have only one parameter. According to the corresponding theory, five parameters in Equation (1)~(3) can be expressed by only one parameter α. For the sake of brevity, we will not describe the theory in detail here. Interested readers may refer to literatures, say, Zhong et al. [11] for more detailed description. The formulae that use α to expression the rest of parameters are listed below:

$$\begin{cases} \beta = -\dfrac{1}{4(1+2\alpha)^2} \\ \gamma = \dfrac{-1-4\alpha-4\alpha^2}{1+4\alpha} \\ \delta = \dfrac{1}{16}(4-\dfrac{2+4\alpha}{(1+2\alpha)^4}+\dfrac{1-8\alpha}{(1+2\alpha)^2}) \\ \zeta = \dfrac{2\sqrt{2}(1+2\alpha)}{1+4\alpha} \end{cases}. \quad \textbf{(4)}$$

The corresponding filter coefficients can be expressed in terms of α as:

$$\begin{cases} h_0 = \dfrac{\sqrt{2}}{16}\dfrac{184\alpha^3+266\alpha^2+125\alpha+20}{(1+2\alpha)^2(1+4\alpha)} \\ h_1 = \dfrac{\sqrt{2}}{32}\dfrac{128\alpha^3+152\alpha^2+58\alpha+5}{(1+2\alpha)^2(1+4\alpha)} \\ h_2 = \dfrac{-\sqrt{2}}{8}\dfrac{3+4\alpha}{1+4\alpha} \\ h_3 = \dfrac{\sqrt{2}}{32}\dfrac{8\alpha^2+6\alpha+3}{(1+2\alpha)^2(1+4\alpha)} \\ h_4 = \dfrac{\sqrt{2}}{32}\dfrac{\alpha(8\alpha^2+6\alpha+3)}{(1+2\alpha)^2(1+4\alpha)} \end{cases} \quad \begin{cases} g_0 = \dfrac{\sqrt{2}}{8}\dfrac{(8\alpha+3)}{(1+2\alpha)} \\ g_1 = \dfrac{\sqrt{2}}{16}\dfrac{9\alpha+4}{1+2\alpha} \\ g_2 = \dfrac{\sqrt{2}}{16}\dfrac{1}{1+2\alpha} \\ g_3 = \dfrac{-\sqrt{2}}{16}\dfrac{\alpha^2}{1+2\alpha} \end{cases}. \quad \textbf{(5)}$$

The low pass and high pass filter banks in the CDF 9-7 wavelet, denoted by $\{h_4,h_3,h_2,h_1,h_0,h_1,h_2,h_3,h_4\}$ and $\{g_3,g_2,g_1,g_0,g_1,g_2,g_3\}$, can thus be parameterized by selecting different α values.

To make the filter banks achieve perfect reconstruction, however, the value of parameter α should not be chosen arbitrarily. Note that, the rational range of the parameter α has not been derived in [11]. According to the conditions listed in [11], we have derived the rational range for the parameter α by ourselves. That is $\alpha \in (-3,-1.2)$. The derivation is given in Appendix.

According to IWT theory [12], we can construct parameterized IWT based on the framework mentioned above. That is,

$$\begin{cases} s_l^{(0)} = x_{2l} \\ d_l^{(0)} = x_{2l+1} \end{cases} \begin{cases} d_l^{(1)} = d_l^{(0)} + Int(\alpha(s_l^{(0)}+s_{l+1}^{(0)})) \\ s_l^{(1)} = s_l^{(0)} + Int(\beta(d_l^{(1)}+d_{l-1}^{(0)})) \end{cases} \quad \textbf{(6)}$$

$$\begin{cases} d_l^{(2)} = d_l^{(1)} + Int(\gamma(s_l^{(1)}+s_{l+1}^{(1)})) \\ s_l^{(2)} = s_l^{(1)} + Int(\delta(d_l^{(2)}+d_{l-1}^{(2)})) \end{cases}.$$

$$\begin{cases} d_l^{(3)} = d_l^{(2)} + Int((\zeta-\zeta^2)s_l^{(2)}) \\ s_l^{(3)} = s_l^{(2)} + Int((-1/\zeta)d_l^{(3)}) \end{cases} \begin{cases} d_l^{(4)} = d_l^{(3)} + Int((\zeta-1)s_l^{(3)}) \\ s_l^{(4)} = s_l^{(3)} + d_l^{(4)} \end{cases} \begin{cases} s_l = s_l^{(4)} \\ d_l = d_l^{(4)} \end{cases}. \quad \textbf{(7)}$$

where $Int(x)$ means taking the integer part of x. Replacing the parameters β, γ, δ, ζ with α using Equation (4), we then have parameterized IWT. Equation (7) is an extra lifting step different from Equation (2). We adopt it here because it can achieve reversible transform according to [12] while Equation (2) cannot.

3 The Proposed Scheme

In this section, the proposed scheme is described.

3.1 Watermark Preprocessing

Without loss of generality, assume the watermark W is a binary image of size $M \times N$, $W = w(i, j)$, and the PN denotes a binary pseudorandom matrix of size $M \times N$, generated by a secret key k , $PN = p_n(i, j)$.

We generate the ultimate hidden watermark W^* by using Equation (8).

$$W^* = W \oplus PN \ . \qquad \textbf{(8)}$$

where $\oplus$ denotes the exclusive OR operation.

3.2 Watermark Embedding

As mentioned in Section 1, semi-fragile watermark should be robust to incidental modification and fragile to malicious tamper. Moreover, to an invisible semi-fragile watermark, it should have the following features: i) Perceptual invisibility; ii) Ability to detect and locate maliciously tampered areas in a modified image. From the definition of the watermark signal, it is clear that to ensure the robustness and the fragility described above, the embedding strength and bitrate of the watermark should be as large as possible. However, this will lead to a decrease of perceptual invisibility. Therefore a compromise is required here. That is, the embedding strength, embedded bitrate and embedding region should be selected carefully.

In this paper, we propose a watermarking scheme based on parameterized IWT. Suppose that an image is decomposed by j-level IWT. It produces 3*j detail subbands and a low frequency subband LL_j. Compared to other detail subbands, the coefficients in LL_j subband have the following features: i) They will be well preserved after common signal processing such as JPEG compression. ii) They have larger perceptual capacity so as to ensure invisibility of the watermarked image after embedding a watermark with certain strength. Therefore, LL_j subband is proposed for watermark embedding. We choose j to be three in our work.

We use the scheme presented in [13] to embed the watermark W^*, defined in Equation (8), in the LL_3 subband. It guarantees some robustness of watermark.

Let $C\_LFB(a)$ denote the five least significant bits of a , $R\_LFB(a,d)$ represent the substitution of the five least significant bits of a with d . The bit embedding in an IWT coefficient in the LL_j is described below.

If $w^*(i, j) = 1$

$$f^*(i,j) = \begin{cases} R\_LFB(f(i,j) - 01000b, 11000b) & C\_LFB(f(i,j)) \le 01000b \\ R\_LFB(f(i,j), 11000b) & \text{otherwise} \end{cases} . \qquad \textbf{(9)}$$

If $w^*(i, j) = 0$

$$f^*(i,j) = \begin{cases} R\_LFB(f(i,j) - 10000b, 01000b) & C\_LFB(f(i,j)) \ge 11000b \\ R\_LFB(f(i,j), 01000b) & \text{otherwise} \end{cases} . \qquad \textbf{(10)}$$

where $f(i, j)$ and $f^*(i, j)$ are IWT coefficients located at (i, j) in LL_3 subband before and after embedding a bit, and $w^*(i, j)$ is a watermark bit of W^* to be embedded into $f(i, j)$. After data embedding, performing the inverse IWT on the modified wavelet coefficients, we can have the watermarked image.

3.3 Watermark Extraction

Three-level IWT is operated on a to-be authenticated image. Let $f'(i, j)$ denote an IWT coefficient located at (i, j) in LL_3 subband.

Let $w^*'(i, j)$ denote the extracted watermark bit, $LFB(a)$ denote the 5th least significant bit of a, we have:

$$w^*(i,j)=\begin{cases}1 & LFB(f'(i,j))=1\\ 0 & LFB(f'(i,j))=0\end{cases}\quad (1\le i\le M,\ 1\le j\le N)\ . \tag{11}$$

Using Equation (12), we can obtain the watermark W', $W'=w'(i,j)$ $(1\le i\le M,\ 1\le j\le N)$.

$$w'(i,j)=w^{*}{}'(i,j)\oplus p_n(i,j)\quad (1\le i\le M,\ 1\le j\le N)\ . \tag{12}$$

It is obliviously that the extraction of watermark does not require the original image.

3.4 Tamper Detection

We use D denoting the difference image of size $M\times N$, $D{=}d(i,j)$. It is the difference between the original and extracted watermark and is expressed in Equation (13):

$$D=|W-W'|\ . \tag{13}$$

When a watermarked image suffers from incidental attacks, most of the watermark error pixels are isolated points on the difference image. On the contrary, most of the watermark error pixels resulted from malicious attacks are gathered together with a high probability.

Based on the difference image, both the subjective evaluation and the objective evaluation are used for tamper detection. By observing if the watermark error pixels are dense or sparse in the extracted watermark, we can distinguish malicious attack from incidental changes. If it is malicious attack, we can further identify the tampered area and the degree of tamper. To be objective, a quantitative metric is given as follows.

For a watermark error pixel in the difference image D, it is a dense pixel if at least one of its eight neighbor pixels is an error pixel. Otherwise, it is a sparse pixel. Thus, we define the following parameters.

$$area_{dense}=\{\text{The total number of dense pixel in the difference image } D\}\ . \tag{14}$$

$$area_{sparse}=\{\text{The total number of sparse pixel in the difference image } D\}\ . \tag{15}$$

$$area=\{\text{The total number of pixel in the difference image } D\}\ . \tag{16}$$

$$area_{total}=area_{dense}+area_{sparse}\ . \tag{17}$$

$$\lambda=\frac{area_{total}}{area},\ \eta=\frac{area_{dense}}{area_{total}}\ . \tag{18}$$

Now, we can evaluate whether a modification is malicious or incidental objectively by using the following rules:

If $\lambda=0$, then the tested image is not altered.

If $\lambda>0$ and $\eta<\tau$, where the threshold τ is selected carefully (generally, we fix it between 0.5 and 1), then the tested image in this category then experiences incidental distortions.

If $\eta\ge\tau$, then the tested image is maliciously tampered.

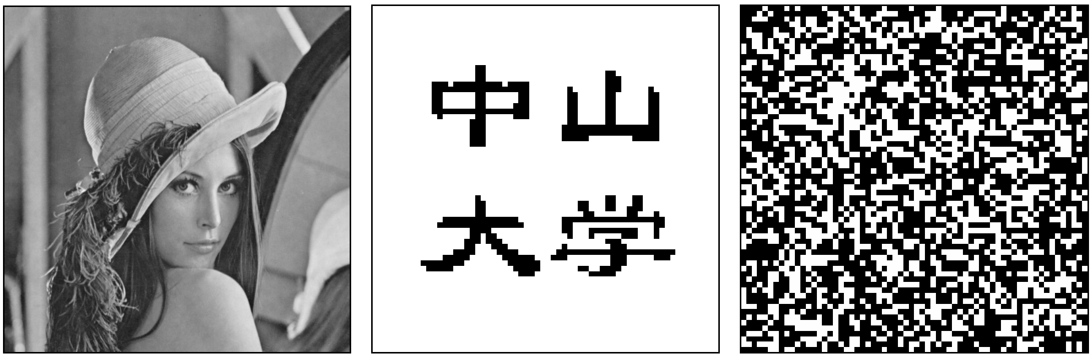
4 Performance Analysis

In this section, the performance is analysed.

4.1 Security

Kerckhoff stated that the security of an encryption system must lie in the choice of a key, not the algorithm used to for encryption [14]. It may be applicable to the security of digital watermarking as well.

To test the sensitivity of the parameter's change, we use four standard images Lena, Baboon, Peppers and Boat (512×512×8 bits). We test our algorithm at 31 different embedding parameters, obtained from [-2.85, -1.35] at interval of 0.05. That is, $\alpha \in \{-2.85,-2.8,...,-1.5,-1.45,-1.4,-1.35\}$. We select the parameter whose difference as compared to the embedding parameter is 10^{-15} to extract the watermark. We cannot extract any useful information even if the difference between the embedding and the extracting parameter is as small as 10^{-15}. We get the similar results for the four images. To the limited length of the article, we only demonstrate the results of Lena in Fig. 1. Fig. 1(a) is a watermarked Lena image using the proposed method, in which the parameter α used is -1.500000000000000. During the hidden data extraction, the parameter -1.500000000000000 and -1.500000000000001 are used, respectively. Fig. 1(b) shows the correctly extracted data, which is the logo composed of Chinese characters. Fig. 1(c) indicates what has been extracted using a wrong parameter, i.e., the second parameter, -1.500000000000001, which is only differ by the first (correct) parameter by 0.000000000000001, an extremely small difference. It shows that our scheme is very sensitive to the parameter's change, and it is extremely difficult to acquire the exact embedding parameter, hence it is secure enough for many applications. It is vain for the attackers to get some useful information about the algorithm without knowing the exact parameter used in data embedding. Furthermore, the rational range of the parameter is (-3, -1.2), meaning that there are many real numbers of rational parameters in it. Hence, it is practically difficult to search exhaustively the exact parameter.



(a) (b) (c)

Fig. 1. Security of the proposed method: (a) Watermarked image (α =-1.500000000000000 is used for embedding);
(b) Extracted mark (64×64) with the correct parameter (α =-1.500000000000000);
(c) Extracted mark with a slightly different parameter (α =-1.500000000000001)

4.2 Computational Complexity

In Section 1, we have mentioned that the schemes based on the conventional DWT offer lower computational complexity than those based on DCT. Given a signal with length *n*, the computational load of DWT and DCT may be expressed as $O(n)$ and $O(n\log(n))$, respectively. For conventional 9-7 DWT, 14 floating-point additions and 16 floating-point multiplications should be used for two wavelet coefficients. In the proposed scheme in this paper, the parameterized 9-7 IWT is constructed by using lifting scheme. According to Equation (6)~(7), our parameterized 9-7 IWT only needs 12 integer additions, 7 floating-point multiplications and 7 round-off operations. As compared with the conventional 9-7 DWT, almost half of the computational cost will be saved. Moreover, since all of the wavelet coefficients are all with integer form, hence, the algorithm is easily to be realized by hardware.

5 Experimental Results

We have tested our scheme on the "Lena" and "Baboon" images (both of 512×512×8 bits). In our work, we choose a three-level IWT since it has been enough for us to embed the selected watermark signal. The embedding parameter α is -1.500000000000000. The PSNR of the watermarked Lena and Baboon images are 42.26 dB and 42.11dB respectively, as shown in Fig. 2. The watermarks are perceptually invisible. Fig. 3(a) shows the extracted watermarks from the marked image that has been compressed by JPEG at different quality factors. We can see that the proposed scheme can resist JPEG compression when the quality factor is as low as 40, while the JPEG compression with a quality factor smaller than 40 should be considered as serious distortion. In order to justify the performance of the proposed scheme, we compare its robustness to JPEG with that in [15]. Fig. 3(b) shows the results obtained with the same watermark signal by using the method in [15]. Obliviously, our proposed scheme is more robust against JPEG compression than that in [15]. Fig. 4 demonstrates the fragility of our proposed scheme to malicious tamper. Furthermore, the proposed scheme can locate the tamper areas when malicious tamper takes place. Fig. 4(a) and Fig. 4(d) depicted two differently tampered Lena images. Fig. 4(b) and Fig. 4(e) show the extracted data, from which the malicious tampering are detected. Fig. 4(c) and Fig. 4(f) are the difference images between the hidden data and the extracted data, from which the tamper areas have been located.

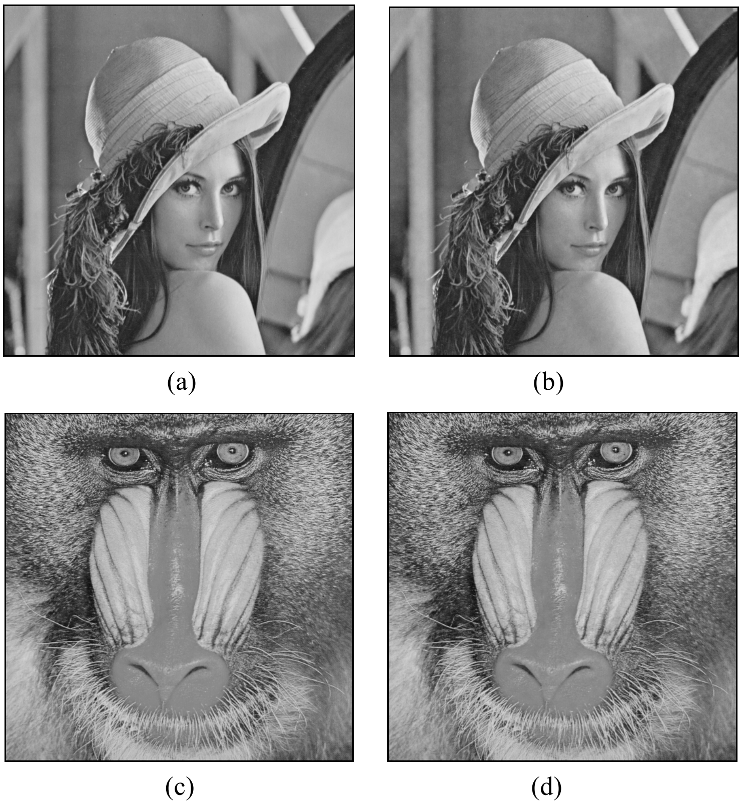
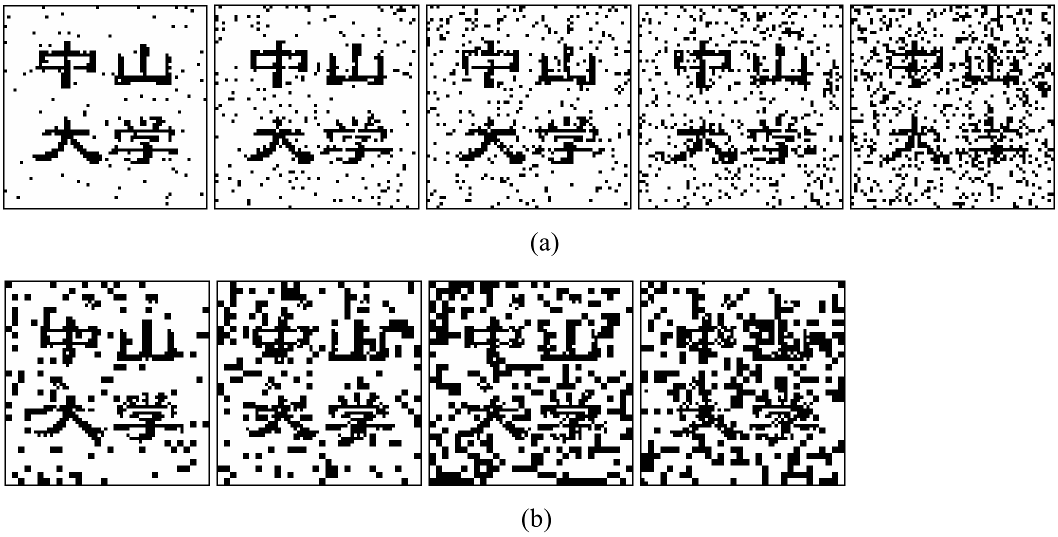
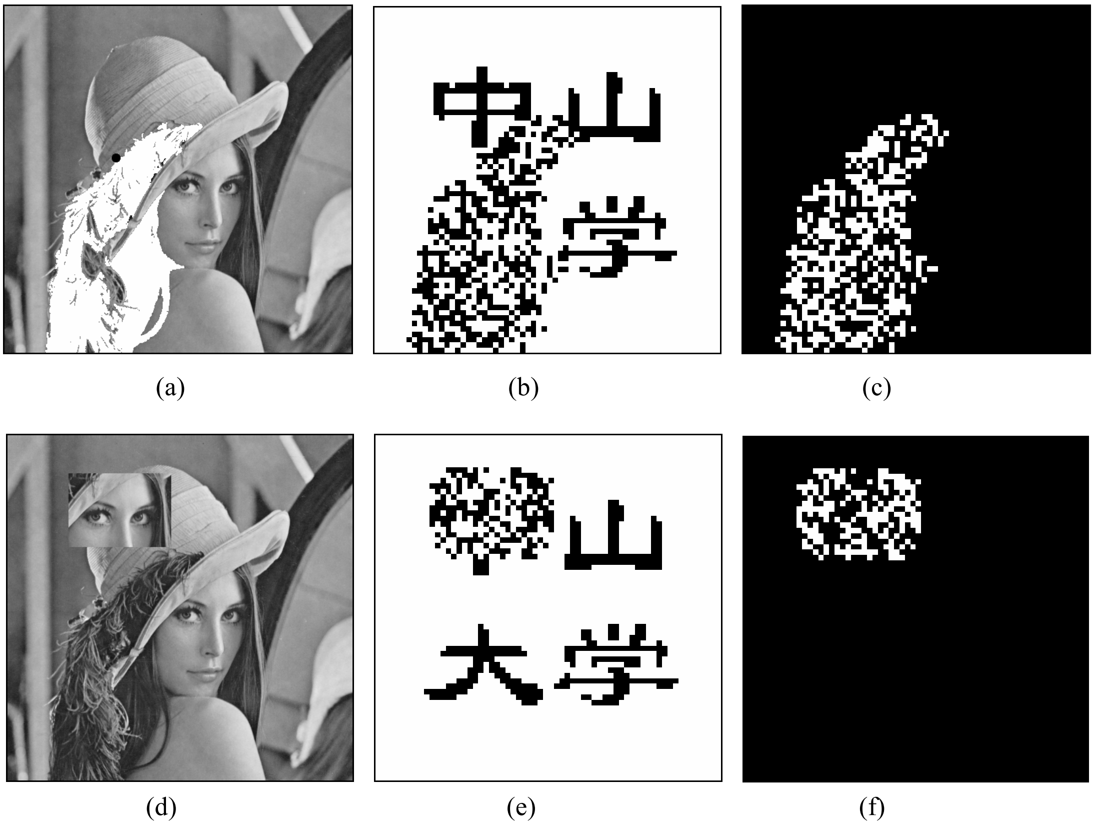

(a) (b)
(c) (d)

Fig.2. Invisibility: (a), (c) The original Lena and Baboon images; (b) The watermarked Lena image (42.26 dB); (d) The watermarked Baboon image (42.11 dB)



(a)
(b)

Fig.3. The mark extracted from the watermarked image that has been compressed by JPEG with different quality factor: (a) Our scheme. (80, 70, 60, 50, 40); (b) Scheme in [15]. (80, 70, 60, 50).



(a) (b) (c)

(d) (e) (f)

Fig.4. Tampered image; (b),(e) Tampered watermark; (c),(f) Difference image

5 Conclusions

In this paper, we propose a secure semi-fragile watermarking for image authentication based on a parameterized IWT. Compared with the existing DCT-based or DWT-based fragile and semi-fragile watermarking schemes, the proposed scheme has lower computational complexity due to IWT via lifting scheme. The appropriate watermark cannot be extracted without knowing the exact parameter owing to the usage of parameterized IWT and thus the security of the watermark is greatly enhanced. A quantitative measure that distinguishes malicious attack from accidental modification is also given in this paper. In addition, tamper detection can be observed by the extracted watermark due to the use of a meaningful binary image as the watermark. Experiments demonstrate the security of the watermark and show that the proposed method is capable of detecting tamper accurately while tolerating JPEG lossy compression to a large extent. It is practical in content authentication system.

6 Acknowledgement

Authors appreciate, respectively, the support received from NSF of China (60325208, 90604008), NSF of Guangdong (04205407), New Jersey Commission of Science and Technology via NJWINS.

References

[1] I. J. Cox and M. I. Miller, “The first 50 years of electronic watermarking,” *Journal of Applied Signal Processing*, 2002, No.2, pp.126-132.

[2] D. Kundur and D. Hatzinakos, "Towards a telltale watermark techniques for tamper-proofing," *Proc of IEEE Int. Conf. on Image Processing*, 1998, Vol.2, pp.409-413.

[3] B. Watson and G. Y. Yang, "Visibility of wavelet quantization noise," *IEEE Trans. on Image Processing*, Vol. 6, 1997, pp.1164-1175.

[4] H. Inoue, A. Miyazaki and T. Katsura, "Wavelet-based watermarking for tamper proofing of still images," *Proc. Int. Conf. on Image Processing*, Vol. 2, 2000, pp. 88-91.

[5] G. Yu, C. Lu, Y. Liao and J. Sheu, "Mean quantization blind watermarking for image authentication," *Proc of IEEE Int. Conf. on Image Processing*, Vol. 3, 2000, pp.706-709.

[6] W. Dietl, P. Meerwald, A. Uhl., "Key-dependent pyramidal wavelet domains for secure watermark embedding," *Security and Watermarking of Multimedia Contents V*, Vol.5020, 2003, pp.728~739.

[7] W. Dietl, P. Meerwald, A. Uhl., "Protection of wavelet-based watermarking systems using filter parameterization," *Signal Processing*, Vol.83, No.10, 2003, pp.2095~2116.

[8] A. Cohen, I. Daubechies, J. C. Feauveau, "Biorthogonal bases of compactly supported wavelets," *Communications on Pure and Applied Mathematics*, XLV, 1992, pp.485 - 560.

[9] W. Sweldens and P. Schrder, "Building your own wavelets at home," *Wavelets in Computer Graphics*, ACM SIGGRAPH Course Notes, 1996, pp.15-87.

[10] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," *Journal of Fourier Analysis*, Vol.4, No.3, 1998, pp.245-267.

[11] G. Zhong, L. Cheng, H. Chen, "A simple 9/7-tap wavelet filter based on lifting scheme," *Proc of IEEE Int. Conf. on Image Processing*, Vol. 2, 2001, pp.249-252.

[12] R. Calderbank, I. Daubechies, W. Sweldens and B. Yeo, "Wavelet transforms that map integers to integers," *Journal of Applied and Computational Harmonic Analysis*, No.5, 1998 pp.332-369.

[13] H. Liu, J. Liu, J. Huang, D. Huang and Y. Q. Shi, "A robust DWT-based blind data hiding algorithm," *Proc. of IEEE Int. Sym. on Circuits and Systems*, Vol. 2, 2002, pp.672-675.

[14] J.L. Massey, "Contemporary cryptology: An introduction," in *Contemporary Cryptology: The Science of Information Integrity*, G.J. Simmons, Ed. New York: IEEE Press, 1992, pp.3-39.

[15] J. Hu, J. Huang, D. Huang, Y. Q. Shi, "Image fragile watermarking based on fusion of multi-resolution tamper detection," *IEE Electronics Letters*, Vol.38, No.24, 2002, pp.1512-1513.

Appendix:

Let the analysis low-pass symmetric filter and synthesis symmetric low-pass filter be

$$H(\omega) = h_0 + 2\sum_{n=1}^{L_1} h_n \cos n\omega \ . \qquad \textbf{(A1)}$$

$$G(\omega) = g_0 + 2\sum_{n=1}^{L_2} g_n \cos n\omega \ . \qquad \textbf{(A2)}$$

To construct biorthogonal wavelet, we have the following theorem [10].

Theorem 1: Suppose

$$H(\omega) = \sqrt{2}(\frac{1+e^{-i\omega}}{2})^{N} F(\omega) \ . \qquad \textbf{(A3)}$$

$$G(\omega) = \sqrt{2}(\frac{1+e^{-i\omega}}{2})^{\tilde{N}} \tilde{F}(\omega) \ . \qquad \textbf{(A4)}$$

where $F(\omega)$ and $\tilde{F}(\omega)$ are polynomials about $e^{-i\omega}$. Then $H(\omega)$ and $G(\omega)$ can construct biorthogonal wavelet, if it meets the following requirements.

i) $H(0) = G(0) = \sqrt{2}$;

ii) $\sup_{\omega\in[0,2\pi)} |F(\omega)| < 2^{N-1}$, $\sup_{\omega\in[0,2\pi)} |\tilde{F}(\omega)| < 2^{\tilde{N}-1}$;

iii) $H(\omega)\overline{G}(\omega) + H(\omega+\pi)\overline{G}(\omega+\pi) = 2$.

To design the desired 9-7 biorthogonal wavelet, let $L_1 = 4, L_2 = 3, N = 2, \tilde{N} = 4$. Then combining Equations A1-A4, we get

$$\begin{aligned} F(\omega) = 2\sqrt{2}(2*(h_4\cos(3\omega) + (h_3 - 2h_4)\cos(2\omega) \\ + (h_2 - 2h_3 + 3h_4)\cos(\omega)) + (h_1 - 2h_2 + 3h_3 - 4h_4)e^{i\omega}) \end{aligned} \ . \qquad \textbf{(A5)}$$

$$\tilde{F}(\omega) = 8\sqrt{2}(2*g_3\cos(\omega) + (g_2 + 4g_3)e^{2i\omega}) \ . \qquad \textbf{(A6)}$$

According to condition ii), we then have

$$|\tilde{F}(\omega)| < 8 \ . \qquad \textbf{(A7)}$$

$$|F(\omega)| < 2 \ . \qquad \textbf{(A8)}$$

Using formula (5), A5, A6, A7 and A8, we have $-3 < \alpha < -1.2$.