A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters

Xiaoyun Wu, Junquan Hu, Zhixiong Gu, Jiwu Huang (contacting author)

School of Information Science and Technology
Sun Yat-Sen University
Guangzhou, 510275, P. R. China.

isshjw@zsu.edu.cn

Abstract

Semi-fragile watermark fragile to malicious modifications while robust to incidental manipulations is drawing many attentions in image authentication. However, watermark security has not received enough attention yet. Lifting scheme can construct second generation wavelets. With regard to the first generation wavelets, its implementation is easier, simpler and faster than the Mallat algorithm. In this paper, we propose a novel semi-fragile watermarking scheme for image authentication based on integer wavelet transform with parameters. The features of the proposed scheme are as follows: i) Parameterized integer wavelet transform is constructed. The wavelet base is chosen by a parameter and thus guarantees the security of the watermark. ii) The performance of the generated watermark is improved and the computation complexity is reduced due to the proposed framework of parameterized integer wavelet transform using lifting scheme. iii) The watermark can tolerate JPEG lossy compression as low as quality of 40% while locate the tampered area accurately. To our best knowledge, such performance to resist JPEG compression for semi-fragile watermarking has not been reported in the literature. Experimental results show that the proposed scheme can guarantee the safety of the watermark and locate the tamper area accurately when the image has been suffered from malicious tamper while tolerating JPEG lossy compression to a large extent.

Keywords: Semi-fragile watermark, Watermark security, Image authentication, Integer wavelet transform, Parameterization;

1 Introduction

With the rapid development of internet, digital media has been widely distributed on the network recently. It leads to an acute need for media authentication because such digital content can be easily edited or modified by certain software or tools. As a new solution for content authentication, digital watermarking, is drawing considerable attention and becomes an active research field.

Digital watermark can be classified as robust watermark, fragile watermark and semi-fragile watermark (Cox and Miller 2002). The robust watermark survives when the watermarked digital content is severely attacked and thus can be applied in copyright protection. On the other hand, the fragile watermark will be destroyed even if the change in the marked digital media is minute. By reason of this property, image authentication becomes a prospective application of it. As a tradeoff of robustness and fragility, semi-fragile watermark that can resist "content preserving" operations (such as JPEG compression) and be sensitive to "content altering" transforms (such as feature replacement) is more practicable than fragile watermark in image authentication.

Fragile or semi-fragile watermarking schemes based on conventional DWT have been reported during the last few years. Kundur et al. (1998) embedded watermark in the selected wavelet coefficients by quantization. Tamper detection at multi-resolution had been achieved. But it violates the nature of the human visual system (Watson et al. 1997). It brings perceptible distortion to the watermarked images. Inoue et al. (2000) embedded fragile watermark by threshold and quantize wavelet coefficients at the coarser scales and gave a measurement for tamper proofing. Yu et al. (2000) modeled the DWT coefficient's changes caused by tamper as Gaussian distribution. Malicious tamper has large variance while incidental tamper has small variance. They embedded mark based on modulating the mean of some coefficients instead of individual coefficients.

Most conventional DWT based fragile or semi-fragile watermarking schemes reported in the literature have three shortcomings: (1) Insecurity. The schemes used only one wavelet base to perform the DWT. Once the algorithm was stolen by an attacker, the hidden information bits may be exposed or changed easily. (2) Low robustness to JPEG. (3) High computational complexity. Compared to DCT (discrete cosine transform), conventional DWT has less computational cost. But in the case of images having large size, it is still a problem when DWT applied to a whole image.

To improve watermark security, Kundur used a random triple to select the embedding region, but it may weaken the ability to tamper detection and tamper location. A feasible method to enhance security is to choose a wavelet base from a set of appropriate wavelet bases by parameters. If the parameter space is large enough, it is impossible for the attacker to get the useful information thus guarantees an extra security. Based on the idea, Meerwald and Uhl (2001) proposed for the first time to use the parameterized wavelet transform in fragile watermarking. However, his scheme is still based on conventional DWT.

Lifting scheme is an effective method to improve the processing speed of DWT. Integer wavelet transform allows to construct lossless wavelet transform which is important for fragile watermarking. By lifting scheme, we can construct integer wavelet transform.

In this paper, we will address the secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters. It incorporates parameters and integer wavelet transform based on lifting scheme to achieve the security and lower computational complexity. The semi-fragile watermarking algorithm is presented by applying the parameterized wavelets. Experimental results show that the proposed scheme can guarantee the safety of the watermark and locate the tamper area accurately when the image has been suffered from malicious tamper while tolerating JPEG lossy compression to a large extent and is effective for image authentication.

The paper is organized as follows. In section 2, we review lifting scheme briefly and then adopt a special scheme to parameterize the conventional 9-7 biorthogonal filter bank by using lifting. Based on it, parameterized integer wavelet transform is constructed. 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 explain the security and efficiency of the proposed scheme. In section 5, we report the experimental results. Finally, conclusions are drawn in section 6.

2 Parameterized Integer Wavelet Transform

Cohen et al. (1992) proposed a novel technique named lifting scheme to construct fast and concisely transform steps for wavelet transform. From then on, lifting scheme has been received more and more attention as it can offer not only fast transform, but "you can construct your owner wavelet in home " (Sweldens and Schrder 1996). Theoretically, lifting scheme is designed based on matrix algebra theory and phase filter bank theory such as perfect reconstructed filter bank theory. Generally speaking, lifting scheme includes three steps that are splitting, prediction and update (Daubechies and Sweldens 1998).

It has turned out that every FIR wavelet or filter bank can be decomposed into lifting steps (Daubechies and Sweldens 1998). The number of lifting steps is bounded by the length of the original filters. It is important to point out 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.

We give an example of the Lifting of CDF 9-7 biorthogonal wavelet (Daubechies and Sweldens 1998) that will be mentioned in the following text. To a prefixed one dimension signal $\{x_l\}_{l\in Z}$, the lifting steps are described as following:

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

$$\begin{cases} d_l^{(2)} = d_l^{(1)} + \gamma(s_l^{(1)} + s_{l+1}^{(1)}) \\ s_l^{(2)} = s_l^{(1)} + \delta(d_l^{(2)} + d_{l-1}^{(2)}) \end{cases} \qquad \begin{cases} s_l = \zeta\, s_l^{(2)} \\ d_l = d_l^{(2)} / \zeta \end{cases} \tag{2}$$

α= -1.586134342; β=-0.05298011854; (3)
γ=0.8829110762;δ=0.4435068522; ζ=1.149604398

Where s_l and d_l are commonly referred to as lower frequency and detail coefficients, respectively. $S^{(i)}{}_l$,$d^{(i)}{}_l$(i=0,1,2) are mid-outputs.

The parameterized procedure is guaranteed by theory. For the sake of brevity, we will not describe the theory in detail here. Interested readers may refer to Zhong et al. (2001) for more detailed description. The main idea is to make lifting steps not depend on those five parameter shown in Equations (1), (2) and (3), but depend on only one parameter α. Perfect reconstructed filter bank theory is used to limit the rational region of α. The formulae that use α to express the rest of parameters are list bellow:

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

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

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

where $\{h_4, h_3, h_2, h_1, h_0, h_1, h_2, h_3, h_4\}$ and $\{g_3, g_2, g_1, g_0, g_1, g_2, g_3\}$ are low pass and high pass filter banks, respectively.

The value of parameter α should not be chosen arbitrary. Because we have to insure that the corresponding filter banks achieve perfect reconstruction. Hence a rational parameter means it can be used for a perfect reconstruction biorthogonal filter bank. In Zhong et al. (2001) however, the parameter's rational range is not discussed. According to the conditions listed in Zhong et al. (2001), we have derived a rational range for the parameter α by analyzing, which is (-3, -1.2).

According to integer wavelet transform theory

(Calderbank et al. 1998), we can construct parameterized integer wavelet transform based on the framework mentioned above. That is:

$$
\begin{cases} s_l^{(0)} = x_{2l} \\ d_l^{(0)} = x_{2l+1} \end{cases}
$$

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

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

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

$$
\begin{cases} d_l^{(4)} = d_l^{(3)} + Int((\zeta - 1)s_l^{(3)}) \\ s_l^{(4)} = s_l^{(3)} + d_l^{(4)} \end{cases} \tag{7}
$$

$$
\begin{cases} s_l = s_l^{(4)} \\ d_l = d_l^{(4)} \end{cases}
$$

where $Int(x)$ means take integer part of x. Replacing parameter β, γ, δ, ζ by α by Equation (4),we then have parameterized integer wavelet transform. The Equation (7) is extra lifting step difference from Equation (1), (2). The aim is to use extra two lifting step to integer the last formula in Equation (2) since it is impossible to achieve reversible transform by integer it directly.

3 The Proposed Scheme

3.1 Watermark Preprocessing

A meaningful binary image was chosen as a watermark in this paper. It should be preprocessed before embedding because the attacker can easily forge a watermark if he has the knowledge of it.

Let digital watermark W be a binary image of size $M \times N$, and PN be a binary pseudorandom matrix of size $M \times N$ generated by a secret key k.

The binary image W and binary pseudorandom matrix PN are represented as

$$
W = w(i,j) \qquad (1 \le i \le M,\ 1 \le j \le N) \tag{8}
$$

where $w(i,j) \in \{0,1\}$.

$$
PN = p_n(i,j) \qquad (1 \le i \le M,\ 1 \le j \le N) \tag{9}
$$

where $p_n(i,j) \in \{0,1\}$.

We adopt formula (10) to get the ultimate watermark W^*:

$$
W^* = W \oplus PN \tag{10}
$$

Where $\oplus$ denotes the exclusive OR.

3.2 Watermark Embedding

Suppose that an image is decomposed by K-level IWT (integer wavelet transform). It produces 3*K detail subbands and a low frequency subband LL_K. Compared to other detail subbands, the coefficients in LL_K subband have the following features: (1) They will be well preserved after common signal processing such as JPEG compression. (2) They have larger perceptual capacity so as to ensure invisibility of the watermarked image after embedding a certain strength watermark. Therefore, for the sake of semi-fragile watermark, LL_K subband was the proposed embedding region.

We use the following formula (Liu et al. 2002) to embed the watermark W^* in the LL_3 subband coefficients.

Let $C\_LFB(a)$ denote the five least significant bits of a, $R\_LFB(a,b)$ represent the substitution of b for the five least significant bits of a.

When $w^*(i,j)$ =0, formula (11) was adopted.

$$
f^*(i,j) = \begin{cases} R\_LFB(f(i,j) - 01000b, 11000b) & C\_LFB(f(i,j)) \le 01000b \\ R\_LFB(f(i,j), 11000b) & \text{otherwise} \end{cases} \tag{11}
$$

When $w^*(i,j)$ =1, formula (12) was adopted.

$$
f^*(i,j) = \begin{cases} R\_LFB(f(i,j) + 10000b, 01000b) & C\_LFB(f(i,j)) \ge 11000b \\ R\_LFB(f(i,j), 01000b) & \text{otherwise} \end{cases} \tag{12}
$$

where $f(i,j)$ is a IWT coefficient in the LL_3 subband before embedding, $f^*(i,j)$ is the IWT coefficient after embedding and $w^*(i,j)$ is a watermark bit of W^*. Performing an inverse IWT on the modified wavelet coefficients, we get a watermarked image.

Although the difference of IWT coefficients before and after embedding varies from -15 to +16, watermarked image is still perceptually invisible.

3.3 Watermark Extraction

The extraction procedure includes the following step:

1. Three-level IWT is operated on the possible marked image. Let $f^*'(i,j)$ denote an IWT coefficient in the LL_3 subband.
2. Let $w^*'(i,j)$ denote the extracted watermark bit, $LFB(a)$ denote the five least significant bits of a, we do the following:

$$
w^*'(i,j) = \begin{cases} 1 & LFB(f^*'(i,j)) = 0 \\ 0 & LFB(f^*'(i,j)) = 1 \end{cases} \quad (1 \le i \le M, 1 \le j \le N) \tag{13}
$$

3. To acquire the ultimate watermark (a binary image), equation (14) is required.

$$
w'(i,j) = w^*'(i,j) \oplus p_n(i,j) \quad (1 \le i \le M,\ 1 \le j \le N) \tag{14}
$$

Note that this is an oblivious watermark, because it can be extracted without knowledge of the original image.

3.4 Tamper Detection

We express the difference mark as (15):

$$
D(i,j) = \left| w(i,j) - w'(i,j) \right| \quad (1 \le i \le M,\ 1 \le j \le N) \tag{15}
$$

If $D(i,j)$ =1, then the pixel in the difference binary image is white and represents mark extraction error. Contrarily, it is black and represents accurate mark extraction.

Two types of evaluation are given for tamper detection in this paper. They are subjective evaluation and objective evaluation, respectively. Both of them obey the following assumption: In the case of incidental attack, most of the watermark error pixels are isolated on the difference image or the extracted watermark. On the contrary, most of the watermark error pixels are gathered together with high probability.

On the basis of the assumption mentioned above, by observing the difference image or extracted watermark, we can judge approximately the tampered area, degree of tamper and distinguish between malicious attack and incidental attack. We call it subjective evaluation. To be objective, a quantitative method is given as follows:

For a mark error pixel in the difference image, it is a dense pixel if at least one of its eight neighbor pixels is a mark error pixel, and a sparse pixel otherwise. Thus, we have the following parameters.

$$area_{dense} = \{\text{The total of dense pixel of LL subband}\}. \quad (16)$$

$$area_{sparse} = \{\text{The total of sparse pixel of LL subband}\}. \quad (17)$$

$$area = \{\text{The total pixel of LL suband}\}. \quad (18)$$

$$area_{total} = area_{dense} + area_{sparse}. \quad (19)$$

$$\lambda = \frac{area_{total}}{area}; \qquad \delta = \frac{area_{dense}}{area_{total}}. \quad (20)$$

Now, we define the following rules to judge whether a modification is malicious or incidental:

1. If $\lambda = 0$, then the tested image is not altered.
2. If $\lambda > 0$ and $\delta < \alpha$, where the threshold is selected carefully. Generally, we fix it between 0.5 and 1. Then the tested image encountered only incidental distortions.
3. If $\delta \geq \alpha$, then the tested image is maliciously tampered.

Such objective evaluation can give accurate result when marked image encounters only incidental attack or malicious attack, whereas accuracy decreases when it is mild compressed first and then tampered slightly. For example, a watermarked image is compressed by 70% JPEG and then was drawn a little line on it. It is undoubtedly a malicious modification while incidental attack is given by objective evaluation.

To improve accuracy of tamper detection, the method that combined subjective evaluation with objective evaluation is recommended in this paper. By subjective evaluation, accurate result was given when encountering mild incidental attack and then malicious tampered. With respect to acute incidental attack and then malicious attack, it is the objective evaluation's work.

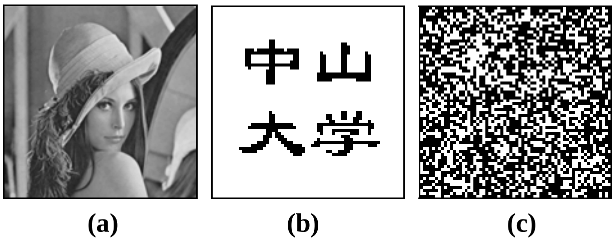
4 Performance analysis

4.1 Security

Kerckhoff's assumption for encryption techniques states that the security of a system must lie in the choice of a key, not the algorithm used to encrypt the data. It is also applicable to the security of digital watermark.

In our proposed scheme, it is computationally infeasible to acquire the correct secret key *k* and the exact embedding parameter simultaneously. The reasons are as below:

1. The watermark we select is of size 64×64. So we can generate 2^{4096} different binary pseudorandom matrices. It makes a large key space. A would-be attacker who tries to get the key is very difficult.
2. Fig.1 is an illustration of watermark extraction by using different parameters. The parameter used to embed the mark is –1. 5000000, and the parameter –1. 5000000 and –1.5000001 are used to extract the mark, respectively. Without the correct parameter, the extracted mark is similar to Gaussian white noise. It demonstrates that our scheme is sensitive to parameter's mild change, and hence it is secure. It is vain for the attackers to get some useful information about the original watermark without knowing the exact parameter. Furthermore, the rational range of the parameter is (-3, -1.2). There are infinitely many real numbers of rational parameters in it. Hence, the attack by exhaustive searching the exact parameter is unpractical.



(a) (b) (c)

Fig.1. Security. (a) Watermarked image (α=-1.5000000 for embedding). (b) Extracted mark with correct parameter (α=-1.5000000). (c) Extracted mark with different parameter (α=-1.5000001).

4.2 Computational Complexity

We examine the time that is taken in one whole procedure of embedding and extracting mark signal to depict the computational complexity.

As we mentioned in Section 1, 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 $O(n \cdot \log(n))$, respectively. In the proposed scheme in this paper, the parameterized integer wavelet transform is constructed by using lifting scheme. To 9-7 conventional DWT, 14 floating-point additions and 16 floating-point multiplications should be used per two wavelet coefficients, while for our parameterized integer wavelet transform, only 12 integer additions, 7 floating-point multiplications and 7 round-off operations are needed. Hence 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 Experiments and 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. The embedding parameter α is -1.5. The PSNR of the watermarked images are 42.26dB and 42.11dB respectively, as shown in Fig.2. The watermarks are perceptually invisible. Fig.3 (a) shows that the extracted watermarks from the marked image compressed by JPEG at different quality factor by using our scheme. We can see that the proposed scheme can resist as low as 40% JPEG compression, while the case with quality less than 40% should be considered as serious distortion. In order to prove the performance of the proposed scheme, we compare its robustness to JPEG with Hu et al. (2002). Fig.3 (b) is the result of Hu et al. (2002). Obviously, our scheme is more efficient than Hu et al. (2002) in considering robustness to JPEG compression. Experiments are done on testing the fragility to malicious tamper and the capacity to locate the tamper areas under malicious tamper (as showed in Fig.4). Without any question, we have detected the tamper and accurately located the tampering region.

6 Conclusions

A secure semi-fragile watermarking for image authentication based on parameterized integer wavelet transform has been proposed. It is highly secure and efficient due to the combination of parameter and integer wavelet transform using lifting scheme. To improve the accuracy in tamper detection, a method that incorporates subjective evaluation with objective evaluation is addressed in this paper. Experiment results have demonstrated that the proposed algorithm is capable of accurate tamper detection when the image has been suffered from malicious tamper while tolerating JPEG lossy compression to a large extent and it is sensitive to the change of parameter.

Our future research will focus on how to enhance the sensitivity to parameter's change.

Acknowledgments

This work is supported by NSFC (60325208, 60172067, 60133020, 60403045), NSF of Guangdong (04205407), Funding of China National Education Ministry.

7 References

Calderbank, R., Daubechies, I., Sweldens, W. and Yeo, B.L. (1998): Wavelet transforms that map integers to integers. *Journal of Applied and Computational Harmonic Analysis*, (5):332-369.

Cohen, A., Daubechies, I. and Feauveau, J.C. (1992): Biorthogonal bases of compactly supported wavelets. *Common Pure and Applied Mathematics*, XLV:485-560.

Cox, I.J. and Miller, M.I. (2002): The first 50 years of electronic watermarking. *Journal of Applied Signal Processing*, (2):126-132.

Daubechies, I. and Sweldens, W. (1998): Factoring wavelet transforms into lifting steps. *Journal of Fourier Analysis*, 4(3):245-267.

Hu, J.Q., Huang, J.W., Huang, D.R. and Shi, Y.Q. (2002): Image fragile watermarking based on fusion of multi-resolution tamper detection. *Electronics Letters*, 38(24):1512-1513.

Inoue, H., Miyazaki, A. and Katsura, T. (2000): Wavelet-based watermarking for tamper proofing of still images. *Proc. Int. Symposium on Image Processing*, (2): 88-91.

Kundur, D. and Hatzinakos, D. (1998): Towards a telltale watermark techniques for tamper-proofing. *Proc. of the IEEE Int. Conf. on Image Processing (ICIP)*, Chicago, (2):409-413

Liu, H.M., Liu, J.F., Huang, J.W., Huang, D.R. and Shi, Y.Q. (2002): A robust DWT-based blind data hiding algorithm. *Proc. of IEEE on Circuits and Systems*, (2):672 - II-675.

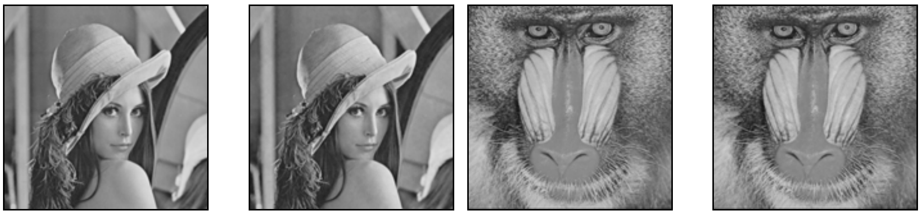
Meerwald, P. and Uhl, A. (2001): Watermark security via wavelet filter parametrization. *Proc. IEEE Int. Conf. on Image Processing*, (3):1027-1030.

Sweldens, W. and Schrder, P. (1996): Building your own wavelets at home. *Wavelets in Computer Graphics*, 1996:15-87, ACM SIGGRAPH Course Notes.

Watson, A.B., Yang, G.Y., Solomon, J.A. and Villasenor, J. (1997): Visibility of wavelet quantization noise. *IEEE Trans. Image Processing*, 8(6):1164-1175.

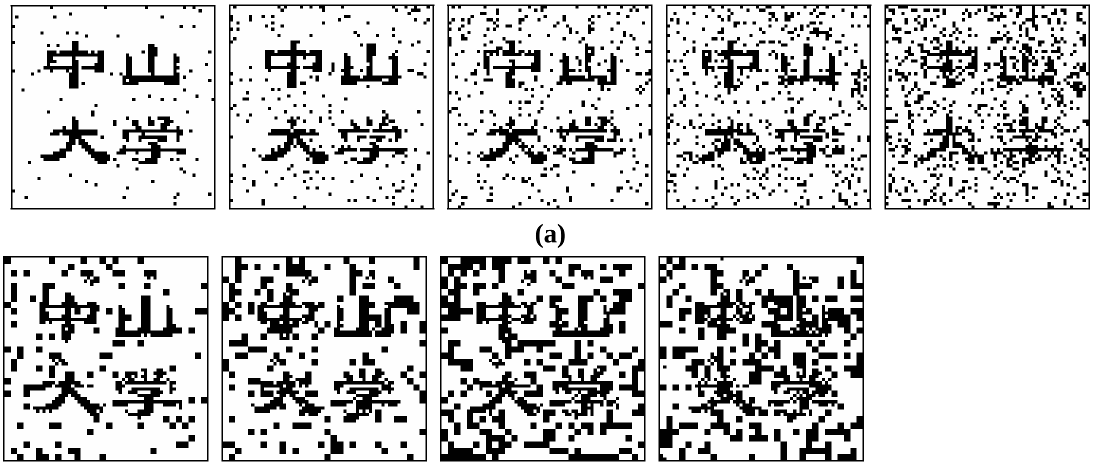
Yu, G.J., Lu, C.S., Liao, Y.M. and Sheu, J.P. (2000): Mean quantization blind watermarking for image authentication. *Proc. IEEE Int. Conf. on Image Processing*, Vancouver, Canada, III:706-709.

Zhong, G.J., Cheng, L.Z. and Chen, H.W. (2001): A simple 9/7-tap wavelet filter based on lifting scheme. *Proc. of ICIP*, 2:249-252.



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

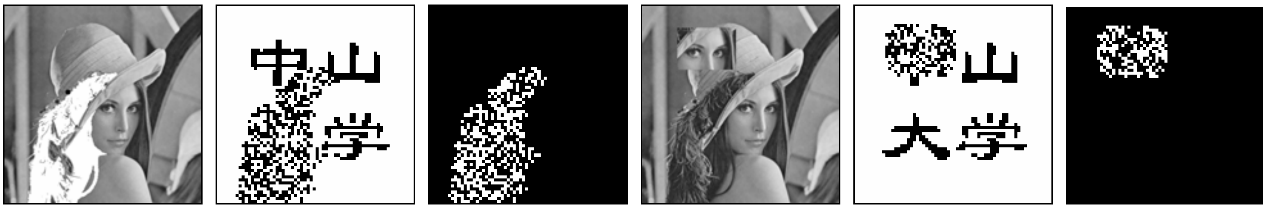
Fig.2. Invisibility. (a), (c) The original Lena and Baboon images. (b) The watermarked Lena image (42.26 dB). (d) The watermarked Baboon image (42.11 dB).



(a)

(b)

Fig.3. The mark extracted from the watermarked image compressed by JPEG with different quality factor. (a) Our scheme. (80%, 70%, 60%, 50%, 40%). (b) Hu et al. (2002). (80%, 70%, 60%, 50%).



(a) (b) (c) (d) (e) (f)

Fig.4: Tamper detection (a),(d) Tampered image. (b),(e) Tampered watermark. (c),(f) Difference image.