IMPROVE SECURITY OF FRAGILE WATERMARKING VIA PARAMETERIZED WAVELET

Jiwu Huang[1], *Junquan Hu*[1], *Daren Huang* [1], *Yun Q. Shi* [2]

1. Dept. of Electronics, Sun Yat-Sen University, Guangzhou 510275, P. R. China
2. Dept. of ECE, New Jersey Institute of Technology, NJ 07102, USA.

ABSTRACT

The security is an important issue in watermarking. It has not, however, received enough attention yet. In this paper, we propose a secure fragile watermarking algorithm based on parameterized integer wavelet transform, and the rational range of the parameter is derived theoretically. Without the parameter of the wavelet base used for watermarking, it is hard for attacker to recover or attack the hidden watermark. Multi-resolution tamper detection is developed for the accurate detection. Both security and lower computational complexity of the generated fragile watermark are achieved.

1. INTRODUCTION

Fragile watermarking has received more and more attentions as it allows placing an imperceptible watermark in multimedia data to authenticate the data's originality and integrity. An effective fragile watermarking scheme should be [1]: 1) Perceptual invisibility; 2) Ability to detect and locate the tampered regions while tolerating JPEG lossy compression; 3) Security of the watermark.

Though some fragile watermark techniques have been reported in recent years, security of watermarks present many challenges [2-4]. Most of existing wavelet-based fragile watermarking schemes, however, have not considered the security issues. These schemes used only one wavelet base to perform the DWT (discrete wavelet transform) and hence, serious danger will be encountered. For example, the hidden information bits may be extracted or changed easily. On the other hand, the conflict between the ability to detect the tamper and the ability to tolerate JPEG has not been solved.

In this paper, we propose a secure semi-fragile image watermarking algorithm based on parameterized integer wavelet transform. The security of the watermark is enhanced by applying parameterized integer wavelet transform. A framework of parameterized integer wavelet transform is presented primarily by using lifting scheme. Then the fragile watermarking algorithm is proposed by applying the parameterized wavelets. Without the exact parameter, it is hard to recover and hence attack the hidden watermark. The integer wavelet transform also lower the bit error rate in watermark extraction caused by the float point operations associated with the conventional DWT/IDWT and reduce the computational complexity.

Multi-resolution tamper detection and image fusion are applied to watermark detection. To distinguish between incidental and malicious modifications, some effective rules are presented. The watermark with the proposed algorithm can detect any malicious tampers and locate the tampered regions accurately while tolerating high quality lossy image compression, say, higher than 80% of quality.

2. THE PROPOSED WATERMARKING

2.1 Parameterized Integer Wavelet Transform

A potential method to enhance the security of fragile watermarks is to adopt a set of wavelet bases instead of only one wavelet base. It makes mark embedding and extraction more secure since the attacker does not know which wavelet base has been adopted. If the space of the wavelet bases for choosing is large enough, it is difficult for attacker to find the exact base to recover the hidden information bits. Parameterized wavelet transform provides a way to construct such a space as it collects a set of wavelet bases controlled by the parameters. Meerwald [5] proposed for the first time to use the parameterized wavelet transform in fragile watermarking. However, his scheme is still based on the conventional DWT.

Moreover, integer wavelet transform allows constructing lossless wavelet transform in practical applications. Though theoretically, the wavelet transform is lossless, we cannot achieve lossless DWT/IDWT due to the finite precision in computation. Being lossless is important for fragile watermarking since it introduces feeble modification to the image, while the conventional DWT may result in some errors in watermark extraction.

The lifting scheme [6] provides an effective way to construct integer wavelet transform. 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: splitting, prediction, and update.

Supported by NSFC (60325208, 60172067, 60133020), Funding of China National Education Ministry.

It has turned out that every FIR wavelet or filter bank can be decomposed into lifting steps [7]. 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.

The follow is an example of the lifting of CDF 9-7 biorthogonal wavelet [7]. The reason to enumerate this example is to compare the especial lifting framework 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:

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

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

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

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. Interested readers may refer to [8] 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 to use α to express the other parameters are as follows:

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

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

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 ensure that the corresponding filter banks achieve perfect reconstruction. Hence a rational parameter means it can be used for a perfect reconstruction of biorthogonal filter bank. In [8], however, the parameter's rational range is not discussed. We have derived a rational range for the parameter α theoretically, which is (-3, -1.2).

According to integer wavelet transform theory, we can construct parameterized integer wavelet transform based on the framework mentioned above. That is:

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

$$\begin{cases} d_l^{(2)} = d_l^{(1)} + Int(\gamma(s_l^{(1)} + s_{l+1}^{(1)})) \\ s_l^{(2)} = s_l^{(1)} + Int(\delta(d_l^{(2)} + d_{l-1}^{(2)})) \end{cases}, \quad \begin{cases} d_l^{(3)} = d_l^{(2)} + Int((\zeta - \zeta^2)s_l^{(2)}) \\ s_l^{(3)} = s_l^{(2)} + Int((-1/\zeta)d_l^{(3)}) \end{cases}$$

$$\begin{cases} d_l^{(4)} = d_l^{(3)} + Int((\zeta - 1)s_l^{(3)}) \\ s_l^{(4)} = s_l^{(3)} + d_l^{(4)} \end{cases}, \quad \begin{cases} s_l = s_l^{(4)} \\ d_l = d_l^{(4)} \end{cases} \tag{6}$$

where $Int(x)$ means taking integer part of x. Replacing parameter β, γ, δ, ζ using α by Equation (4), we then have parameterized integer wavelet transform. Equation (6) contained extra lifting steps from Equation (1), (2), aiming at achieving wavelet transform.

2.2 Watermark Embedding

In our work, the watermark is a binary logo. For multi-resolution tamper detection and convenience to embed, we construct an image pyramid of the logo by resolution reduction. The resolution reduction scheme suggested by JBIG is adopted in this paper. In this way, we generate the pyramid structure of the watermark, denoted as $\{W_l, l=1,2,\ldots L\}$.

The integer wavelet transform is applied to the original image by using a predefined parameter. Denote the wavelet coefficients of all HH sub-bands as $f_l(i,j)$. We can calculate:

$$Q_{i,j} = \begin{cases} 0 & if\ \lfloor f_l(i,j)/(2l) \rfloor\ is\ even \\ 1 & if\ \lfloor f_l(i,j)/(2l) \rfloor\ is\ odd \end{cases} \tag{7}$$

Different from [9], we only embed one bit into a coefficient. Let $W_l(i,j)$ denote the current mark bit to embed. The coefficients are modified as:

$$\tilde{f}_{k,l}(i,j) = \begin{cases} f_l(i,j) & Q_{i,j} = W_l(i,j) \\ (\lfloor f_l(i,j)/(2l) \rfloor \pm 1.5) \cdot 2l & Q_{i,j} \neq W_l(i,j) \end{cases} \tag{8}$$

where the choice of "+" or "–" is determined by the sign of $f_l(i,j)$. Positive is "+", and otherwise, "–". Finally, inverse integer wavelet transform is applied to the

modified DWT coefficients to obtain the watermarked image.

2.3 Watermark Embedding

In watermark extraction, L-level integer wavelet transform with the same parameter is performed on the possible marked image firstly. Denoting the all HH sun-bands coefficients as $f'_l(i,j)$, the extracted watermark can be expressed as:

$$W'_l(i,j)=\begin{cases}0 & if\ \lfloor f'_l(i,j)/(2l)\rfloor\ is\ even\\ 1 & if\ \lfloor f'_l(i,j)/(2l)\rfloor\ is\ odd\end{cases} \quad (9)$$

Then, calculate the difference image:

$$D_l(i,j)=\left|W_l(i,j)-W'_l(i,j)\right| \quad (10)$$

The pixel with value 1 is black in difference image, and white, otherwise. Hence, we can use difference image to determine whether or not tamper has happened. The tamper region can also be located accurately.

The idea of fragile authentication is similar to that of our previous work [9], where we applied 9-7 conventional DWT and the threshold deduced by Watson [10] to embed mark signal. In this paper, we utilize nonlinear integer wavelet transform, hence the threshold must be re-chosen carefully. Another reason to change the threshold is that the coefficients' change caused by the mild change of parameter α is not large. So, large threshold will make it undetected, while in practical applications, the watermark must be fragile to the parameter's mild change in order to enhance the security of watermarking scheme. Our experiments have shown that there still has change not less than 7 in wavelet transform coefficients while the change of parameter has been decreased to even smaller than 10^{-6}. It means a large numbers of parameters are rational for being chosen to fragile watermarking. Another experiment was also carried out for determining the threshold. It is observed that the change caused by parameter change is linear to the changes of resolution levels. Suppose that the level number of wavelet decomposition, denoted as L, to be 3, the experiment illustrates that if the mean change value is Δ in HH_1, then 2Δ, 3Δ in HH_2 and HH_3, respectively. The cases in HL and LH sub-bands are similar to that in HH sub-band. Hence, we just use $2l$ as the threshold instead of Watson's threshold used in [9], where l is the level of resolution with l=1,2,…L.

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

i) If $\lambda_l = 0$ for every resolution level $l \in [1,2,3,....,L]$, then the tested image is neither maliciously tampered nor incidental distorted.

ii) If there exists some $l \in [1,2,3,....,L]$, such that $\lambda_l > 0$ and $\delta_l \le \alpha$, where the threshold is selected carefully. Generally, we fix it between 0.5 and 1. Then the tested image encountered only incidental distortions.

iii) If $\delta_l > \alpha$ for each $l \in [1,2,3,....,L]$, then the tested image is maliciously tampered.

where

$area_{l,dense}$={The total of dense pixel}.

$area_{l,sparse}$ ={The total of sparse pixel}.

$area_{l,total}$= $area_{l,dense}$ + $area_{l,sparse}$.

$area_l$= {The total pixel of channel l}.

$$\lambda_l=\frac{area_{l,total}}{area_l},\quad \delta_l=\frac{area_{l,dense}}{area_{l,total}}$$

3. EXPERIMENTAL RESULTS

We tested the security and the fragility to parameter change of the proposed scheme on a few images with different texture. The experiments reported here are on Lena of 256×2568×8 bits. The original image and the watermarked image with the PSNR of 43.2 dB are shown in Fig. 1(a) and (b). We cannot find out any perceptible difference between the original and the marked images. Fig.1 (c) ~ (g) are the illustrations of the proposed scheme's ability to detect malicious tamper. Fig.1 (c) and (e) show the tampered watermarked images with hair brightened and the image content in the rectangle replaced, respectively. The corresponding extracted watermarks are in Fig. 1 (f) and (g). Without any question, we have detected the tamper and accurately located the tampering region. The watermark can tolerate JPEG compression with higher than 80% of quality. Fig. 1(h) is an illustration of watermark extraction by using different parameters. The parameter used to embed the mark is –1.5, and the parameter –1.5000001 is used to extract the watermark. From the extracted watermark, distributed randomly, we cannot get any useful information about the original watermark. It demonstrates that our scheme is sensitive to parameter's change, and hence it is secure. It is ineffective to use different parameter to attack our scheme. It is noted that we only give the watermarks after the fusion due to the limitation of length.

(a) (b)

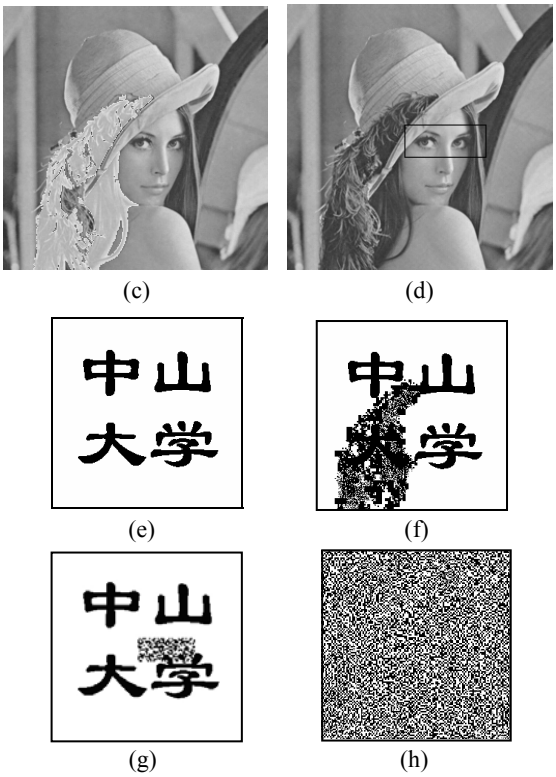

Fig. 1. Experimental Results. (a) The original Lena image. (b) The watermarked Lena image (43.2 dB). (c) The tampered image with hair brightened. (d) The tampered image with the content in the rectangle replaced. (e) The original watermark. (f) The extracted watermark from (c). (g) The extracted watermark from (d). (h) The extracted watermark from (b) with different parameter (α=-1.5 for embedding and α=-1.5000001 for extracting)

4. CONCLUSIONS

In this paper, we embed fragile watermark based on parameterized integer wavelet transform. The features of proposed algorithm are as follows:

i) A framework of parameterized integer wavelet transform for fragile watermarking is presented using lifting scheme. Moreover, the rational range of the parameter is derived. To our best knowledge, there has not been similar report in literature.

ii) A fragile watermarking scheme is proposed under the framework of parameterized integer wavelet transform. The experimental results have demonstrated that the proposed algorithm is capable of accurate tamper detection while being robust to c certain degree of JPEG. The extracted watermark is very sensitive to the change of parameter, hence being very secure.

As to fragile watermarking, the main threaten comes from attackers. They want to find out the information about algorithm such as embedding regions, embedding strategy, extraction strategy and the mechanism for tamper detection. Then, a fake authenticated image can be created. To avoid such an attack, we consider security requirements carefully in the scheme. For the scheme based on the conventional DWT, the same wavelet base is applied to every marked image. If the algorithm is known to the public, the scheme is easy to be attacked. In other words, the scheme based on the conventional DWT must be kept private. This will impede the standard work of watermarking. Even though some scheme applied extra mechanism to enhance security, it is at the cost of decrease of efficiency. In this paper, we used a new parameterized integer wavelet transform to design fragile watermarking scheme. Furthermore, the experiments have demonstrated that our scheme is fragile to parameter's mild change. Specifically, our experimental work has shown that the average wavelet coefficients will change larger than 7 with the change of the parameter α to be smaller than 10^{-6}. Hence, it is vain for the attackers to get some useful information about the original watermark without knowing the exact parameter. The rational range of the parameter is (-3, -1.2). There are infinitely many numbers of rational parameters in this range. Hence, the attack by exhaustive searching the exact parameter is unpractical.

7. REFERENCES

[1] J. Fridrich, "Methods for tamper detection in digital images," *Proc. ACM Workshop on Multimedia and Security*, 1999, pp.19-23

[2] F. Deguillaume, S. Voloshynovskiy, T. Pun, "Secure hybrid robust watermarking resistant against tampering and copy attack," *Signal Processing*, 2003, 83 (10): 2133-2170.

[3] M.U. Celik, G. Sharma, E. Saber, A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. on Image Processing*, 2002, 11 (6): 585-595.

[4] G. J. Yu, C. S. Lu, H. Y. M. Liao, "Mean-quantization-based fragile watermarking for image authentication," *Optical Engineering*, 2001, 40 (7): 1396-1408.

[5] P. Meerwald, A. Uhl, "Watermark Security Via Wavelet Filter Parametrization," *Proc. IEEE ICIP*, 2001, vol. 3, pp.1027-1030.

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

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

[8] G. Zhong, L. Cheng, H. Chen, "A simple 9/7-tap wavelet filter based on lifting scheme," *Proc. IEEE ICIP*, 2001, vol. 2, pp. 249-252

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

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