Watermarking Still Images Using Parametrized Wavelet Systems

Zhuan Qing Huang and Zhuhan Jiang

School of Computing and IT, University of Western Sydney, NSW 2150, Australia zhuang@cit.uws.edu.au, z.jiang@uws.edu.au

Abstract: We propose a wavelet-based watermarking scheme by dynamically constructing the filters embedded with the watermark as well as potentially the private key patterns associated with the individual images. This scheme explores the watermark dissemination in a non-traditional dimension, allows the dual purpose of the embedded data as either watermarks or private keys, and offers additional analysis and optimization through the dynamic filter choices. We also propose an additional systematic watermark detection scheme in terms of a *trend criterion*, which proves to be both robust and flexible. Moreover, our watermarking and detection processes are also investigated to include the defence against noises, cropping and distortions, and to include the non-availability of the original images at the detections.

Keywords: Watermarking, wavelet, image cropping

1 Introduction

Watermarking is an increasingly important technology for the copyright protection and ownership authentication for the multimedia data that flourish at the advent of the Internet. For digital still images, the purpose of watermarking is typically to hide some identity data in the host images so that the data can be later extracted, or simply tested for the existence, to demonstrate the ownership of the images. Initially concentrated mostly on the pixel domain [1,2], the study of watermarking has moved in force to the transformed domains induced by such as DCT and wavelets [1,3-5]. In particular, waveletbased transforms and algorithms gained much popularity in recent years. These include adding pseudo-random codes to the large coefficients at the high and middle frequency bands [3], storing filters as the private authentication data [4], and embedding decomposed watermarks of different resolutions into the corresponding resolution of the decomposed images [5], to name a few. In a wavelet-transformed domain, a traditional scheme will typically embed a watermark by superposing or replacing a selected subband with a signature image pattern. In this paper, however, we proposed a method that embeds watermarks, either in entirety or in part, directly into the wavelet filters that are to be dynamically constructed. This approach thus explores the watermark dissemination in a non-traditional perspective, offers more room for analysis and optimization due to the ample choices of the filters, and allows the embedded data as either watermarks or private keys. By a private key, we mean a bit pattern privately held by the owner of a particular original

image. The key needs to be produced to a legal authority in order to be able to successfully extract a watermark or test for its existence. As such, the use of a private key will better safeguard the watermarking scheme against potential watermark theft and possible collusions. Our proposed method will hence lead to the improved security, robustness as well as flexibility. In what follows, we first in section 2 introduce the technical background and our proposed watermarking strategy with detailed analysis on its feasibility and legitimacy. We will outline the watermarking process as well as the detection process that require no original images. Section 3 is then dedicated to the study of detecting watermarks that were subject to cropping or other noises or distortions. We will then conduct further watermarking experiments in section 4. Final conclusions are made in section 5.

2 Proposed Algorithm

2.1 Main strategy

It is known that wavelet filters can decorrelate signals into averages and *details* [6], and likewise can also decompose cascadingly an image into multiple levels of bands, see Figure 1 for the multiresolutional decomposition, via the following analysis

filters [7,8]



Figure 1: Multiresolutional Decomposition

$$c_{j} = \sum_{k \in Z} h_{k-2j} x_{k,}$$

$$d_{j} = \sum_{k \in Z} (-1)^{k} \overline{h}_{1-k+2j} x_{k,}$$
(1)

where Z denotes the set of all integers. The reconstruction can be done recursively in the reverse order through the repeated use of the synthesis filter

$$x_k = \sum_{j \in Z} \ \overline{h}_{k-2j} c_j + \sum_{j \in Z} (-1)^k h_{1+k-2j} d_j, \ k \in Z \quad , \qquad (2)$$



Figure 2. Decomposition



Figure 3. Reconstruction

see Figures 2 and 3. Moreover, quality filters will result in better separation or decorrelation of the details from the smoother components of the image, leaving filtered bands more generically independent of the others. We may also denote quadrants LL, HL, HH and LH by 1, 2, 3 and 4 respectively later on. For a given set of filter coefficients $\{h_i, h_i\}$, (1) uniquely characterizes the subbands. Characteristics or data embedded in such a channel band will resonantly resurface when undergone the same filters. If for each level of decomposition via (1) we utilize 1 set of filters for the horizontal passing and another for the vertical passing, we can then collect an ordered set of filters whose definition uniquely specifies the definition of the finally filtered out subband. If we replace this subband with a sorted pattern or another "landmark" pattern and synthesize all the way back to a full-sized image, then the resulting image is a watermarked image and the watermark essentially consists of all the information of the path filters and the subband replacement. We can also partition such info into 2 sets of bit patterns, with 1 set being the true watermark and the other being the private key. This way, when the private key is available, an image can be tested to see if it carries a particular watermark.

How do we embed watermarks into wavelet filters, then? If we define $A(z) = \sum_{k \in z} A_k z^{-k}$ with A_k being a 2x2 matrix of (h_{2k}, h_{2k+1}) in the 1st row and $(h_{1-2k}, -h_{2k})$ in the 2nd, then A(z) induces orthogonal wavelet filters iff A(z) admits the following factorization [6]

$$A(z) = z^{d} \begin{bmatrix} 1 & 0 \\ 0 & \sigma \end{bmatrix} R(\theta_{0}) \begin{bmatrix} 1 & 0 \\ 0 & z^{-1} \end{bmatrix} R(\theta_{1}) \dots \begin{bmatrix} 1 & 0 \\ 0 & z^{-1} \end{bmatrix} R(\theta_{q}) ,$$

$$R(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} .$$
(3)

with $\sigma = \pm 1$, $q \ge 0$, q, $d \in Z$ and $\theta_0 + \theta_1 + \ldots + \theta_q \equiv \pi/4$ (mod 2π). The θ 's can be used to carry the watermark bit patterns. We will in fact partition the θ 's into 2 subsets: one contains a predefined watermark, and the other contains a private key or can be optimized to improve the quality of filters. For a step size $\Delta \theta$, if i-th watermark bit is 1, then one of the θ_k 's should have a contribution of $2^i \Delta \theta$ if it is to contain that portion of watermark.

2.2 Design and analysis of the watermarking method

A watermarking scheme should be designed to be as robust as possible, capable of resisting to certain extent the distortions arising from such as artificial noises, cropping and lossy compression. The step size $\Delta\theta$ should be chosen so that the error due to the difference of the exact watermark and that extracted through the use of an incorrect filter coefficient with an error larger than $\Delta \theta$ should exceed clearly the difference caused by visually tolerable white noises. Hence the choice of $\Delta \theta$ is a balance between better robustness and higher storage capacity for the watermark: a larger $\Delta \theta$ leads to a more robust watermark at the cost of storing lesser watermark bits per filter. A threshold for $\Delta \theta$ will thus be first determined here by analyzing both the effect of white noises and the effect of $\Delta \theta$ at distinguishing effectively a selected subband. For this purpose, we first narrow down our algorithms to two more precise forms. The first is a simplistic approach without loss of generality, and will be termed sorting approach. The selected subband will be replaced by its sorted elements. The ordering inside the subband is thus the only feature that characterizes the existence of the watermark carried exclusively by the filter coefficients. The second approach is to replace the selected subband with a predefined pattern, which can be used as part of the watermark or simply as the indication of the watermark existence. This pattern will also be adjusted for the energy so as to improve the visual fidelity of the watermarked images. This 2nd approach will be termed pattern approach. In both approaches, we also scramble the replaced subband for extra security protection. For any vector seed S of positive integers and any vector B of subband elements, if the 1^{st} element of S is denoted by s, we first fetch the s-th element as the 1st element of the scrambled vector. We then remove the fetched element from B, move all the earlier elements in B to the bottom of B in the same order, and move the 1^{st} element of S to the bottom of S. Treat B as cyclic and repeat this process until *B* becomes empty. The resulting vector is then our scrambled vector. The choice of a scrambling seed can be random, if it is to

be used as a private key, and can also be conveniently induced by the watermark-embedded filter coefficients automatically.

To estimate a proper $\Delta\theta$ threshold, we first illustrate our analysis with the sorting approach on the Lena image of 256x256 pixels. We choose q=2 in (3), hence each filter has 2 free θ parameters. The decomposition levels are 4 and the middle frequency bands are chosen for the band replacement. We add 1-10% white noises and let θ_0 vary with $\Delta\theta=.01$. The results are summarized in Tables 1 and 2, where A-B are 2 selected typical cases for $\theta_1=.1$ or .3.

Table 1. Effect of $\Delta \theta$ in RMS ($\Delta \theta = \Delta \Theta x \ 10^{-2}$)

ΔΘ	1	2	3	4	5	6	7	8	9	10
Α	0.4	0.8	1.2	1.6	2.0	2.4	2.8	3.2	3.6	4.0
В	0.4	0.8	1.2	1.6	1.9	2.3	2.7	3.1	3.5	3.9

Table 2. Effect of noise in RMS

n%	1	2	3	4	5	6	7	8	9	10
А	0.6	1.2	1.9	2.4	3.0	3.8	4.4	4.9	5.7	6.1
В	0.7	1.4	1.9	2.6	3.4	3.9	4.3	5.4	6.1	6.5

We observe that the pattern can be easily detected when the θ 's deviation is less than 0.06, as is indicated by RMS \approx 2.4 at θ =0.06 in Table 1. On the other hand, the pattern can be properly detected when the white noises are no more than 4%, as is indicated by RMS≈2.5 in Table 2. Other decomposition paths and "landmark" patterns have also been tested and they yield similar results. Hence, if we choose 0.06 or larger for $\Delta\theta$, and ϵ =2.5 in RMS as the threshold for detection, we can say that the watermark is detectable when noises are less than 4%. In other words, a change of θ by a single $\Delta \theta$ will result in the pattern deviation of more than ε . In this test, we reserve one θ for the use of private key, and use the other free θ to carry the watermark bits. Hence the $\Delta\theta$ threshold may somewhat vary in the other regions.

Since a filter in

typically have

several free θ

parameters, we

can use all of

them to carry

bits. We can

also use one, or

some of them,

watermark

will

(3)

the



Figure 6: Fidelity effect of θ

to serve as part of a private key, or to optimize the fidelity of the watermarked images. The potential need for optimization is illustrated in Figure 6, in which we used only one θ to code the watermark "lena" and let the other θ to vary within $[0,2\pi]$. The curves "a" and "b" correspond to the Lena image watermarked with "lena" and "anel" respectively, while the curve labeled by "c" corresponds to the *Pout* image with "lena" as its watermark. The figure also shows that, with different decomposition paths, different watermarks and different images, the PSNR may gain as much as about 10 dB. Hence it is worthwhile to forfeit a parameter to optimize the fidelity when there is a need to do so. The optimized θ will eventually play the role of a private key.



Figure 7: Embedding process



Figure 8: Detection process

For the given type of filters (3) and a predefined $\Delta \theta$, the whole watermark embedding process can be summarized in Figure 7. We basically first decide what θ 's are to be used to carry watermark bits, what and if other θ 's will be used for private key or for optimization. We note that filter quality can be further improved if we impose additional vanishing moments when we have more free θ 's. This will however be partially addressed in the following subsections along with the construction of biorthogonal filters.

For the detection process, see Figure 8, we decompose the image with the filters having the watermark, and unscramble the subband of the predefined path, and then compare it with the anticipated pattern. If the corresponding RMS is smaller than the detection threshold ε , one can then

claim that the image carries the watermark. If otherwise, we can still apply the cropping test to be introduced in section 3 to further verify the watermark existence.

2.3 Biorthogonal filters

We dynamically constructed the orthogonal wavelet filters that embed the watermark as described in the above. We saw that the way to generate the filters also allows the optimization of the filters. There is however another important type of wavelet systems, the biorthogonal wavelet filters, that can also provide perfect reconstruction for the images from their corresponding smooth and detail components [7].

For an image represented by $\{x_k\}_{k \in \mathbb{Z}}$, suppose the $\{h_k\}$ and $\{\overline{h}_k\}$ satisfy the biorthogonality condition

$$\Sigma_{k\in Z} \quad \overline{h}_k h_{k+2j} = \delta_{j,0}, \qquad j \in Z \tag{4}$$

where $\delta_{l,m}$ is the Kronecker delta symbol. The filter coefficients $\{h_k\}$ and $\{\overline{h}_k\}$ will generate two subbands $\{c_j\}$ and $\{d_j\}$ via (1), and the subbands can be synthesized by the synthesis filter via (2). The biorthogonal filters will become orthogonal when h_k $\equiv \overline{h}_k$ holds for all k. We know the quality filters would highly decorrelate the image data and thus cause less reconstruction errors. One of the wavelet properties such as the number of consecutive vanishing moments will for instance result in better decorrelation for the image data.

If we let [7] $\underline{A}_k = [(h_{2k}, g_{2k})^T, (h_{2k+1}, g_{2k+1})^T]$ and likewise for \overline{A}_k , and define the discrete moments by

$$\mu_r^{(0)} = \sum k^r h_k, \qquad \mu_r^{(1)} = \sum k^r g_k, \\ \overline{\mu_r^{(0)}} = \sum k^r h_k, \qquad \overline{\mu_r^{(1)}} = \sum k^r g_k, \quad k \in \mathbb{Z}$$
 (5)

where $r \ge 0$ is an integer, ^{*T*} represents vector transposition, $g_k = (-1)^k \overline{h}_{1-k}$ and $\overline{g}_k = (-1)^k h_{1-k}$. If the vanishing moments conditions

$$\mu_r^{(0)} = 2^{1/2} * \delta_{r,0}, \qquad r = 0, \dots, N_0, \mu_r^{(0)} = 2^{1/2} * \delta_{r,0}, \qquad r = 0, \dots, \overline{N}_0, \mu_r^{(1)} = 0, \qquad r = 0, \dots, N_1, \mu_r^{(1)} = 0, \qquad r = 0, \dots, \overline{N}_1$$

$$(6)$$

are satisfied, for the signals $\{x_k\}$ sampled from any N degree polynomial, the details d_j are all zero and the average c_j are of the type of polynomial signals due to (1). So the signals of any N degree polynomial sampled at an equal step are completely decorrelated when there are sufficiently many vanishing moments [7]. Other desirable features for a wavelet system include such as linear phase and minimum reconstruction norm. For any positive integer K, suppose a pair of filters of linear phase has analysis filter with length 2K+1 and the synthesis filter with length 2K-1, so there are 2K+1 variables. For K = 3, the coefficients of the corresponding 7/5-tap filters are determined by the wavelet biorthogonality

$$h_0 h_0 + 2h_1 h_1 + 2h_2 h_2 = 1$$
,

$$\begin{split} h_0 & h_2 + h_1 & h_1 + h_2 & h_0 + h_3 & h_1 = 1 , \\ h_2 & \overline{h}_2 + h_3 & \overline{h}_1 = 0 , \\ h_0 + 2h_1 + 2h_2 + 2h_3 = 2^{1/2} , \\ \overline{h}_0 + 2 & \overline{h}_1 + 2 & \overline{h}_2 = 2^{1/2} \end{split}$$
 (7)

and the vanishing moment $\mu_0^{(1)} = 0$,

$$\overline{h}_0 - 2 \ \overline{h}_1 + 2 \ \overline{h}_2 = 0$$
 (8)

The solution of (7) and (8) subsequently reads

$$\overline{h}_{1} = 2^{1/2}/4,$$

$$\overline{h}_{2} = -2^{1/2} h_{3} / 4h_{2},$$

$$\overline{h}_{0} = 2^{1/2}/2 - 2 \overline{h}_{2},$$

$$h_{1} = -(2h_{2}^{2} + 5h_{2}h_{3} + 2h_{3}^{2} - 2^{1/2}h_{3})/(h_{2} + 2h_{3}),$$

$$h_{0} = 2^{1/2} - 2(h_{1} + h_{2} + h_{3}).$$
(9)

There are two free parameters h_2 and h_3 , which can be used to embed the watermark. As such, we could potentially use one free parameter to embed the watermark and use the other free parameter to carry a private key or further watermark bits. If the filter length increases, then more vanishing moments may be imposed to improve the filter quality. It is thus anticipated that further improvement can be achieved on the filters, which will in turn reflect on the overall watermarking performance of our proposed scheme. As an example, we set the filter step to 0.01 and watermark the image with "lena". Then the watermarked image has RMS=0.8. If the image has the watermark "anel" rather than "lena", and we still use the filter watermarked by "lena" to decompose the image, then the RMS of the resulting selected band is 12.8, which implies the image doesn't contain "lena" as the watermark. The details and expansions in this direction will however be left to our future work.

3 Detection of Cropped Image

One of the advantages of wavelet-based watermarking is its ability to spread the watermark all over the image. If a part of the image is cropped, it may still contain parts of the watermark. These parts of watermark may be detected by certain mechanism even if the image has been further scaled or rotated. Our proposed method for detecting watermark from a cropped image is as the following. Suppose an image is suspected of being cropped from a watermarked image with the watermark W. We first add white noises N to the watermarked image in full size, and assume that the noises n in the cropped image are tolerable in terms of the caused visual degradation.

We choose N such that N >> n, i.e. noises N are significantly larger than noise n. We then replace the cropped region in the full-sized image by the suspected cropped image, see Figure 9. If we extract the watermark as usual, the difference of the extracted pattern and the anticipated pattern is expected to decrease when the cropped area is replaced with the cropped image. The larger the cropped area, the more

the difference decreases. If the cropped image has no watermark W or contains a different watermark, the difference is expected to increase. If we partition the cropped image into several large enough regions, then the above trend of difference changes will also be observed. Although the precise quantitative measurement is still under investigation, this *trend criterion* is already accurate enough in all the tests we have conducted. Repeated generation of noises N for the repeated tests could also further increase the confidence of the watermark existence.



Figure 9: Patched image

For а given cropped image, to illustrate, we just divide it into 4 pieces Then equally. we add the white noises with 1% to 10% of the magnitude to the cropped image, and add white noises of

ratio 10% to the original watermarked image. The cropped image will be put back piecewise to replace the corresponding region in the watermarked image with noises N. The size of the cropped images for testing ranges from 8x8, 16x16, 32x32, 48x48, 64x64, 128x128, 192x192, to 240x240. The results for the case of 128x128 are showed in Figures 10 and 11, and are consistent with our earlier anticipation. In the case the cropped image has no specified watermark, the RMS induced from the reconstructed image increases sharply with the replacement of each additional piece of the cropped image. When the size of cropped image is larger than 48x48 (3.5% of the original) and the noise ratio in the cropped image is less than 50% of that for the watermarked image, the decreasing trend of RMS is very strong. When the noise ratio in the cropped image is larger than 50% of that in watermarked image, the trend may have occasional exceptions. However this is not a problem as this trend is still well distinguished from the sharp increasing trend of RMS of the cropped image without the specified watermark. When the size of cropped image is less than 48x48, the RMS changes are small and inconclusive. We also found the RMS for the patched image containing specified watermark is smaller than or very close to the RMS of the watermarked image with noise ratio 10%, while the RMS for the case of the cropped image without specified watermark is much larger than the RMS of the watermarked image with noise ratio 10%. This also supports well our detection scheme.

We note that the above strategy proposed for testing watermarks inside cropped images can also be applied to normal full-sized images, as in Figure 8. For the full-sized complete image, the owner can divide it into several pieces each of which is larger than the minimal detectable area.

Although the analysis here is restricted to the square cropped images, its principle also applies to the irregularly cropped images. The details will however be delegated to our next work. We also note that the rescaling in a cropped image has no significant effects on the watermark detection if the lowest frequency band is not chosen all the way for the decomposition. For the rotational distortion, it just needs to rotate the image back to the normal position, and then conducts detection for the cropped images.



Figure 10: Cropped image has predefined watermark



Figure 11: Image has no predefined watermark



Figure 12: Original and watermarked Barbara

4 Experiments

We now watermark the Barbara image of size 512x512 with q=2 in (3) and the decomposition path LH1, HL2, LH3, LH4, i.e. path 2423. We will use θ_0 for the watermark "barbara" and θ_1 for a private key. We first allocate 5 bits to store a letter in one θ ,

causing $\Delta \theta$ =0.1, and then induces all the filters from (3). We then decompose the image *I* using the filters with the "barbara" watermark, replace the filtered subband with the pattern, and finally synthesize back the watermarked image I_w as in Figure 12. We now use different filters or add white noises to the watermarked image for testing. The results are summarized in Table 3.

Path	Watermark	Noise	PSNR	RMS	3
2423	barbara		319.71	0	<
2424	barbara		20.18	24.99	<
2443	barbara		19.90	25.81	<
2423	barbara	2%	44.87	1.46	<
2423	barbara	3%	40.83	2.32	<
2423	barbara	4%	38.67	2.97	>
2423	barbara	5%	36.80	3.68	>
2423	carbara		37.11	3.56	>
2423	basbara		37.54	3.384	>

Table 3: Watermark detection via threshold

Since we chose ϵ =2.5 earlier on as the threshold for the detection, we see from Table 3 that when white noises added to the image are less than 4%, the watermark can be detected immediately. If the noises are larger than 4%, the threshold method may be inconclusive. We could however still apply the trend criterion designed for the cropped images to the fullsized images as well.

In the following test, we add white noise 5% to the Barbara image, since the RMS of the result band exceeds the detection threshold ε , we further carry out the *cropping test* on it. We first crop this image into pieces with size of 48x72 which is larger than the detectable size of 48x48, next patch back the cropped pieces to the watermarked image containing 10% white noise, then observe the trend of RMS. Table 4 below displays this trend, and it also provides the results for other test images and for different watermarks or patterns.

Table 4: Watermark detection via cropping test

Watermark					Other	
or pattern		barbara	lena	None	pattern	
	Diece 1	6 990	7.050	7 1 5 1	7 3 7 1	
	TILLET	0.990	7.039	7.131	7.371	
	Piece 2	6.971	7.142	7.354	7.732	
R	Piece 3	6.935	7.190	7.506	7.896	
M Piece 4		6.883	7.253	7.630	8.049	
S	Piece 5	6.853	7.316	7.728	8.161	
	Piece 6	6.811	7.315	7.823	8.284	
	Full	3.632	8.327	21.884	21.905	
Trend		decrease	increase	increase	increase	
RM S of 10%		<	>	>	>	
noisE 7.018						
Det ection		Yes	No	No	No	

From Table 4, we can see the strictly decreasing trend of RMS with the patching up of each additional piece of the cropped image if the image contains the "barbara" watermark, while for the image containing "lena" watermark or no watermarks at all, the trend of RMS increases with each addition of the pieces. If the private key pattern has been changed, the trend of corresponding RMS also increases with the patching up of the pieces. We also note that the RMS' of the image containing the predefined watermark are always smaller than the RMS of the image with 10% noise, while the RMS' in the other three cases in Table 4 become larger than the RMS of the image with 10% noise.

5 Conclusion

We proposed and analyzed a watermarking scheme based on embedding watermarks, and optionally private keys, inside the wavelet filters, along with the investigation of the watermark security and robustness. The detection process requires no original image, and also handles well those cropped from the watermarked images with potential addition of noises and other distortions.

6 References

- Katzenbeisser, S. Fabien and Petitcolas, A.P. (edrs.), *Information Hiding Techniques for Steganography and Digital Watermarking*, MA: Artech House, Norwood (2000).
- [2] Barni, M., Bartolini, F. and Piva, A., "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking", *IEEE Trans. Image Proc.*, 10 pp783-791 (2001).
- [3] Xia, X.G., Boncelet, C.G. and Arce, G.R., "A Multiresolution Watermark for Digital Images", *ICIP*'97, pp548-551 (1997).
- [4] Wang, Y., Doherty, J.F. and Dyck, R.E.V., "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", *IEEE Trans. Image Proc.*, pp77-88 11 (2002).
- [5] Hsu, C.T. and Wu, J.L., "Multiresolution Watermarking for Digital Images", *IEEE Trans. Circuits and Systems-II: analog and digital signal processing*, **45** pp1097-1101 (1998).
- [6] Burrus, C.S., Gopinath, R.A. and Guo, H., Introduction to Wavelets and Wavelet Transforms: A Primer, Prentice Hall, New Jersey, 1998.
- [7] Jiang, Z. and Guo, X., "A Note on the Extension of A Family of Biorthogonal Coifman Wavelet Systems", The ANZIAM Journal, in press, 2003.
- [8] Jiang, Z. and Guo, X., "Wavelets of Vanishing Moments and Minimal Filter Norms and the Application to Image Compression", Proc. of 6th ISSPA, Kuala-Lumpur, Malaysia, pp108-111 (2001)