

A Parametric Family of Wavelet Filters for Diversity in Watermarking Application

Slaven Marusic, David B. H. Tay, Guang Deng
Department of Electronic Engineering,
LaTrobe University,
Bundoora, Victoria 3086, Australia.
E-mail: {s.marusic, d.tay, g.deng}@ee.latrobe.edu.au

Abstract— A family of biorthogonal wavelet filters for digital watermarking application is presented here. The filters are explicitly parametrized by two free parameters and can be used to provide diversity in watermarking. Diversity can be used to improve the security of the watermarking system from hostile attacks. Each filter has at least two vanishing moments which is important for ensuring some degree of smoothness in the resulting wavelet function.

I. INTRODUCTION

The recent rapid growth of research activity in digital watermarking is largely due to the need for efficient and effective copyright protection in this age where multimedia data disseminate quickly through the internet. Numerous watermarking techniques have been proposed in the research literature, each with its own advantages and disadvantages. Some of the more promising techniques are based on the use of the wavelet transform, which has been successfully applied in many other areas of signal processing, most notably in image compression as seen by its adoption in several international standards.

Most wavelet based watermarking schemes proposed in the literature differ in the strategy used to embed the watermarks into the wavelet coefficients. Most authors do not give much attention to the type of wavelets used. Recently, however, some authors have started to look at aspects of the wavelet transform in the watermarking system. In [1], Meerwald and Uhl proposed diversity as a way to improve the security of the watermarking system. By using a secret wavelet filter from a sufficiently large family of filters, the watermark is more able to withstand hostile attacks. Even though the watermarking algorithm is known, the lack of knowledge of the key (the parameter that determines the secret wavelet) makes it more difficult for the attacker to mount a successful attack. This wavelet diversity method was also considered recently by Wang et. al. [2] as a way to thwart the attempts of counterfeiters. The wavelets considered in [1] and [2] are of the orthonormal types. There are no vanishing moments in the wavelets (which is the principal mechanism to achieve regularity) in both [1] and [2]. In [2], each time a different secret filter is needed, a

spectral factorization needs to be performed. In [1] the parametrization is implicit and the filter coefficients are computed by using recursive equations.

In this paper we present a new family of biorthogonal wavelet filters for use in watermarking. The coefficients are explicitly parametrized by two variables, can be computed easily and provide filter diversity. Two vanishing moments are structurally imposed in each filter, which guarantees some degree of smoothness. The filters are applied in the image watermarking scheme proposed by Kim and Moon [3] and tested for robustness and security. To our knowledge, this is the first reported work on diversity using biorthogonal filters.

II. TWO PARAMETER FAMILY OF WAVELET FILTERS

The family of wavelet filters in this paper is obtained by generalizing the '9/7' pair of CDF (Cohen, Daubechies and Feauveau) [4]. The CDF '9/7' pair is perhaps the most well known wavelet and has been adopted in the FBI fingerprint compression standard and also in the new JPEG2000 standard. The CDF '9/7' pair is obtained by factorizing the length 16 Lagrange Halfband Filter which has a maximum number of zeros at $z = -1$, ie. maximum number of vanishing moments. In the previous work reported in [5] the number of vanishing moments was reduced and this introduced some degrees of freedom. The two degrees of freedom introduced allowed filters with binary coefficients (numbers of the form $k/2^a$ where k and a are integers) to be obtained (the original CDF '9/7' filters coefficients are irrational). The two degrees of freedom was however eventually reduced to one degree because of the requirement of binary coefficients and a one parameter family of binary coefficient filters was developed in [5]. In this paper however the filters coefficients are not restricted to be binary so we have a truly two parameter family of filters. The details of the derivation of the filters are available in [5] and we shall only present the final results here.

The analysis and synthesis low-pass filters are denoted by H_0 and F_0 respectively and are of length 9 and 7

respectively. The analysis and synthesis high-pass filters are denoted by H_1 and F_1 respectively and are obtained by quadrature mirroring the low-pass filters; $H_1(z) = z^{-1}F_0(-z)$, $F_1(z) = zH_0(-z)$. The filters $H_0(z)$ and $F_0(z)$ in the family are given by:

$$H_0(z) \equiv h_0 + h_1(z + z^{-1}) + h_2(z^2 + z^{-2}) + h_3(z^3 + z^{-3}) + h_4(z^4 + z^{-4}) \quad (1)$$

$$F_0(z) \equiv f_0 + f_1(z + z^{-1}) + f_2(z^2 + z^{-2}) + h_3(z^3 + z^{-3}) \quad (2)$$

where

$$h_0 \equiv -\frac{2 + 8\alpha^3 + \alpha^2(18 + 20\beta) + 3\alpha(4 + 7\beta + 4\beta^2)}{8(2 + 2\alpha^2 + \alpha(4 + \beta))},$$

$$h_1 \equiv \frac{2 + 2\alpha^3 + 3\alpha^2(2 - \beta) + \alpha(6 - 3\beta - 4\beta^2)}{8(2 + 2\alpha^2 + \alpha(4 + \beta))},$$

$$h_2 \equiv \frac{\alpha(2 + 2\alpha^2 + 3\beta + \beta^2) + \alpha(4 + 3\beta)}{4(2 + 2\alpha^2 + \alpha(4 + \beta))},$$

$$h_3 \equiv -\frac{1}{8}(1 + \alpha), \quad h_4 \equiv \frac{1}{16},$$

$$f_0 \equiv \frac{1}{2}(1 + \alpha + \beta), \quad f_1 \equiv \frac{1}{8}(3 + 4\alpha + 4\beta),$$

$$f_2 \equiv \frac{1}{4}(1 + \alpha), \quad f_3 \equiv \frac{1}{8}$$

The coefficients are parametrized by the two free parameters α and β . Both filters have at least 2 vanishing moments each regardless of the values of α and β . Setting

$$\beta = -\frac{1}{15} \left(20 - \frac{35^{2/3}}{(10 + 3\sqrt{15})^{1/3}} + (35(10 + 3\sqrt{15}))^{1/3} \right) \approx -1.6848 \quad (3)$$

$$\alpha = \beta - 1 \approx -0.6848 \quad (4)$$

gives the '9/7' filter pair of CDF. The two parameter family presented above can be used to provide diversity in watermarking application to improve its security.

In comparison, the filters considered in [1] are a two parameter orthonormal family of length 6 wavelet filters obtained using the result of Schneid [6]. The coefficients are not explicitly parametrized and are computed using recursive equations. The free parameters are arguments of sine and cosine functions. Hence its effective values are restricted to $(-\pi, \pi)$. However we found that the practical range is $(0, \pi)$ as the negative range gives filters which are identical to the filters in the positive range. Finally no zero moment conditions were explicitly imposed. On the other hand, the biorthogonal filters in (1) and (2) are explicitly parametrized, have at least 2 vanishing moments and do not have any limits to their parameter range.

As a measure of the smoothness of the wavelets, we shall employ a measure that is similar to the second-order local variation proposed in [1]. Let $g^{(J)}(n)$ denote the equivalent J level iterated filter bank impulse response of the bandpass channel (approximately the shape of the corresponding wavelet function $\psi(t)$) and let L denote the length of $g^{(J)}(n)$. The smoothness measure we employ is given by:

$$S \equiv \frac{1}{L} \sum_n \left| g^{(J)}(n) - g^{(J)}(n-1) + g^{(J)}(n-2) \right| \quad (5)$$

The difference between (5) and the measure in [1] is the normalization factor in the former. The normalization allows wavelets filters with different lengths to be compared on an equal footing.

III. WAVELET BASED WATERMARKING

The technique used in this paper to embed watermark information is based on that presented by Kim and Moon [3]. It extends upon the work of Cox et. al. [7] where watermarks were embedded in DCT coefficients and Xia et. al. [8] where watermarks were embedded in the coefficients of all but the low frequency subband of a discrete wavelet transform (DWT). Taking advantage of the fact that frequency domain watermarking methods are robust to noise and common image processing, Kim's technique embeds the watermark in perceptually significant coefficients of a DWT. Consequently, robustness to attacks is increased as is the watermark invisibility.

The watermark X_n is a Gaussian distributed random vector, generated using the Box-Muller transform. This was then normalised to between -0.5 and 0.5.

The watermark insertion process begins by performing the DWT of the original image. For each level (n) of wavelet decomposition a threshold is calculated to determine perceptually significant coefficients. After first finding the largest coefficient C_n from the high-pass subbands (HL_n, LH_n, HH_n), the threshold for a given level (T_n) is given by

$$T_n = 2^{\lfloor \log_2 C_n \rfloor - 1}$$

We also performed this function for the low frequency subband (LL).

The watermark is then embedded into coefficients above the threshold in the following manner:

$$V'_n = V_n + \alpha V_n X_n$$

where V_n is the original wavelet coefficient, X_n is the watermark and V'_n is the watermarked coefficient. The scaling factor α for each decomposition level is predetermined. We used $\alpha = 0.01$ for LL and $\alpha = 0.01$ for the high frequency subbands at all decomposition levels, to avoid visual artifacts. The strength of the watermark is thus dependent on the scaling factor and the amplitude of the respective coefficients. The inverse DWT is then performed to obtain the watermarked image.

The watermark extraction is essentially the reverse of the insertion process. The DWTs of the original and watermarked images are first performed. The watermark is then obtained by subtracting the original image coefficients from the watermarked image coefficients.

The presence of the watermark is then evaluated based on the similarity between the extracted and original watermarks. The normalised similarity is given by

$$\text{sim}(X, X^*) = \left(\frac{X \cdot X^*}{\sqrt{X^* \cdot X^*}} / \frac{X \cdot X}{\sqrt{X \cdot X}} \right) \times 100$$

where X is the original watermark and X^* is the extracted watermark.

IV. RESULTS

In our simulations a $J = 4$ level wavelet decomposition was used. To ensure sufficient smoothness in the wavelet, a threshold value of $S_{\text{threshold}} = 0.06$ was used, i.e. only wavelets with $S \leq S_{\text{threshold}}$ were considered for use in the watermarking process.

Figure 1 (top) shows the parameter space of the 9/7 biorthogonal family and regions that yield sufficiently smooth wavelets filters. Figure 1 (bottom) shows the corresponding parameter space and regions of smooth filters for the length 6 orthonormal family of wavelets that was used in [1].

Figure 2 shows the robustness of the wavelet filters subject to varying levels of JPEG compression attacks. Figure 3 show the corresponding robustness subject to varying levels of JPEG2000 attacks. The results in both attacks represent an average result from a set of smooth filters in the parameter space. Both sets of filters have comparable levels of robustness.

To test the security of the wavelet filters, a set of filters (within each family) with sufficient diversity was used. We found that we could obtain around 6200 pairs of filters with sufficient smoothness and diversity within the key space in Figure 1 (top) for the 9/7 biorthogonal family. For the length 6 orthonormal family around 5800 pairs of filters within the key space in Figure 1 (bottom) could be found.

To assess the level of security, one filter (unknown to unauthorised persons) is used to embed the watermark and test were performed to see if other filters could be used to extract the watermark. Figure 4 is a typical result, showing the similarity measure when extracting the watermarks with different filters in the 9/7 family. Figure 5 shows a corresponding result for the orthonormal family. In both cases, we see that most filters are unable to give a large enough measure to indicate the presence of the watermark. In other words, without knowing the actual filter used in the embedding process, it would be difficult for unauthorised persons to extract the watermark. If, for example, we select a detection threshold

to be 50% of the maximum similarity value (obtained using the embedding filter), it can be seen that the two filter families produce similar levels of security. In this instance, the biorthogonal wavelet filter would produce three false positives and the orthonormal wavelet family would produce two. The significance of such false positives is application dependent. As such, the detection threshold can be set accordingly.

V. CONCLUSION

A new family of biorthogonal of wavelet filters was presented here. The filters are explicitly parametrized by two free parameters and have in-built two vanishing moments to ensure some degree of regularity. The filters can provide diversity in watermarking applications which can improve the security from hostile attacks. The filters were found to be sufficiently robust against JPEG and JPEG2000 compression attacks. The biorthogonal family of filters presented here has a comparable level of diversity compared to the length 6 orthonormal family.

Future work in this area will include testing the filters with other wavelet based watermarking schemes that might incorporate the characteristics of the human visual system. More comprehensive testing to determine robustness under a wider range of attacks will also be performed.

REFERENCES

- [1] P. Meerwald and A. Uhl. Watermark Security Via Wavelet Filter Parametrization. In *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, 2001.
- [2] Yiwei Wang, John F. Doherty, and Robert E. Van Dyck. A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images. *IEEE Trans. Image Proc.*, 11(2):77–88, February 2002.
- [3] Jong Ryul Kim and Young Shik Moon. A Robust Wavelet-Based Digital Watermarking Using Level-Adaptive Thresholding. In *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, 1999.
- [4] A. Cohen, I. Daubechies, and J. C. Feauveau. Biorthogonal bases of compactly supported wavelets. *Comm. Pure Appl. Math.*, 45:485–560, 1992.
- [5] D. B. H. Tay. Families of Binary Coefficient Biorthogonal Wavelet Filters. In *Proc. IEEE Symp. Circuits Sys.*, 2000.
- [6] J. Schneid and S. Pittner. On the Parametrization of the Coefficients of Dilation Equations for Compactly Supported Wavelets. *Computing*, 51:165–173, May 1993.
- [7] I. Cox, J. Kilian, F. Leighton, and T. Shamoan. Secure Spread Spectrum Watermarking for Multimedia. *IEEE Trans. Image Proc.*, 6(12):1673–1687, December 1997.
- [8] X. G. Xia, C. G. Boncelet, and G. R. Arce. A Multiresolution Watermark for Digital Images. In *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, 1997.

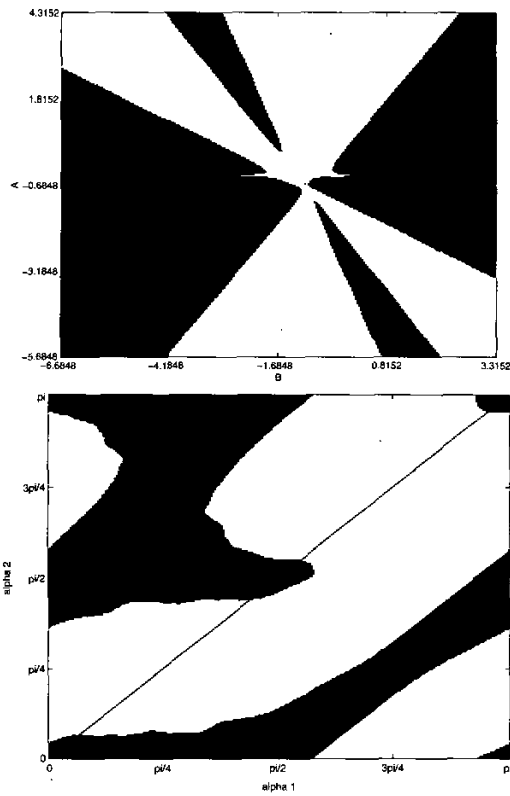


Fig. 1. Top: parameter space of the 9/7 biorthogonal family. Bottom: parameter space of the length 6 orthonormal family. Shaded regions indicating sufficiently smooth wavelets, i.e. $S \leq 0.06$.

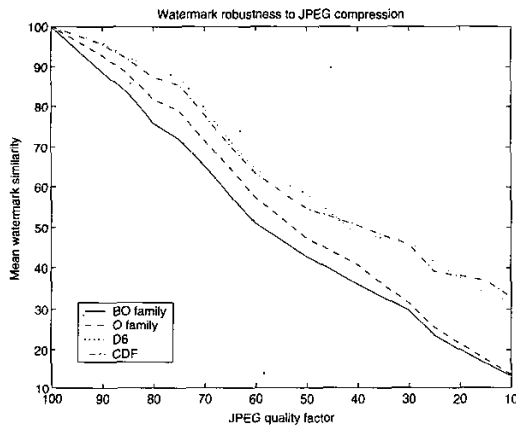


Fig. 2. Robustness testing result under JPEG compression attacks. BO family - 9/7 biorthogonal wavelets; O family - length 6 orthonormal wavelets; CDF - CDF 9/7 pair; D6 - Daubechies length 6 wavelet.

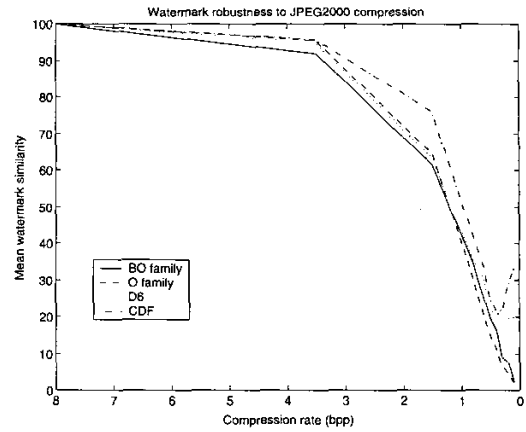


Fig. 3. Robustness testing result under JPEG2000 compression attacks. BO family - 9/7 biorthogonal wavelets; O family - length 6 orthonormal wavelets; CDF - CDF 9/7 pair; D6 - Daubechies length 6 wavelet.

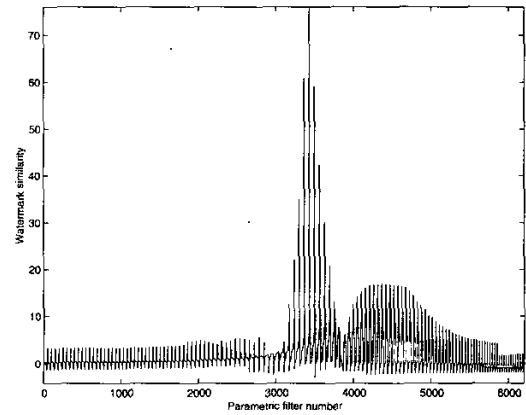


Fig. 4. Security testing of the 9/7 biorthogonal wavelet filters.

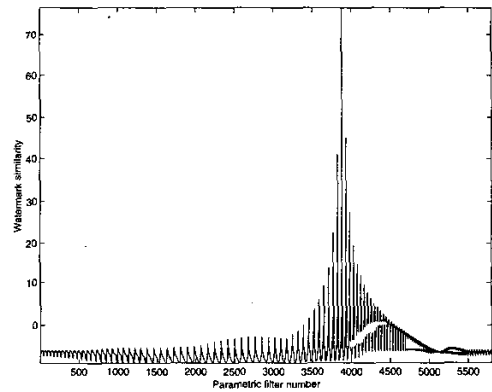


Fig. 5. Security testing of the length 6 orthonormal wavelet filters.