A STUDY OF BIORTHOGONAL WAVELETS IN DIGITAL WATERMARKING

Slaven Marusic[*†], *David B. H. Tay*[*], *Guang Deng*[*] *and Marimuthu Palaniswami*[†]

[*]Department of Electronic Engineering, La Trobe University, Victoria 3086, Australia
[†]Department of Electrical and Electronic Engineering, The University of Melbourne
Victoria 3010, Australia

ABSTRACT

A study of a family of biorthogonal wavelet filters for use in digital watermarking is presented. 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.

Along with robustness and security, other factors which impact upon the successful implementation of the filters in a watermarking application are analysed. The relationship between the strength of the inserted watermark and wavelet energy is also discussed.

1. 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, of which some of the more promising techniques are based on the use of the wavelet transform.

Most wavelet based watermarking schemes proposed in the literature differ in the strategy used to embed the watermarks into the wavelet coefficients. Until recently, most authors have not given much attention to the type of wavelets used. 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 and contain no vanishing moments (which is the principal mechanism to achieve regularity). 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 study on a new family of biorthogonal wavelet filters for use in watermarking. The coefficients are explicitly parametrized by two variables and can be computed easily. Two vanishing moments are structurally imposed in each filter. The filters are applied in the image watermarking scheme proposed by Kim and Moon [3] and tested for robustness and security. An alternative normalisation for the filters is suggested, which improves aspects of the watermarking application. The relationship between the strength of the inserted watermark and wavelet energy is also discussed.

2. TWO PARAMETER BIORTHOGONAL 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 details of the derivation of the filters are available in [5] and only the final results are presented here.

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 are given by:

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

$$\begin{aligned} F_0(z) &\equiv f_0 + f_1(z+z^{-1}) + f_2(z^2+z^{-2}) \\ &+ f_3(z^3+z^{-3}) \end{aligned} \quad (2)$$

0-7803-7750-8/03/$17.00 ©2003 IEEE

where

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

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

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

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

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

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

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. Note that when $\alpha = -0.6848$ and $\beta = -1.6848$, the filter pair becomes the CDF 9/7 pair.

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. As the free parameters are arguments of sine and cosine functions, 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 normalisation of the second-order local variation proposed in [7]. 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:

$$S \equiv \frac{1}{L}\sum_n \left| g^{(J)}(n) - 2g^{(J)}(n-1) + g^{(J)}(n-2) \right| \quad (3)$$

The normalization allows wavelet filters with different lengths to be compared on an equal footing.

3. WAVELET BASED WATERMARKING

The technique used in this paper to embed watermark information is based on that presented by Kim and Moon [3]. 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 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 X_n is a Gaussian distributed random vector, generated using the Box-Muller transform and normalised between -0.5 and 0.5. The watermark is then embedded into coefficients above the threshold as follows,

$$V_n' = V_n + \gamma_n V_n X_n \quad (4)$$

where V_n is the original wavelet coefficient, X_n is the watermark and V_n' is the watermarked coefficient. The scaling factor γ_n for each decomposition level is predetermined. We used 0.01 for LL and 0.1 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

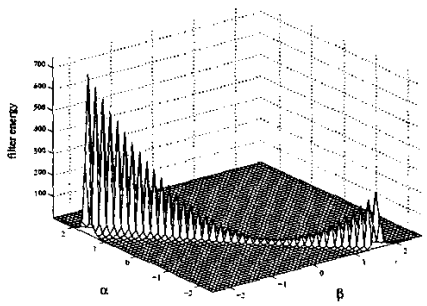
$$sim(X, X^*) = \left(\frac{X \cdot X^*}{\sqrt{X^* \cdot X^*}} / \frac{X \cdot X}{\sqrt{X \cdot X}} \right) \times 100$$

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

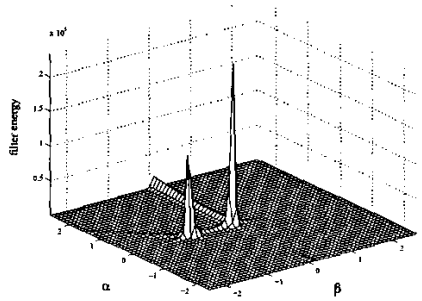
4. FILTER NORMALISATION

The use of the 9/7 family of biorthogonal wavelet filters in this particular watermarking application, raises certain issues not previously encountered with the parametric orthonormal wavelets used by Meerwald [1]. It becomes evident that the energy of the biorthogonal wavelet filters varies significantly through the keyspace (refer to Figure 1).

When used in the proposed watermarking application, these high energy wavelets produce significant artifacts in the resulting image. Obviously, this contravenes the invisibility requirement of the watermark. We thus propose the l^2-normalisation of the filters obtained from this biorthogonal wavelet family.

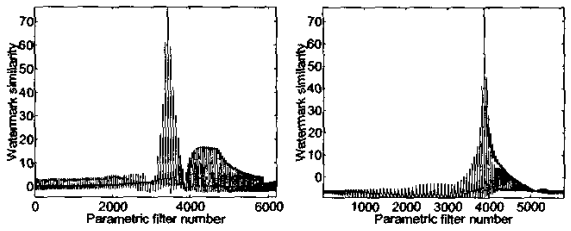


(a) length 7 filter



(b) length 9 filter

Fig. 1. Filter energy of the l^1-normalised biorthogonal wavelet family



(a) 9/7 biorthogonal filter (b) length 6 orthonormal filter

Fig. 2. Wavelet security testing

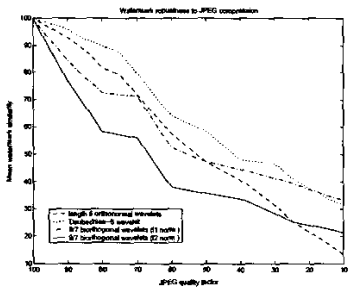


Fig. 3. Robustness to JPEG compression attacks

5. RESULTS

5.1. Security and Robustness

The security offered by the technique, in using a particular wavelet filter as the secret key, is measured by attempting to extract the watermark using the other filters in the keyspace. As seen in Figure 2, the security/diversity offered by the biorthogonal wavelet family is comparable to that of the parametric length 6 orthonormal wavelet given in [1]. Analysis of different regions of the keyspace has also shown the l^2-normalised biorthogonal filters to be more secure overall than the l^1-normalised biorthogonal filters.

The robustness of the different wavelet families to JPEG and JPEG 2000 compression attacks is shown in Figures 3 and 4. These are the average results from a set of comparatively smooth filters (i.e. filter parameters taken from the dark regions of Figure 5).

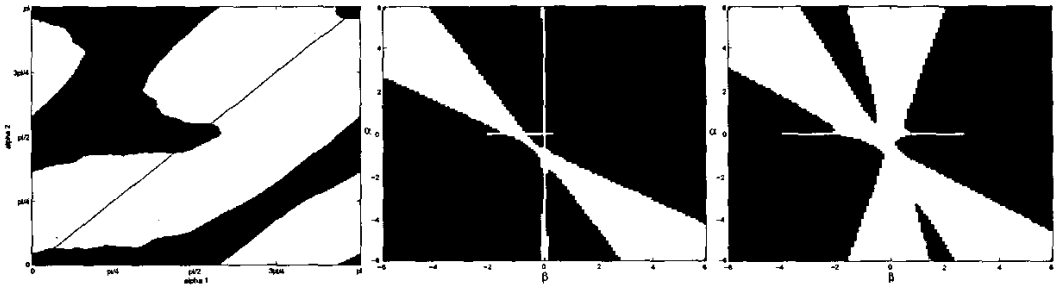
5.2. Smoothness and PSNR

Using the smoothness of the HAAR wavelet as a threshold, the maps of available wavelets are given in Figure 5 for the parametric length 6 orthonormal wavelets [1], as well as the l^1 and l^2-normalised biorthogonal wavelets respectively. As shown in Figure 1, the energy along a number of planes through the l^1-normalised keyspace is extremely high. Following l^2-normalisation, these planes coincide with the associated smoothness map. The proposed normalisation thus makes the smoothness measure (Equation 3) more indicative of the usability of the filter in this application.

By testing all filters in the keyspace for the watermarking application, it becomes clear that watermark invisibility is compromised in certain cases. Mapping the PSNR of the respective watermarked images, low PSNR values (indicating significant image degradation) are observed in the areas of the previously mentioned planes where the filters have high energy values. The PSNR maps, in fact, correspond directly to both the smoothness maps and the original energy maps of the l^1-normalised biorthogonal filters.

5.3. Wavelet Energy, Image Artifacts and Watermark Strength

With a fixed scaling vector for the watermark embedding strength, while suitable for orthonormal wavelet filters, limits the usability of the proposed family of biorthogonal wavelet filters. The use of biorthogonal filters requires a more careful selection of the scaling vector used to determine the strength of the embedded watermark. Due to the nature of the watermark embedding function (4), image artifacts are produced by embedding watermarks that are too large. Likewise, using a wavelet filter of large energy requires a further reduction of the watermark magnitude. Ideally, to achieve a highly robust watermark, a high watermark



(a) Parametric length 6 orthonormal wavelets

(b) l^1-normalised 9/7 biorthogonal wavelets

(c) l^2-normalised 9/7 biorthogonal wavelets

Fig. 5. Parameter space of wavelet families, shaded regions indicating sufficiently smooth wavelets ($S < 0.0526$)

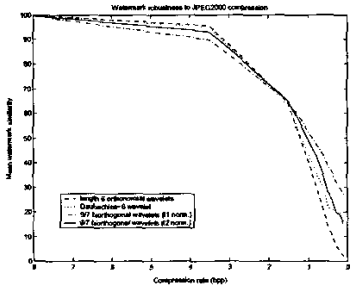


Fig. 4. Robustness to JPEG 2000 compression attacks

should be embedded into wavelet coefficients obtained from a low energy filter. A compromise between the robustness and invisibility of the watermark is thus required.

Sufficiently reducing the strength of the watermark in such cases will remove any artifacts. Although the detectability of the watermark is slightly reduced, simulations have shown that the filters in question are still usable. Consequently, performing such modifications further increases the library of filters available to form the keyspace.

The number of usable filters within the keyspace can be expanded by modifying the watermark strength in conjunction with the filter energy. A somewhat objective measure is thus provided which is more indicative of watermark invisibility that the smoothness measure. The computational complexity is also comparable. This enables the use of filters that would otherwise be considered to be insufficiently smooth and/or have excessive energy.

6. CONCLUSION

We have provided a study of a new biorthogonal wavelet filter family in the context of digital watermarking. We have shown that biorthogonal wavelets offer sufficient robustness and security to particular watermark attacks. The number of available wavelets in the filter library has been increased by performing an alternative filter normalisation, as well as adaptively setting the watermark strength according to the filter energy. The latter measure also ensures watermark invisibility. The utilisation of biorthogonal wavelets in blind watermarking schemes is currently being investigated.

7. REFERENCES

[1] P. Meerwald and A. Uhl, "Watermark Security Via Wavelet Filter Parametrization," Proc. IEEE Int. Conf. on Image Processing, 2001, pp. 1027-1030.

[2] Y. Wang, J. F. Doherty and R. E. Van Dyck, A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images," IEEE Trans. Image Processing, 11(2):77-88, Feb. 2002.

[3] J. R. Kim and Y. S. Moon, "A Robust Wavelet-Based Digital Watermarking Using Level-Adaptive Thresholding," Proc. IEEE Int. Conf. on Image Processing, 1999, Vol. 2, pp. 226-230.

[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," Proc. IEEE Int. Symp. on Circuits and Systems, 2000, Vol. 4, pp. 17-20.

[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] S. Maslakovic, I. R. Linscott, M. Oslick and J. D. Twicken, "Smooth Orthonormal Wavelet Libraries: Design and Application," Proc. Int. Conf. on Acoustics, Speech and Signal Processing, 1998, pp. 1793-1796.