A PERFORMANCE ANALYSIS OF SPREAD-SPECTRUM WATERMARKING BASED ON REDUNDANT TRANSFORMS

Li Hua and James E. Fowler
Department of Electrical and Computer Engineering
Engineering Research Center
Mississippi State University, Mississippi State, MS

ABSTRACT

Spread-spectrum watermarking, in which random noise is added to transform coefficients and detected with a correlation operator, has become a preferred paradigm for many watermarking applications. This paper analyzes the performance of such a watermarking system when the underlying transform is a tight frame rather than a traditional orthonormal expansion. The analysis indicates that a tight frame offers no inherent performance advantage over an orthonormal transform in the watermark-detection process despite the well known ability of redundant transforms to accommodate greater amounts of added noise for a given distortion.

1. INTRODUCTION

Image watermarking is a technique for labeling digital images by embedding electronic stamps or so-called watermarks into an image for a variety of purposes including copyright protection and image authentication. Due to the explosion in use of the digital media, watermarking has recently attracted significant interest from academia and industry alike.

A number of techniques have been developed for image watermarking. Perhaps the most widely employed technique is spread-spectrum watermarking [1] which embeds a white-noise watermark into coefficients of an orthonormal or biorthogonal transform. In this case, the watermark is detected by computing a correlation between the watermarked coefficients and the watermark noise sequence, with this correlation being compared to a properly selected threshold to determine watermark presence or absence. The discrete wavelet transform (DWT) is an appealing transform for spread-spectrum watermarking because its space-frequency tiling exhibits a strong similarity to the way the human visual system (HVS) processes natural images [2]. Thus, watermarking applied in the wavelet domain can largely exploit the HVS characteristics and effectively hide a robust watermark. Orthonormal and biorthogonal DWTs have been proposed frequently (e.g., [2]) for spread-spectrum watermarking.

However, alternative wavelet-transform paradigms exist. For example, the redundant discrete wavelet transform (RDWT) (see, for example, [3]) gives an overcomplete representation of the input sequence which functions to a certain extent as an approximation to the continuous wavelet transform. The RDWT is shift invariant, and its redundancy introduces an overcomplete frame expansion. It is known that frame expansions increase robustness to additive noise [4, 5]; that is, the addition of noise to transform coefficients results in less signal distortion for frame expansions than for orthonormal expansions. Thus, RDWT-based signal processing tends to be more robust than DWT-based techniques, and the RDWT has been successfully deployed in a variety of applications, notably noise reduction and feature detection. Additionally, prior work has proposed the RDWT for image watermarking [6]. Initially, one might think that, since frame expansions like the RDWT offer increased robustness to added noise, such overcomplete expansions have the potential to outperform traditional orthonormal expansion in the watermarking problem. In this report, we offer analysis that contradicts this intuition. Specifically, we present analysis that shows that, although spread-spectrum watermarking of tight-frame coefficients does produce less image distortion for the same watermarking energy, the correlation-detector performance of tight-frame based watermarking is identical to that obtained by using an orthonormal expansion.

Below, we first recall some fundamental theory concerning frame expansions and their robustness to added noise. We then analyze the performance of spread-spectrum correlation detectors for both tight-frame and orthonormal expansions. We follow with several concluding remarks.

2. FRAME EXPANSIONS AND ROBUSTNESS TO ADDED NOISE

A family of functions $(\psi_i)_{i\in J}$ is called a frame if there exist $A > 0$ and $B < \infty$ so that, for all f in Hilbert space $\mathcal{H}$,

$$A\|f\|^2 \leq \sum_{i\in J} |<\psi_i, f>|^2 \leq B\|f\|^2, \tag{1}$$

where A and B are called the *frame bounds* [4]. The *dual frame* $(\tilde{\psi}_i)$ of (ψ_i) is an expansion set in Hilbert space $\mathcal{H}$, and for all f in $\mathcal{H}$,

$$\frac{1}{B}\|f\|^2 \leq \sum_i |<\tilde{\psi}_i, f>|^2 \leq \frac{1}{A}\|f\|^2. \tag{2}$$

Any function $f \in \mathcal{H}$ can be expanded as

$$f = \sum_i <\psi_i, f> \tilde{\psi}_i = \sum_i <\tilde{\psi}_i, f> \psi_i \tag{3}$$

If the frame bounds are equal, i.e., $A = B$, the frame is called a *tight frame*. In a tight frame, we have

$$\sum_{i\in J} |<\psi_i, f>|^2 = A\|f\|^2, \tag{4}$$

$$\tilde{\psi}_i = \frac{1}{A}\psi_i, \tag{5}$$

$$f = \frac{1}{A}\sum_i \langle\psi_i, f\rangle\,\psi_i. \tag{6}$$

In this case, A gives the "redundancy ratio," a measure of the degree of overcompleteness of the expansion (we assume that the ψ_i's have unit norm). An orthonormal expansion is the special case that $A = 1$, i.e., a transform with no redundancy.

In *Proceedings of the IEEE International Conference on Multimedia and Expo*, August, 2002, to appear

The RDWT removes the decimation operators from DWT filter banks, yielding a redundant representation of the input sequence It can be shown [7] that the RDWT is a frame expansion with frame bounds $A = 2$ and $B = 2^J$, where J is the number of levels in the transform. Thus, for one scale of decomposition, the RDWT is a tight frame.

Tight-frame expansions increase the robustness to added white noise with respect to orthonormal transforms. Specifically, suppose zero-mean, variance-ϵ^2 Gaussian noise is added to transform coefficients. The mean square error (MSE) of the reconstructed signal with respect to the original signal is

$$MSE = E[\|f - \hat{f}\|^2], \tag{7}$$

where f is the original signal, and $\hat{f}$ is the corrupted signal. It has been shown [5] that the MSE distortion due to the added noise is $\frac{N\epsilon^2}{A}$ for a tight-frame expansion. The orthonormal basis is a special case of a tight frame with redundancy $A = 1$; for a nonorthogonal tight frame, $A > 1$. Thus, we have $\frac{N\epsilon^2}{A} < N\epsilon^2$, and the distortion incurred by a tight frame is less than that arising with an orthonormal basis.

3. TIGHT FRAME AND WATERMARKING

In spread-spectrum watermarking, the signal is transformed using an expansion basis,

$$f = \sum_i \alpha_i \psi_i, \tag{8}$$

and the watermark sequence, i.e., white Gaussian noise, is added to the coefficients in the transform domain to form the watermarked signal,

$$f' = \sum_i \alpha'_i \psi_i = \sum_i (\alpha_i + \epsilon n_i)\psi_i, \tag{9}$$

where n_i is zero-mean, unit-variance white Gaussian noise, and ϵ is a parameter that controls the watermark strength. The watermark can be detected assuming the watermark noise sequence is known exactly to the detector. This is done by performing the forward transform on the watermarked signal and then computing a correlation on the coefficients,

$$\rho = \sum_i \hat{\alpha}_i n_i, \tag{10}$$

where $\hat{\alpha}_i$ are the expansion coefficients of the watermarked image f',

$$\hat{\alpha}_i = \left\langle \tilde{\psi}_i, f' \right\rangle. \tag{11}$$

For watermark detection, the correlation ρ is compared to a threshold to decide the presence of the watermark. An optimal threshold can be set to minimize the probability of missing the presence of the watermark given a probability of false detection according to the Neyman-Pearson criterion [2].

Below, we compare the watermarking performance of an orthonormal basis versus that of a tight-frame expansion. In this comparison, we adjust the watermark strength such that both procedures achieve the same MSE and the same false-alarm error P_F, and then measure the performance by computing the minimum missed-detection error, P_M, as obtained with the Neyman-Pearson criterion. We focus our analysis on the discrimination between two hypotheses [2]:

Case A: the image is watermarked with a random sequence m_i different from the watermark n_i we are trying to detect, but using the same watermarking approach,

Case B: the image is watermarked with the watermark n_i that we are trying to detect.

The Neyman-Pearson test obtains a decision rule by minimizing the missing error, P_M subject to a constraint on the false-alarm error, P_F. The decision criterion is

$$\rho \underset{H_0}{\overset{H_1}{\gtrless}} T_\rho. \tag{12}$$

As was done in [2], we model the correlation ρ as normally distributed, which is a realistic assumption arising from the central-limit theorem. In this case, the binary hypothesis problem is formulated as

$$H_0 : \text{Case A} \qquad P(\rho|H_0) = \frac{1}{\sqrt{2\pi}\sigma_{\rho A}} \exp\left[-\frac{\rho^2}{2\sigma_{\rho A}^2}\right]$$

$$H_1 : \text{Case B} \qquad P(\rho|H_1) = \frac{1}{\sqrt{2\pi}\sigma_{\rho B}} \exp\left[-\frac{(\rho-\mu_{\rho B})^2}{2\sigma_{\rho B}^2}\right].$$

Consequently, the false alarm error P_F and the missing error P_M can be expressed with respect to the threshold T_ρ,

$$P_F = P(D_1|H_0) = \frac{1}{2}\,\mathrm{erfc}\left(\frac{T_\rho}{\sqrt{2}\sigma_{\rho A}}\right) \tag{13}$$

$$P_M = P(D_0|H_1) = \begin{cases} \frac{1}{2} + \frac{1}{2}\,\mathrm{erf}\left(\frac{T_\rho - \mu_{\rho B}}{\sqrt{2}\sigma_{\rho B}}\right), & T_\rho \geq \mu_{\rho B}, \\ \frac{1}{2}\,\mathrm{erfc}\left(\frac{\mu_{\rho B} - T_\rho}{\sqrt{2}\sigma_{\rho B}}\right), & T_\rho < \mu_{\rho B}. \end{cases} \tag{14}$$

In order to obtain the Neyman-Pearson test for each watermarking procedure, the probability distributions of the watermark correlation ρ are needed. These are calculated as follows:

(1) *Orthonormal basis*

If the image is watermarked with a watermark other than the one we are trying to detect (Case A), then the watermarked image is

$$f' = \sum_i (\alpha_i + \epsilon m_i)\psi_i, \tag{15}$$

and the correlation of the watermarking is

$$\rho_A = \sum_{i=1}^{N} (\alpha_i + \epsilon m_i) n_i \tag{16}$$

with mean

$$\mu_{\rho A} = E[\rho_A] = 0 \tag{17}$$

and variance

$$\begin{aligned} \sigma_{\rho A}^2 &= E[\rho_A - \mu_{\rho A}]^2 = E[\sum_{i=1}^{N} (\alpha_i + \epsilon m_i) n_i]^2 \\ &= \sum_i E[\alpha_i^2 + \epsilon^2 m_i^2 + 2\epsilon m_i \alpha_i] E[n_i^2] \\ &= \|f\|^2 + N\epsilon^2. \end{aligned} \tag{18}$$

If the image is watermarked with the watermark we are detecting (Case B), we have that the correlation is

$$\rho_B = \sum_{i=1}^{N} (\alpha_i + \epsilon n_i) n_i \tag{19}$$

with mean

$$\mu_{\rho B} = E[\rho_B] = \epsilon \cdot N \tag{20}$$

and variance

$$\begin{aligned}\sigma^2_{\rho B} &= E[\rho_B - \mu_{\rho B}]^2 = E[\rho_B^2] - \mu^2_{\rho B} \\ &= E[\sum_{i=1}^{N}(\alpha_i + \epsilon n_i)n_i]^2 - \epsilon^2 N^2 \\ &= \sum_{i=1}^{N} \alpha_i^2 + 3N\epsilon^2 + \epsilon^2(N^2 - N) - \epsilon^2 N^2 \\ &= \|f\|^2 + 2N\epsilon^2. \end{aligned} \tag{21}$$

(2) *Tight Frame*

If the image is watermarked with a watermark other than the one we are trying to detect (Case A), the correlation of the watermarking is

$$\begin{aligned}\rho_A &= \sum_{i=1}^{AN} \hat{\alpha}_i n_i = \sum_i \langle \psi_i, f' \rangle n_i \\ &= \sum_i \left\langle \psi_i, \frac{1}{A} \sum_j (\alpha_j + \epsilon m_j)\psi_j \right\rangle n_i \\ &= \frac{1}{A} \sum_i \sum_j (\alpha_j + \epsilon m_j) n_i \langle \psi_i, \psi_j \rangle . \end{aligned} \tag{22}$$

In this case, the mean and variance of the correlation are

$$\mu_{\rho A} = E[\rho_A] = 0 \tag{23}$$

and

$$\begin{aligned}\sigma^2_{\rho A} &= E[\rho_A - \mu_{\rho A}]^2 = E[\rho_A^2] \\ &= E\left[\frac{1}{A} \sum_i \sum_j (\alpha_j + \epsilon m_j) n_i \langle \psi_i, \psi_j \rangle \right]^2 \\ &= \frac{1}{A^2} \sum_{i=1}^{AN} \left[\sum_j \alpha_j \langle \psi_i, \psi_j \rangle \right]^2 + \frac{\epsilon^2}{A^2} \sum_{i=1}^{AN} \sum_{j=1}^{AN} \langle \psi_i, \psi_j \rangle^2 . \end{aligned} \tag{24}$$

Since for a tight frame

$$f = \frac{1}{A} \sum_j \langle \psi_j, f \rangle \psi_j = \frac{1}{A} \sum_j \alpha_j \psi_j, \tag{25}$$

we have

$$\sum_{i=1}^{AN} \left[\sum_j \alpha_j \langle \psi_i, \psi_j \rangle \right]^2 = \sum_{i=1}^{AN} \langle \psi_i, Af \rangle^2 = A^2 \sum_{i=1}^{AN} \alpha_i^2.$$

Additionally, a tight frame has the property that

$$\sum_i |\langle \psi_i, f \rangle|^2 = A\|f\|^2. \tag{26}$$

Thus, the second term in (24) is

$$\begin{aligned}\sum_{i=1}^{AN} \sum_{j=1}^{AN} \langle \psi_i, \psi_j \rangle^2 &= \sum_{i=1}^{AN} A\|\psi_i\|^2 \\ &= \sum_{i=1}^{AN} A = A^2 N. \end{aligned} \tag{27}$$

Therefore, we have

$$\begin{aligned}\sigma^2_{\rho A} &= \frac{1}{A^2} \cdot A^2 \sum_{i=1}^{AN} \alpha_i^2 + \frac{\epsilon^2}{A^2} \cdot A^2 N \\ &= \sum_{i=1}^{AN} \alpha_i^2 + \epsilon^2 N \\ &= A\|f\|^2 + \epsilon^2 N. \end{aligned} \tag{28}$$

If the image is watermarked with the watermark we are detecting (Case B), we have that the correlation is

$$\rho_B = \frac{1}{A} \sum_i \sum_j \alpha_j n_i \langle \psi_i, \psi_j \rangle + \frac{1}{A} \sum_i \sum_j \epsilon n_j n_i \langle \psi_i, \psi_j \rangle . \tag{29}$$

In this case, the mean and variance of the correlation are

$$\mu_{\rho B} = E[\rho_B] = \epsilon \cdot N \tag{30}$$

and

$$\begin{aligned}\sigma^2_{\rho B} &= E[\rho_B - \mu_{\rho B}]^2 = E[\rho_B^2] - \mu^2_{\rho B} \\ &= \frac{1}{A^2}\left[A^2 \sum_{i=1}^{AN} \alpha_i^2 + \epsilon^2 A^2 (N^2 + 2N)\right] - \epsilon^2 N^2 \\ &= \sum_{i=1}^{AN} \alpha_i^2 + \epsilon^2 (N^2 + 2N) - \epsilon^2 N^2 \\ &= A\|f\|^2 + 2\epsilon^2 N. \end{aligned} \tag{31}$$

4. PERFORMANCE COMPARISON

Assume we adjust the watermarking strength ϵ in (9) such that an MSE of D is obtained. Then, we have

$$\text{Orthonormal Basis:} \quad MSE = E[\|f - f'\|^2] = N\epsilon^2 = D$$

$$\text{Tight Frame:} \quad MSE = E[\|f - f'\|^2] = \frac{N\epsilon^2}{A} = D$$

so that, in order to achieve the same MSE, the watermarking strength ϵ is adjusted as

$$\text{Orthonormal Basis:} \quad \epsilon = \sqrt{\frac{D}{N}} \tag{32}$$

$$\text{Tight Frame:} \quad \epsilon' = \sqrt{\frac{AD}{N}}. \tag{33}$$

Under these conditions, the statistics of the Gaussian-modeled correlation ρ are given in Table 1.

The performance at watermark detection is measured with the optimal missed-detection error, P_M, in the sense of the Neyman-Pearson test, while the watermark distortion and false-alarm error P_F are held fixed.

Orthonormal Basis:

$$\begin{aligned}P_F &= \frac{1}{2}\,\mathrm{erfc}\left(\frac{T_\rho}{\sqrt{2}\sigma_{\rho A}}\right) \\ &= \frac{1}{2}\,\mathrm{erfc}\left(\frac{T_\rho}{\sqrt{2}\sqrt{\|f\|^2 + D}}\right) \end{aligned} \tag{34}$$

	Orthonormal Basis	Tight Frame
Case A	$\mu_{\rho A} = 0$ $\sigma^2_{\rho A} = \|f\|^2 + N\epsilon^2$ $= \|f\|^2 + D$	${\mu'}_{\rho A} = 0$ ${\sigma'}^2_{\rho A} = A\|f\|^2 + N{\epsilon'}^2$ $= A\|f\|^2 + AD$
Case B	$\mu_{\rho B} = \epsilon \cdot N = \sqrt{ND}$ $\sigma^2_{\rho B} = \|f\|^2 + 2N\epsilon^2$ $= \|f\|^2 + 2D$	${\mu'}_{\rho B} = \epsilon' \cdot N = \sqrt{AND}$ ${\sigma'}^2_{\rho B} = A\|f\|^2 + 2N{\epsilon'}^2$ $= A\|f\|^2 + 2AD$

Table 1: Mean and standard deviation of the watermark correlation.

Tight Frame:

$$P'_F = \frac{1}{2}\,\mathrm{erfc}\left(\frac{T'_\rho}{\sqrt{2}{\sigma'}_{\rho A}}\right) = \frac{1}{2}\,\mathrm{erfc}\left(\frac{T'_\rho}{\sqrt{2}\sqrt{A\|f\|^2 + AD}}\right) \quad (35)$$

In order for $P_F = P'_F$, we need

$$\frac{1}{2}\,\mathrm{erfc}\left(\frac{T_\rho}{\sqrt{2}\sqrt{\|f\|^2 + D}}\right) = \frac{1}{2}\,\mathrm{erfc}\left(\frac{T'_\rho}{\sqrt{2}\sqrt{A\|f\|^2 + AD}}\right)$$

so that

$$T'_\rho = \sqrt{A}T_\rho.$$

We have two cases to consider, $T_\rho \geq \mu_{\rho B}$ and $T_\rho < \mu_{\rho B}$.

(1) If $T_\rho \geq \mu_{\rho B}$, then $T'_\rho = \sqrt{A}T_\rho \geq \sqrt{A}\mu_{\rho B} = \mu'_{\rho B}$ and we have

$$P_M = \frac{1}{2} + \frac{1}{2}\,\mathrm{erf}\left(\frac{T_\rho - \mu_{\rho B}}{\sqrt{2}\sigma_{\rho B}}\right) \quad (36)$$

$$P'_M = \frac{1}{2} + \frac{1}{2}\,\mathrm{erf}\left(\frac{T'_\rho - \mu'_{\rho B}}{\sqrt{2}\sigma'_{\rho B}}\right) \quad (37)$$

$$\frac{T'_\rho - \mu'_{\rho B}}{\sqrt{2}\sigma'_{\rho B}} = \frac{\sqrt{A}T_\rho - \sqrt{A}\mu_{\rho B}}{\sqrt{2}\sqrt{A}\sigma_{\rho B}} = \frac{T_\rho - \mu_{\rho B}}{\sqrt{2}\sigma_{\rho B}}. \quad (38)$$

Therefore, we have $P_M = P'_M$.

(2) If $T_\rho < \mu_{\rho B}$, we have $T'_\rho < \mu'_{\rho B}$ and

$$P_M = \frac{1}{2}\,\mathrm{erfc}\left(\frac{\mu_{\rho B} - T_\rho}{\sqrt{2}\sigma_{\rho B}}\right) \quad (39)$$

$$P'_M = \frac{1}{2}\,\mathrm{erfc}\left(\frac{\mu'_{\rho B} - T'_\rho}{\sqrt{2}\sigma'_{\rho B}}\right) \quad (40)$$

$$\frac{\mu'_{\rho B} - T'_\rho}{\sqrt{2}\sigma'_{\rho B}} = \frac{\sqrt{A}\mu_{\rho B} - \sqrt{A}T_\rho}{\sqrt{2}\sqrt{A}\sigma_{\rho B}} = \frac{\mu_{\rho B} - T_\rho}{\sqrt{2}\sigma_{\rho B}}. \quad (41)$$

Again, we have $P_M = P'_M$.

That is, the probability of missed-detection error, P_M, is the same regardless of whether an orthonormal or tight-frame expansion is used.

5. CONCLUSIONS

The primary conclusion we draw from the above theoretical analysis is that a redundant expansion in the form of a tight frame yields less distortion than an orthonormal expansion when watermarked with a fixed watermark energy, yet the redundant expansion does not achieve performance advantages over the orthonormal basis for spread-spectrum watermarking detection. We conclude that the overcompleteness of the expansion, which aids the watermark insertion by accommodating greater watermark energy for a given distortion, actually hinders the correlation operator in watermark detection. As a result, the tight-frame expansion does not inherently offer greater spread-spectrum watermarking performance. We note that this analytical observation should be tempered with the fact that spread-spectrum watermarking is often deployed in conjunction with an image-adaptive weighting mask (e.g., [2]) so as to improve perceptual performance. In the case of image-adaptive watermarking, a redundant transform may offer advantages towards the computation of the weighting mask, as was the case in [6].

6. REFERENCES

[1] I. J. Cox, J. Killian, F. T. Leighton, and T. Sharmoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, December 1997.

[2] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 783–791, May 2001.

[3] M. J. Shensa, "The discrete wavelet transform: Wedding the À trous and mallat algorithms," *IEEE Transactions on Signal Processing*, vol. 40, no. 10, pp. 2464–2482, October 1992.

[4] I. Daubechies, *Ten Lectures on Wavelets*, Society for Industrial and Applied Mathematics, Philadelphia, PA, 1992.

[5] V. K. Goyal, M. Vetterli, and N. T. Thao, "Quantized overcomplete expansions in $\mathbb{R}^n$: Analysis, synthesis, and algorithms," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 16–31, January 1998.

[6] J.-G. Cao, J. E. Fowler, and N. H. Younan, "An image-adaptive watermark based on a redundant wavelet transform," in *Proceedings of the International Conference on Image Processing*, Thessaloniki, Greece, October 2001, pp. 277–280.

[7] L. Hua and J. E. Fowler, "Image watermarking and the redundant wavelet transform," Tech. Rep. MSSU-COE-ERC-01-18, Engineering Research Center, Mississippi State University, December 2001.