OPTIMAL LINEAR DETECTOR FOR SPREAD SPECTRUM BASED MULTIDIMENSIONAL SIGNAL WATERMARKING

Tuan T. Nguyen and David Taubman

University of New South Wales, Sydney, Australia

ABSTRACT

This paper presents a new efficient Spread Spectrum (SS) based watermarking technique for multidimensional signals. In this method, the Karhunen Loeve Transform (KLT) is used to completely decorrelate the components of the cover signal and obtain the maximum energy compaction. In order to improve the robustness, the same secret message is embedded into all components and linear fusion is used to exploit the collaboration among the local correlation detectors. Based on a theoretic analysis, the condition for perfect reconstruction of the KLT without the original signal is established. The performance of the proposed scheme is considered for both average and optimal detector and a closed-form expression of the optimal weighting coefficients to minimize the error probability is then derived. Experimental results are provided in the context of color image watermarking, with and without additive Gaussian noise attack.

Index Terms— watermarking, SS, KLT, multidimensional signal, optimization

1. INTRODUCTION

Watermarking is one of the modern data hiding technologies. It inserts information into multimedia without perceptiveness, which means only a small change in the original data. Many requirements for designing a watermarking system are imposed depending on applications and purposes of the watermarking. However, in real-world efficient watermarking systems, there are some common criteria including imperceptibility, robustness, payload, security, complexity and watermark recovery with or without the original data [1, 2, 3].

The first publications on watermarking were in the early 1990s by Tanaka (1990), Caroni and Tirkel (1993). Since 1995, digital watermarking has rapidly developed and has been applied in several fields such as copyright protection, fingerprinting, copy protection, broadcast monitoring, data authentication, data hiding, indexing, etc. Cox et al. [4] were among the first to exploit spread spectrum communication theory to develop watermarking algorithms. The basic idea of this approach is to add a zero-mean sequence with only two values to the host image. This sequence is generated from a PRN generator with a certain key. The watermark is extracted by using a correlation detector with the same key. Due to spreading the watermark over the whole image, this method yields invisibility as well as robustness. In addition, by using a key for the embedding and detecting process, it is also very secure. Other authors also used the spread spectrum concept but in different manners without the original signal in the recovery process. In general, this technique is computationally efficient. Such detectors are suitable to applications in copyright protection and copy control [5]. However, in this method, the original signal itself is a source of interference, so embedding the watermark into the high energy components of the cover signal can cause some errors [6].

Although various watermarking techniques have been researched widely, extension to multidimensional signals such as color images, hyperspectral images, etc. presents many opportunities. In most cases, this extension is carried out by embedding the watermark directly into one specified component of the cover signal such as the blue channel of RGB color space [7], the luminance component of YUV color space [8] or by processing each component separately [9] without examining the correlation between components. Piva et al. [10] exploited the cross-correlation of RGB-channels by designing a global correlation-based detector that takes into account the information carried out by all the three color channels, thus the performance of the system is improved. However, this technique is only examined for the average combination in the global detector and very difficult to derive a optimum detection strategy. In addition, it requires the host signal in the detecting process. Unlike the work by Piva et al., Barni et al. [11] exploited the complete decorrelation property of KLT to embed the watermark across all KL-transformed bands. By dealing with uncorrelated components, the optimum detector algorithm based on Bayes statistical decision theory can be derived. Unfortunately, one disadvantage of the KLT is that it depends on host signal statistics. Therefore, the results in [11] is only valid under assumption that the difference between the covariance matrix of the watermarked image and that of the original image is not too much.

In our paper, a new robust blind SS based multidimensional signal watermarking system is presented. Unlike the average combination in the global detector in [10], we use an adaptive linear weighting vector to improve robustness. It is obvious that if a component generates a high correlation detector that may lead to correct detection on its own, it should be assigned a larger weighting coefficient. On the contrary, for those components that have low correlation detectors, their weights are decreased in order to reduce their negative contribution to the decision fusion. Consequently, the performance of the proposed watermarking system is improved in general. In order to derive the closed-form expressions for the optimal weighting factors and error probability, the KLT is used to decorrelate completely components of the cover signal. However, unlike some hypotheses in [11], the watermark in this case is selected so that perfect reconstruction of KLT is obtained without the original signal under no attack or uncorrelated attacks. In addition, issue of selecting the watermark strength with respect to the energy of each component of the cover signal is also addressed.

The rest of this paper is organized as follows. In Section 2, first, the proposed embedding and detecting schemes are explained and formulated. Second, the condition for perfect reconstruction of the KLT without the original signal is established. Based on theoretical analysis, the closed-form expressions for the error probability are then given for both average and optimal weighting factors. Experimental results are presented in Section 3 to demonstrate the preeminence of the optimal linear correlation-based detector compared to approaches using only one detector corresponding to the principal component of the color images. Section 4 summarizes and concludes the paper.

2. PROBLEM STATEMENT AND SOLUTION

2.1. Analysis of embedding and detection process

We consider the embedding process of the general spread spectrum based watermarking system for multidimensional signals as shown in Fig. 1.

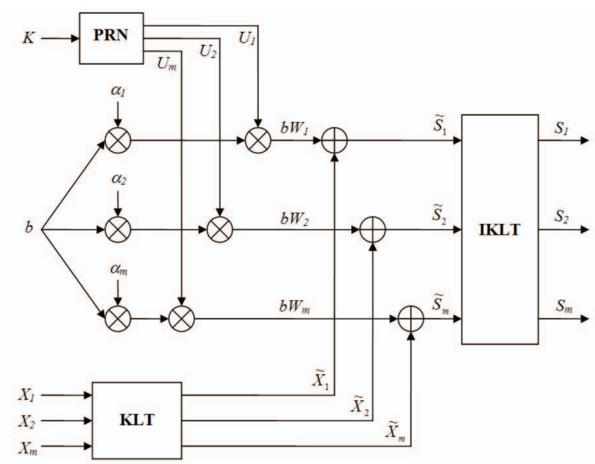


Fig. 1. Embedding process.

Let $\mathbf{X} = [X_1, X_2, \cdots, X_m]^T$ be the vector containing m components corresponding to the number of dimensions of the cover signal. Firstly, this cover signal is completely decorrelated using KLT as

$$\widetilde{\mathbf{X}} = \begin{bmatrix} \widetilde{X}_1 \\ \widetilde{X}_2 \\ \cdots \\ \widetilde{X}_m \end{bmatrix} = \mathbf{\Phi_X}^T\mathbf{X} = \begin{bmatrix} \phi_{\mathbf{X}1}^T \\ \phi_{\mathbf{X}2}^T \\ \cdots \\ \phi_{\mathbf{X}m}^T \end{bmatrix} \mathbf{X} \tag{1}$$

where $\phi_{\mathbf{X}k}$ is the eigenvector corresponding to the kth eigenvalue $\lambda_{\mathbf{X}k}$ of the covariance matrix $\mathbf{\Sigma_X}$ of the signal vector $\mathbf{X}$, i.e.,

$$\mathbf{\Sigma_X}\phi_{\mathbf{X}_k} = \lambda_{\mathbf{X}k}\phi_{\mathbf{X}_k} \qquad (k = 1, \cdots, m) \tag{2}$$

Next, a secret key K is used by a PRN to produce the orthogonal sequences $\mathbf{U} = [U_1, U_2, \cdots, U_m]^T$ with zero-mean and whose elements are equal to $+1$ or -1. Each sequence U_i is then added to each component of eigen-signal $\widetilde{X}_i$ obtained after KLT according to the variable b and the strength factor α_i, where b assumes the values of $+1$ or -1 according to the bit transmitted by the watermarking process as shown below

$$\widetilde{S}_i = \widetilde{X}_i + bW_i = \widetilde{X}_i + b\alpha_i U_i. \tag{3}$$

Finally, the inverse KLT is used to obtain the watermarked signal

$$\mathbf{S} = \mathbf{\Phi_X}\widetilde{\mathbf{S}} = \sum_{i=1}^{m} \widetilde{S}_i\phi_i.$$

The distortion D in the embedded signal is defined by

$$D = \|\mathbf{S} - \mathbf{X}\| = \frac{1}{m}\sum_{i=1}^{m}\alpha_i^2. \tag{4}$$

where

$$\|x\| \triangleq \langle x, x\rangle, \quad \text{and} \quad \langle x, u\rangle \triangleq \frac{1}{N}\sum_{i=0}^{N-1} x_i u_i \tag{5}$$

with N is the length of the vectors x, u.

To derive the closed-form expressions for the optimal weighting factors and the error probability, the channel is modeled as additive noise:

$$\mathbf{Y} = \mathbf{S} + \mathbf{N}. \tag{6}$$

and each component of the eigen-signal $\widetilde{\mathbf{X}}$ and the noise $\mathbf{N}$ is assumed to be independent identically distributed Gaussian random processes, i.e,

$$\widetilde{X}_i \sim \mathcal{N}(0, \sigma^2_{\widetilde{X}_i}) \quad \text{and} \quad \widetilde{N}_i \sim \mathcal{N}(0, \sigma^2_N) \tag{7}$$

On the detection side, the KLT is used again for the received signal $\mathbf{Y}$ and each component of the eigen-signal $\widetilde{\mathbf{Y}} = \mathbf{\Phi_Y}^T\mathbf{Y}$ is brought to each local correlation detector as shown in Fig. 2.

$$r_i = \langle \widetilde{Y}_i, U_i\rangle = \alpha_i b + \langle \widetilde{X}_i, U_i\rangle + \langle \widetilde{N}_i, U_i\rangle \tag{8}$$

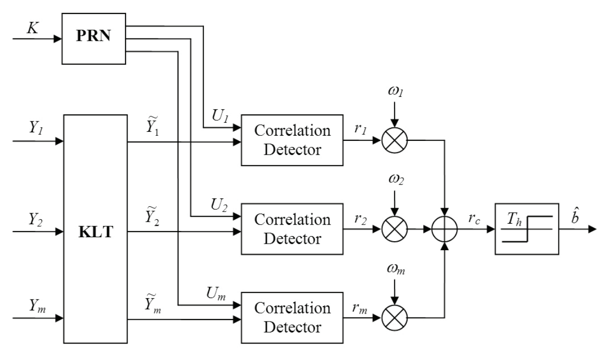


Fig. 2. Detecting process.

It is easily seen that the correlation detector with respect to each component is also Gaussian process, i.e. $r_i \sim \mathcal{N}(\overline{r}_i, \sigma^2_{r_i})$ where

$$\overline{r}_i = b\alpha_i = \{-1, 1\}\alpha_i, \text{ and } \sigma^2_{r_i} = \frac{\sigma^2_{\widetilde{X}_i} + \sigma^2_N}{N} = \frac{\sigma^2_{\widetilde{Y}_i} - \alpha_i^2}{N} \tag{9}$$

Next, a global test statistic is calculated linearly as

$$r_c = \sum_{i=1}^{m}\omega_i r_i. \tag{10}$$

where $\{\omega_i \geq 0\}$ are the weighting coefficients used to control the global correlation detector.

Since r_i are normal random variables, their linear combination is also normal. Consequently, r_c has mean and variance

$$\overline{r}_c = E[r_c] = \sum_{i=1}^{m} b\alpha_i\omega_i. \tag{11}$$

$$\sigma^2_{r_c} = E[(r_c - \overline{r}_c)^2] = \sum_{i=1}^{m}\sigma^2_{r_i}\omega_i^2. \tag{12}$$

The extracting bit is determined by the sign of the global correlation detector

$$\widehat{b} = \text{sign}(r_c). \tag{13}$$

The error probability of the proposed watermarking system then can be evaluated as a function of signal to noise ratio (SNR):

$$p = \frac{1}{2}\text{erfc}\Big(\frac{SNR}{\sqrt{2}}\Big). \tag{14}$$

where

$$SNR = \frac{\overline{r}_c}{\sigma_{r_c}} = \frac{\sum_{i=1}^{m} \alpha_i \omega_i}{\sqrt{\sum_{i=1}^{m} \sigma_{r_i}^2 \omega_i^2}}. \tag{15}$$

2.2. Perfect reconstruction for the KLT

It is noted that, for the watermark embedding, the KLT is based on the original signal, while, for watermark detecting, it is reconstructed from the watermarked signal. Therefore, it is important to design the watermark so that it has no effect on the KLT in the case of the absence of attack. The condition for the perfect reconstruction is given by:

$$\mathbf{\Phi_Y} = \mathbf{\Phi_S} = \mathbf{\Phi_X}. \tag{16}$$

We will prove that by designing $\mathbf{W}$ orthogonal and independent with $\mathbf{X}$ as we proposed, the equation (16) is satisfied.

From equation (3), we have

$$\mathbf{S} = \mathbf{X} + b\mathbf{\Phi_X}\mathbf{W}. \tag{17}$$

Notice that $\mathbf{X}$ and $\mathbf{W}$ are independent, so we have

$$\mathbf{\Sigma_S} = \mathbf{\Sigma_X} + \mathbf{\Phi_X}\mathbf{\Sigma_W}\mathbf{\Phi_X}^T. \tag{18}$$

Furthermore, since $\mathbf{\Sigma_X}$ is symmetric, $\mathbf{\Phi_X}$ is orthogonal matrix, i.e. $\mathbf{\Phi_X}^T = \mathbf{\Phi_X}^{-1}$. So we have

$$\mathbf{\Phi_X}^T\mathbf{\Sigma_S}\mathbf{\Phi_X} = \mathbf{\Phi_X}^T\mathbf{\Sigma_X}\mathbf{\Phi_X} + \mathbf{\Sigma_W} = D_\mathbf{X} + \mathbf{\Sigma_W}. \tag{19}$$

where $\mathbf{D_X}$ is the diagonal matrix corresponding to the eigenvalues $\lambda_{\mathbf{X}k}$, $(k = 1, \cdots, m)$.

Obviously, the condition $\mathbf{\Phi_S} = \mathbf{\Phi_X}$ in equation (16) is satisfied if and only if $\mathbf{\Sigma_W}$ is diagonal, i.e. $\mathbf{W}$ is orthogonal. Thus, the watermark has no impact on the reconstruction KLT from the watermarked signal without attack. In general, perfect reconstruction is rarely obtained in the case of the presence of attacks except for the additive Gaussian noise. From (6) and (7) we have above:

$$\mathbf{\Phi_X}^T\mathbf{\Sigma_Y}\mathbf{\Phi_X} = \mathbf{\Phi_X}^T\mathbf{\Sigma_S}\mathbf{\Phi_X} + \mathbf{\Phi_X}^T\mathbf{\Sigma_N}\mathbf{\Phi_X} = \mathbf{D_X} + \mathbf{\Sigma_W} + \mathbf{\Sigma_N}. \tag{20}$$

It is clear that the right side of (20) is diagonal, so the condition $\mathbf{\Phi_Y} = \mathbf{\Phi_X}$ in the equation (16) is satisfied.

2.3. Average weighting vector

Based on the condition of perfect reconstruction, we consider the detector with the equal weighting coefficients. From (14), the error probability of the average detector is given by

$$p_{ave} = \frac{1}{2}\text{erfc}\Big(\frac{\sum_{i=1}^{m} \alpha_i}{\sqrt{2}\sqrt{\sum_{i=1}^{m} \sigma_{r_i}^2}}\Big). \tag{21}$$

With the given distortion D, the error probability of the average detector is minimized if and only if the watermark strength for each component is equal, i.e. $\alpha_i = \alpha_j = \sqrt{D}$ and

$$p_{ave}^{min} = \frac{1}{2}\text{erfc}\Big(\frac{m\sqrt{D}}{\sqrt{2}\sqrt{\sum_{i=1}^{m} \sigma_{r_i}^2}}\Big). \tag{22}$$

It is clear that, when m increases, the performance of the average detector in (22) is much better than that of each local detector.

2.4. Optimal weighting vector

Instead of using the average detector as discussed above, the weighting vector $\omega = [\omega_1, \omega_2, ..., \omega_M]^T$ is now chosen to minimize the error probability by setting the derivative of p in (14) to zero:

$$\frac{\omega_{i_{opt}}}{\omega_{j_{opt}}} = \frac{\alpha_i}{\alpha_j}\frac{\sigma_{r_j}^2}{\sigma_{r_i}^2}. \tag{23}$$

Substituting (23) into (14) we obtain

$$p_{opt} = \frac{1}{2}\text{erfc}\Big(\frac{1}{\sqrt{2}}\sqrt{\sum_{i=1}^{m}\frac{\alpha_i^2}{\sigma_{r_i}^2}}\Big). \tag{24}$$

3. EXPERIMENTAL RESULTS

Firstly, we investigate the performance of both detectors in some special cases of the watermark strength. Fig. 3 shows the comparison of error probability for average and optimal detectors with uniform and proportional watermark strength. In the latter case, the watermark strength is selected so that the error probability of each component is equal, i.e. $\alpha_i/\alpha_j = \sigma_{r_i}/\sigma_{r_j}$. The distortion is fixed for both cases. From Fig. 3, it can be seen that the error probability of the optimal detector is always less than that of the average detector. It is also noted that the performance of the optimal detector with the proportional watermark strength is the same as that of the average detector with the uniform watermark strength. Therefore, uniform watermark strength is the effective solution for both average and optimal detectors when the degradation of the watermarked signal is only measured by the MSE metric.

Based on the above results, we demonstrate watermarking for color images. First, the pixels at the same position of the original RGB bands are transformed into a vector of size 3×1 and considered as one observation of the signal vector $\mathbf{X}$. Second, the KLT is calculated and applied to this signal vector to obtain three eigen-images. The watermark with the suitable watermark strength then is embedded separately into these eigen-images according to the transmitted bit and transformed inversely into spatial domain to obtain the watermarked image. In order to measure the quality of the watermarked image, the peak signal to noise ratio (PSNR) is used as a quantitative index. This index is defined by:

$$PSNR = 10\log_{10}\frac{255^2}{D}. \tag{25}$$

where D is the distortion between the watermarked image and the original image as given in (4).

The new KLT-based method using the linear detector has been compared with techniques embedding the watermark into only one specified component such as the blue channel [7], luminance component [8] or the most principle KL-transformed component. Fig. 4

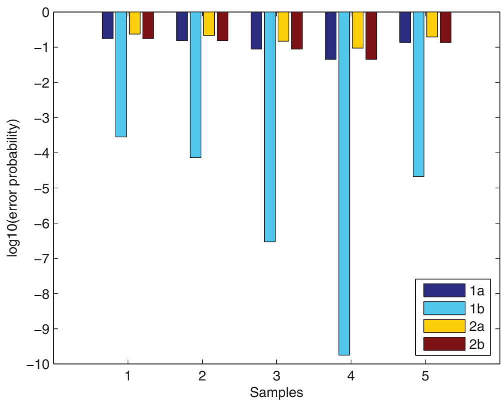


Fig. 3. Comparison of error probability of the average (a) and optimal (b) detectors with respect to different selections of the watermark strengths. (1) $\alpha_i = \alpha_j$. (2) $\alpha_i/\alpha_j = \sigma_{r_i}/\sigma_{r_j}$.

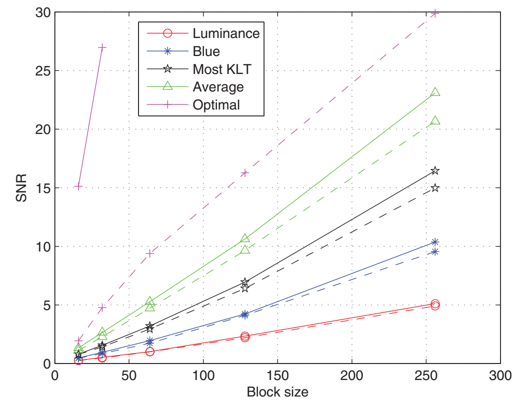
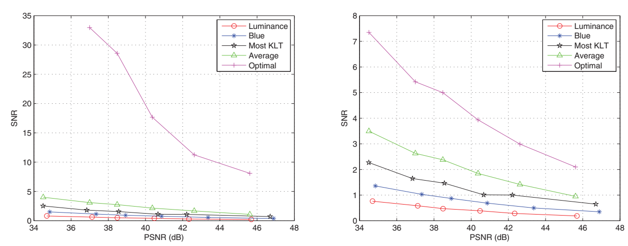


Fig. 5. SNR as a function of block size. Solid lines correspond to the case of absence of attack and dashed lines correspond to the case of Gaussian noise.

shows the performance of detector SNR versus the quality of watermarked image $PSNR$ without attack and with Gaussian noise. Obviously, the better the quality of the watermarked image, the worse the performance of the system becomes. From Fig. 4, it can be concluded that our proposed scheme outperforms the method using only a single detector both cases under no attack and with Gaussian noise.



(a) Without attack (b) Gaussian noise

Fig. 4. SNR versus PSNR.

Finally, we examine the effect of block size to the performance of the system. Fig. 5 shows that the larger the block size, the more improvement there is in the error probability of our proposed scheme compared to methods embedding the watermark into specified components of the cover signal both in the absence and presence of attack. However, the larger the block size is, the less bits can be embedded.

4. CONCLUSIONS

In this paper, we have proposed a novel approach for multidimensional signal watermarking. By using KLT and an optimal linear combination of the correlation detectors, the performance of the proposed system is improved significantly, especially in the case of the uniform watermark strength. In addition, this method does not require the original signal in the detecting process while perfect reconstruction is still satisfied. Furthermore, the implementation of color image watermarking based on this technique is also investigated.

5. REFERENCES

[1] "Special issue on signal processing for data hiding in digital media and secure content delivery," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, April 2003.

[2] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding techniques for steganography and digital watermarking*, Security Technologies for the World Wide Web, Rolf Oppliger.

[3] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data," *IEEE Signal Processing Magazine*, vol. 17, no. 5, September 2000.

[4] I. J. Cox, J. Kilian, T. Leighton, and T. G. Shamoon, "Cox's dct, additive, non-blind image watermarking algorithm," in *Proc. ICIP*, California, 1997, pp. 1673–1687.

[5] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673–1687, December 1997.

[6] I. Cox, M. Miller, and A. McKellips, "Watermarking as communications with side information," in *Proc. IEEE*, July 1999, vol. 87, pp. 1127–1141.

[7] M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of colour images using amplitude modulation," *Journal of Electronic Imaging*, vol. 7, no. 2, 1998.

[8] R. B. Wolfgang and E. J. Delp, "A watermark for digital images," vol. 3, pp. 219–222, September 1996.

[9] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Processing*, vol. 66, no. 3, pp. 385–403, May 1998.

[10] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "Exploiting the cross-correlation of rgb-channels for robust watermarking of color images," in *Proc. ICIP*, Kobe, Japan, October 1999, vol. 1, pp. 306–310.

[11] M. Barni, F. Bartoloni, A. De Rosa, and A. Piva, "Color image watermarking in the karhunen-loeve transform domain," *Journal of Electronic Imaging*, vol. 11, no. 1, 2002.