Information-theoretic resolution of perceptual WSS watermarking of non i.i.d. Gaussian signals

Gaëtan Le Guelvouit, Stéphane Pateux and Christine Guillemot
IRISA/INRIA, Campus de Beaulieu,
35042 Rennes Cedex, FRANCE
Tel: +33 2 99 84 73 60; fax: +33 2 99 84 25 31
e-mail: Gaetan.Le_Guelvouit@irisa.fr

ABSTRACT

The theoretical foundations of data hiding have been revealed by formulating the problem as message communication over a noisy channel. We revisit the problem in light of a more general characterization of the watermark channel and of weighted distortion measures. Considering spread spectrum based information hiding, we release the usual assumption of an i.i.d. cover signal. The game-theoretic resolution of the problem reveals a generalized characterization of optimum attacks. The paper then derives closed-form expressions for the different parameters exhibiting a practical embedding and extraction technique.

1 INTRODUCTION

Information hiding refers to nearly invisible embedding of a message within a host signal. This paper focuses on the data hiding problem, assuming a blind and symmetric system. In the spirit of a communication problem one seeks the maximum rate of reliable transmission over any hiding and attack strategies. This rate is called the hiding capacity and depends on admissible distortion levels and on the watermark channel characterization.

Watermarking is often regarded as a form of spread spectrum communication with various forms of channel characterizations. The perceptual sensitivity of the host signal is often taken into account for choosing embedding sites and strength [1, 7]. The attacks are often modelled as the addition of White Gaussian noise (AWGN) [8, 4], or as linear filtering plus additive noise [9, 3]. The authors in [10] show that the optimum attack is obtained by Wiener filtering and that to be maximally robust, the watermark should have a power spectrum matching the one of the original signal.

The problem of robust embedding and extraction based on spread spectrum is revisited here in light of a more general model of the cover signal and of the watermark channel. Most of the approaches introduced so far consider that the cover signal can be modelled as an ergodic wide sense stationary Gaussian random process. This assumption is rarely satisfied for real signals. We assume instead that it can be modelled as the realization of a set of independent non identically distributed Gaussian random variables (referred to as non i.i.d. signals). The attack channel is considered to be of the type amplitude scaling and additive white Gaussian noise (SAWGN) [2]. The game-theoretic resolution of the problem with weighted distortion measures leads to a characterization of optimum attack domains. By maximizing the watermarking channel signal to noise ratio, we then derive a closed-form expression of the watermark spectral density corresponding to the best defense. The performance limits of the approach in terms of hiding capacity are then analyzed. The approach can be seen as a generalization of previous work to the case of non i.i.d. Gaussian sources, considering weighted distortion measures and a more general SAWGN attack channel, with the exhibition of closed-form expressions for a practical embedding and extraction scheme.

2 PROBLEM STATEMENT

Let $\underline{\mathbf{b}} = \{b_1, b_2, \dots, b_n\}$ with $b_i \in \{-1, +1\}$ $\forall i \in \{1, 2, \dots, n\}$ be the message to be embedded in a host signal $\underline{\mathbf{x}}$. Many approaches introduced so far assume that the signal $\underline{\mathbf{x}}$ can be modelled as an ergodic zero-mean wide sense stationary Gaussian random process [4, 9]. This assumption is rarely satisfied for real signals or for content adaptive watermarks. We assume instead that the host signal $\underline{\mathbf{x}}$ can be modelled as the realization of a set of non stationary Gaussian random variables $\underline{\mathbf{X}} = \{X_1, X_2, \dots, X_m\}$ where $X_i \sim \mathcal{N}(0, \sigma_{X_i})$. The information is then used as a key for indexing pseudo-random noise sequences which are additively combined with the signal. Let $\underline{\mathbf{G}}$ be a $n \times m$ matrix composed of n pseudo-random generated vectors $\underline{\mathbf{G}_j} \in \{-1, +1\}^m$. The watermarked signal is obtained by

$$y_i = x_i + w_i = x_i + \alpha_i \sum_{j=1}^{n} G_{i,j} b_j, \quad (1)$$

where x_i represents the i^{th} site of the host signal and y_i the corresponding watermarked site. In order to extract each embedded bit b_i, a correlation product between the vector $\underline{\mathbf{G}_j}$ and $\underline{\mathbf{y}}$ is computed. The term α_i is a weighting factor allowing to adjust the amplitude (or energy) of the mark. In the following we derive a closed-form expression of this parameter in the case of SAWGN attacks, with weighted distortion measures and non i.i.d Gaussian cover signals. The attack channel is often assumed to be AWGN [6]. This model assumes that the distortion induced by the attack is independent of the watermarked signal, hence can hardly apply to attacks such as filtering and compression. More accurate models assuming that the distortion depends on the watermarked signal and based on linear filtering plus additive noise have been considered in [9, 3]. Here, we consider that the attacked signal $\underline{\mathbf{y}'}$ can be expressed as

$$y'_i = \gamma_i y_i + \delta_i = \gamma_i x_i + \gamma_i \alpha_i \sum_{j=1}^{n} G_{i,j} b_j + \delta_i, \qquad (2)$$

where γ_i is an attenuation factor on each watermarked site. This amounts to consider the attack channel as a SAWGN channel (amplitude scaling by the factor γ_i, and additive white Gaussian noise of $\delta_i \sim \mathcal{N}(0, \sigma_{\delta_i}^2)$).

The distortion measure is defined as a weighted sum of the MSE on each sample of the host signal, in order to reflect the perceptual quality. The embedding distortion is therefore given by

$$D_{xy} = E\left[\sum_{i=1}^{m} \varphi_i^2 \left(y_i - x_i\right)^2\right] = \sum_{i=1}^{m} \varphi_i^2 n \alpha_i^2, \qquad (3)$$

where φ_i is a perceptual factor. Similarly, the expected attack distortion is given by

$$D_{xy'} = \sum_{i=1}^{m} \varphi_i^2 \left(\sigma_{X_i}^2 \left(1-\gamma_i\right)^2 + n\gamma_i^2 \alpha_i^2 + \sigma_{\delta_i}^2\right). \qquad (4)$$

3 MAP WATERMARK ESTIMATION

The *maximun a posteriori* (MAP) estimation of the bit b_j is defined as

$$\widehat{b_j} = \arg\max_{b_j} \left\{P(B_j = b_j \,|\, Y'^m = \underline{\mathbf{y}'})\right\}. \qquad (5)$$

The a posteriori probability $\mathcal{P} = P(B_j = b_j \,|\, Y'^m = \underline{\mathbf{y}'})$ can be rewritten (using Bayes law) as

$$\mathcal{P} = \frac{P(Y'^m = \underline{\mathbf{y}'} \,|\, B_j = b_j) \times P(B_j = b_j)}{P(Y'^m = \underline{\mathbf{y}'})}. \qquad (6)$$

Since the received vector $\underline{\mathbf{y}'}$ is fixed, and that no a priori knowledge on the message $\underline{\mathbf{b}}$ is assumed, we have the a posteriori probability $\mathcal{P} \propto P(Y'^m = \underline{\mathbf{y}'} \,|\, B_j = b_j)$, where $\propto$ denotes an obvious renormalization. Assuming that the watermarked sites are independent, it can be shown [5] that the quantity can be expressed as a product of Gaussian distributions of the form $\mathcal{P}_i \sim \mathcal{N}(0, \gamma_i^2(\sigma_{X_i}^2 + \alpha_i^2(n-1)) + \sigma_{\delta_i}^2)$, i.e. as

$$\begin{aligned}\mathcal{P} &\propto \prod_{i=1}^{m} \frac{1}{\sqrt{2\pi}\sqrt{\gamma_i \sigma_{X_i^2} + \alpha_i^2(n-1)) + \sigma_{\delta_i}^2}} \\ &\quad \exp\left[-\frac{\left(y'_i - \gamma_i \alpha_i b_j G_{i,j}\right)^2}{2\left(\gamma_i^2(\sigma_{X_i}^2 + \alpha_i^2(n-1)) + \sigma_{\delta_i}^2\right)}\right], \qquad (7)\\ &\propto \frac{C}{2} \exp \frac{-\Lambda}{2}, \qquad (8)\end{aligned}$$

where C is a constant and

$$\Lambda = \sum_{j=1}^{n} \frac{\left(b_j - \widehat{b_j}\right)^2}{\sigma_{b_j}^2} \qquad (9)$$

with

$$\widehat{b_j} = \frac{\sum_{i=1}^{m} \frac{\gamma_i \alpha_i y'_i G_{i,j}}{\gamma_i^2(\sigma_{X_i}^2 + \alpha_i^2(n-1)) + \sigma_{\delta_i}^2}}{\sum_{i=1}^{m} \frac{\gamma_i^2 \alpha_i^2}{\gamma_i^2(\sigma_{X_i}^2 + \alpha_i^2(n-1)) + \sigma_{\delta_i}^2}}, \qquad (10)$$

$$\sigma_{b_j}^2 = \left(\sum_{i=1}^{m} \frac{\gamma_i^2 \alpha_i^2}{\gamma_i^2(\sigma_{X_i}^2 + \alpha_i^2(n-1)) + \sigma_{\delta_i}^2}\right)^{-1}. \qquad (11)$$

The term $\widehat{b_j}$ represents the optimal estimator. From Eqn.(8) and (9), watermarking channel can be seen as a gaussian channel. Estimator's performance can be measured in terms of the signal to noise ratio E_b/N_0 of the watermarking channel. This quantity is defined as the ratio between the energy of the embedded bit and the overall noise introduced by the cover signal ($\sigma_{X_i}^2$), by the other embedded bits ($\alpha_i^2(n-1)$) and by the attack (i.e. $\sigma_{\delta_i}^2$). It is then expressed as

$$\frac{E_b}{N_0} = \frac{E(b_j^2)}{\sigma_{b_j}^2} = \frac{1}{\sigma_{b_j}^2} = \sum_{i=1}^{m} \rho_i, \qquad (12)$$

where

$$\rho_i = \frac{\alpha_i^2 \gamma_i^2}{\gamma_i^2(\sigma_{X_i}^2 + \alpha_i^2(n-1)) + \sigma_{\delta_i}^2}. \qquad (13)$$

4 GAME-THEORETIC RESOLUTION

The optimization of the embedding and attack parameters can be formulated as a game between an attacker and a hider. The attack searches the two vectors $\underline{\gamma}$ and $\underline{\sigma_\delta}$ minimizing the extractor performance (i.e. E_b/N_0) while maintaining the distortion below an acceptable level ($D_{xy'} < D_{xy'}^{\max}$). This problem can be solved by a Lagrangian optimization:

$$(\underline{\gamma^\star}, \underline{\sigma_{\delta^\star}}) = \arg\min_{\underline{\gamma}, \underline{\sigma_\delta}} \left\{ J_\lambda = \frac{E_b}{N_0} + \lambda\left[D_{xy'} - D_{xy'}^{\max}\right]\right\},$$

where $\lambda > 0$ is a Lagrangian multiplier. From Eqn.(4) and (12) it appears that J_λ is an additive functional. The optimization can then be made separately on each $J_{\lambda,i}$ given by

$$J_{\lambda,i}(\gamma_i, \sigma_{\delta_i}) = \rho_i + \lambda\varphi_i^2\left(\sigma_{X_i}^2(1-\gamma_i)^2 + n\gamma_i^2\alpha_i^2 + \sigma_{\delta_i}^2\right)$$

by setting its derivatives with respect to the attack parameters γ_i and σ_{δ_i}

$$\begin{aligned}\frac{\partial J_{\lambda,i}}{\partial \gamma_i} &= 2\frac{\gamma_i \alpha_i^2 \sigma_{\delta_i}^2}{\left(\gamma_i^2\left(\sigma_{X_i}^2 + \alpha_i^2\left(n-1\right)\right) + \sigma_{\delta_i}^2\right)^2} \\ &\quad + 2\lambda\varphi_i^2\left(n\gamma_i\alpha_i^2 - \sigma_{X_i}^2\left(1-\gamma_i\right)\right), \qquad (14)\end{aligned}$$

and

$$\frac{\partial J_{\lambda,i}}{\partial \sigma_{\delta_i}} = \frac{-2\gamma_i^2\alpha_i^2\sigma_{\delta_i}}{\left(\gamma_i^2\left(\sigma_{X_i}^2 + \alpha_i^2\left(n-1\right)\right) + \sigma_{\delta_i}^2\right)^2} + 2\lambda\varphi_i^2\sigma_{\delta_i} \qquad (15)$$

to zero on the validity domain. The resolution of the resulting set of equations leads to the following two expressions for $\sigma^2_{\delta_i}$:

$$\sigma^2_{\delta_i} = -\gamma_i \left[n\gamma_i\alpha_i^2 - \sigma^2_{X_i}\left(1-\gamma_i\right)\right] \qquad (16)$$

and

$$\sigma^2_{\delta_i} = \gamma_i \left[\frac{\alpha_i}{\sqrt{\lambda}\varphi_i} - \gamma_i\left(\sigma^2_{X_i} + \alpha_i^2(n-1)\right)\right]. \qquad (17)$$

Equating Eqn.(16) and (17) leads to the optimum values

$$\gamma_i^\star = \frac{\sqrt{\lambda}\varphi_i\sigma^2_{X_i} - \alpha_i}{\sqrt{\lambda}\varphi_i\alpha_i^2} \qquad (18)$$

and

$$\sigma^2_{\delta_i^\star} = \gamma_i^\star\left(\gamma_{wi} - \gamma_i^\star\right)\left(\sigma^2_{X_i} + n\alpha_i^2\right), \qquad (19)$$

where $\gamma_{wi} = \frac{\sigma^2_{X_i}}{\sigma^2_{X_i}+\sigma^2_{wi}}$, and $\sigma^2_{wi} = n\alpha_i^2$. The term γ_{wi} represents the response of a Wiener filter. Since the attack parameters $\sigma^2_{\delta_i^\star}$ and $\gamma_i^\star$ must verify $\sigma^2_{\delta_i^\star} \geq 0$ and $\gamma_i^\star \geq 0$, the solutions of Eqn.(18) and (19) are valid only for

$$\mu - \alpha_i \geq 0 \qquad (20)$$

$$\left(\alpha_i - \mu\right)\left(\sigma^2_{X_i} + n\alpha_i^2\right) + \mu\alpha_i^2 \geq 0, \qquad (21)$$

where $\mu = \sqrt{\lambda}\varphi_i\sigma^2_{X_i}$. This set of inequations defines three domains $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$ shown in Fig. 1.

The optimum attacks can then be characterized in terms of the domains of validity of the attack parameters γ_i and σ_{δ_i}. Let us first consider their limits of validity ($\gamma_i = 0$ and $\sigma_{\delta_i} = 0$). If $\gamma_i^\star = 0$ (the marked value y_i is erased), a minimum is obtained for $\sigma_{\delta_i^\star} = 0$. A greater value for the additive noise will increase $D_{xy'}$ but will not decrease E_b/N_0. This attack is referred to as the **Erase** attack. If $\sigma_{\delta_i} = 0$, another minimum is given by $\gamma_i^\star = \gamma_{wi}$. This attack is a **Wiener** filtering. The last attack (defined for $\gamma_i^\star > 0$ and for $\sigma_{\delta_i^\star} > 0$) is a combination of filtering and additive Gaussian noise. This is called here the **Intermediate** attack. Table 1 gives the corresponding expressions of the cost function $J_{\lambda,i}(\gamma_i, \sigma_{\delta_i})$ denoted J_E, J_W and J_I for respectively the erase, Wiener and intermediate attacks. To find the optimum attack, one has to find on each domain (defined in terms of α_i and σ_{X_i}), the attack that will minimize

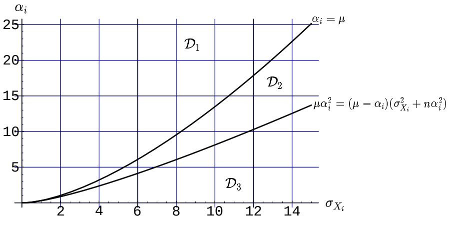

Figure 1: Domains defined by the validity constraints $\gamma_i^\star \geq 0$ and $\sigma_{\delta_i^\star} \geq 0$ ($\lambda = 0.2$, $\chi = 0.002$, $n = 1$ bit).

	Value of $J_{\lambda,i}(\gamma_i, \sigma_{\delta_i})$
J_E	$\lambda\varphi_i^2\sigma^2_{X_i}$
J_W	$\frac{\alpha_i^2}{\sigma^2_{X_i}+\alpha_i^2(n-1)} + \lambda\frac{n\varphi_i^2\alpha_i^2\sigma^2_{X_i}}{\sigma^2_{X_i}+n\alpha_i^2}$
J_I	$2\sqrt{\lambda}\varphi_i\frac{\sigma^2_{X_i}}{\alpha_i} - 1 + \lambda\varphi_i^2\sigma^2_{X_i}\left(1 - \frac{\sigma^2_{X_i}}{\alpha_i^2}\right)$

Table 1: Cost function $J_{\lambda,i}(\gamma_i, \sigma_{\delta_i})$ for the different types of attack (Erase, Wiener, Intermediate).

$J_{\lambda,i}(\gamma_i, \sigma_{\delta_i})$. From table 1 and constraints (20)-(21) the minimum values of $J_{\lambda,i}(\gamma_i, \sigma_{\delta_i})$, in the domains of validity of γ_i and σ_{δ_i}, are given by J_E and J_W on $\mathcal{D}_1$ and $\mathcal{D}_3$ respectively (see [5] for details). Similarly, on $\mathcal{D}_2$, $J_I \leq J_E$ and $J_I \leq J_W$. Thus, if the validity constraint $\gamma_i^\star \geq 0$ of the Intermediate attack domain is satisfied, the optimum attack is given by the Intermediate attack (with parameters given by Eqn.(18) and (19)). Otherwise, the attacker should use instead the Erase or the Wiener solution.

Given the optimum attack, we then search the parameters α_i (strength of the watermark) that maximize E_b/N_0, under constraints of a maximum watermarked signal distortion ($D_{xy}^{\max}$). This leads to a Lagrangian approach:

$$\underline{\alpha}^\star = \arg\max_{\underline{\alpha}} \left\{ J_\chi = J_\lambda - \chi\left[D_{xy} - D_{xy}^{\max}\right]\right\}, \qquad (22)$$

where $\chi > 0$ is a Lagrangian multiplier. The cost function J_χ being the additive functional $J_\chi = \sum_i^m J_{\lambda,i}(\gamma_i, \sigma_{\delta_i}) - \chi\left[D_{xy} - D_{xy}^{\max}\right]$, the optimization can be carried out separately on each $J_{\chi,i}(\alpha_i) = J_{\lambda,i}(\gamma_i, \sigma_{\delta_i}) - \chi n\varphi_i^2\alpha_i^2$. Let us consider the three attack strategies. In the case of the Erase attack, i.e. $(\alpha_i, \sigma_{X_i}) \in \mathcal{D}_1$, $J_{\chi,i}(\alpha_i) = \lambda\varphi_i^2\sigma^2_{X_i} - \chi n\varphi_i^2\alpha_i^2$. The function $J_{\chi,i}(\alpha_i)$ is a decreasing function and the minimum valid value of α_i is given by $\alpha_i^\star = \sqrt{\lambda}\varphi_i\sigma^2_{X_i}$. In $\mathcal{D}_2$, setting the derivative

$$\frac{\partial J_{\chi,i}}{\partial\alpha_i} = -2\frac{\sqrt{\lambda}\varphi_i\sigma^2_{X_i}}{\alpha_i^2} + 2\frac{\lambda\varphi_i^2\sigma^4_{X_i}}{\alpha_i^3} - 2\chi n\varphi_i^2\alpha_i \qquad (23)$$

to zero leads to $\mu^2 - \mu\alpha_i - \chi n\varphi_i^2\alpha_i^4 = 0$ where $\mu = \sqrt{\lambda}\varphi_i\sigma^2_{X_i}$. The derivative is negative for $\alpha_i = \mu$ and positive for $\alpha_i = 0$. The polynomial being monotonous on the interval $[0;\mu]$, one can conclude that Eqn.(23) has a valid solution on $[0;\mu]$. If the derivative is negative on $\mathcal{D}_2$, the solution adopted is α_i such that $\mu\alpha_i^2 = (\mu - \alpha_i)(\sigma^2_{X_i} + n\alpha_i^2)$. Let $n\alpha_i^2 = \sigma^2_{W_i}$, $n\lambda = \lambda'$ and $n\chi = \chi'$. Let us assume that $\sigma^2_{W_i}$ is very close to $\alpha_i^2(n-1)$. In the Wiener case ($(\gamma_i, \sigma_{\delta_i}) \in \mathcal{D}_3$), the cost function $J_{\chi,i}(\alpha_i)$ expressed in terms of $\sigma^2_{W_i} = n\alpha_i^2$ is given by

$$J_{\chi,i}(\sigma^2_{W_i}) = \left(1 + \lambda'\varphi_i^2\sigma^2_{X_i}\right)\frac{\sigma^2_{W_i}}{\sigma^2_{W_i} + \sigma^2_{X_i}} - \chi'\varphi_i^2\sigma^2_{W_i}. \qquad (24)$$

Setting the derivative of $J_{\chi,i}(\sigma^2_{W_i})$ with respect to $\sigma^2_{W_i}$

$$\frac{\partial J_{\chi,i}}{\partial\sigma^2_{W_i}} = \left(1 + \lambda'\varphi_i^2\sigma^2_{X_i}\right)\frac{\sigma^2_{X_i}}{\left(\sigma^2_{W_i} + \sigma^2_{X_i}\right)^2} - \chi'\varphi_i^2 \qquad (25)$$

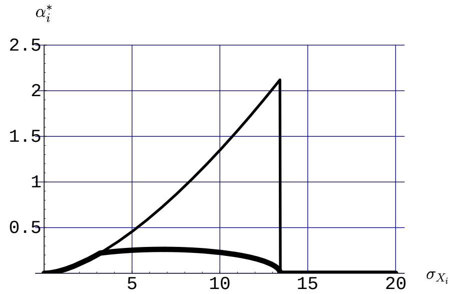

Figure 2: Optimum values of α_i for $\lambda = 0.002$, $\chi = 0.0028$ and $n = 100$ bits.

to zero, given that $\sigma^2_{W_i} = n\alpha_i^2$, leads to

$$\alpha_i^\star = \sqrt{\frac{\sigma_{X_i}\sqrt{1+\lambda'\varphi_i^2\sigma^2_{X_i}} - \sqrt{\chi'}\varphi_i\sigma^2_{X_i}}{\sqrt{\chi'}n\varphi_i}}. \quad (26)$$

This provides a closed-form of the optimum embedding parameter α_i in terms of the host signal power spectrum ($\sigma^2_{X_i}$) and for an SAWGN attack. The Wiener filtering can restore the signal, hence may lead to $D_{xy'} < D_{xy}$. This can be avoided by filtering the watermarked signal (after embedding). The distortion measure is then $D_{xy} = \sum_{i=1}^{m} \varphi_i^2 \frac{\sigma^2_{X_i}\sigma^2_{W_i}}{\sigma^2_{X_i}+\sigma^2_{W_i}}$, where $\sigma^2_{W_i} = n\alpha_i^2$. The resolution of the problem leads to new parameters (see [5] for details): $\alpha_i^\star \simeq \sqrt{\lambda}\varphi_i\sigma^2_{X_i}$. Fig. 2 illustrates the variations of the parameter α_i in terms of $\sigma^2_{X_i}$ for both approaches i.e., without (bold curve) and with a Wiener post-filtering (light curve) of the watermarked signal (with $\varphi_i = (1+\sigma_{X_i})^{-1/2}$). Unlike [1], it can be observed that for high values of $\sigma^2_{X_i}$, no watermark can be robustly embedded on the corresponding sites.

5 RESULTS

The approach has been tested on images against techniques using $\alpha_i = constant$, and $\alpha_i = c|x_i|$ [6], considering embedding in the wavelet transform domain. Fig. 3 depicts the respective E_b/N_0 performances in terms of the attack distortion. A message of 156 bits is embedded (i.e. $n = 156$) in the 512×512 gray scale *Lena* image (i.e. $m = 262\ 144$). The Lagragian multipliers λ and χ are set so that $D_{xy} = D_{xy}^{\max}$ and $D_{xy'} = D_{xy'}^{\max}$. The embedding parameters have been tuned in order to get the same perceptual distortion $D_{xy}/m = 1$ (with $\varphi_i = (1+\sigma_{X_i})^{-1/2}$) with the different techniques. The watermarked image has been attacked with a lossy compression JPEG, from 95% to 5% quality. The tests, using the Stirmark benchmark have shown that the technique is robust to all the non-geometric attacks.

6 CONCLUSION

This paper provides an information-theoretic analysis of information hiding in non i.i.d signals with perceptual distortion metrics. Note that previous work, when considering perceptual watermaking was often led by intuition. Here we have derived closed-form expressions of the different extraction and embedding parameters, revealing an efficient and practical information hiding system.

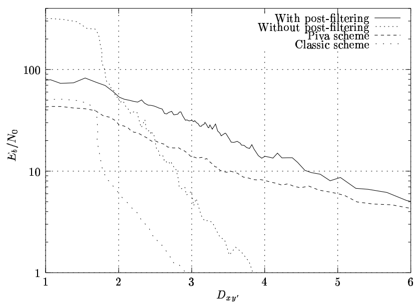

Figure 3: Performances of the proposed scheme in presence of a compression attack JPEG.

References

[1] I. J. Cox, J. Kilian, T. Leightom, and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Proc.*, 6(12):1673–1687, Dec. 1997.

[2] J. J. Eggers, R. Bäuml, and B. Girod. Digital watermarking facing attacks by amplitude scaling and additive white noise. In *4th Int. ITG Conf. on Source and Channel Coding*, Jan. 2002.

[3] P. Moulin and A. Ivanovic. The watermark selection game. In *Proc. Conf. on Info. Sciences and Systems*, Mar. 2001.

[4] P. Moulin and J. A. O'Sullivan. Information-theoretic analysis of watermarking. In *Proc. Int. Conf. on Acoustic, Speech and Signal Processing.*, Istanbul, Turkey, Jun. 2000.

[5] S. Pateux, G. Le Guelvouit, and C. Guillemot. Information-theoretic analysis of WSS watermarking of non i.i.d. Gaussian signals. *submitted to IEEE Trans. Signal Proc.*, Dec. 2001.

[6] A. Piva, M. Barni, F. Bartolini, and V. Cappellini. Threshold selection for correlation-based watermark detection. In *Proc. COST 254 Workshop on Intelligent Communications*, pages 66–72, L'Aquila, Italy, Jun. 1998.

[7] C. I. Podilchuk and W. Zeng. Image-adaptive watermarking using visual models. *IEEE Journal on Special Areas in Communications*, 16(4):525–539, May 1998.

[8] S. Servetto, C. I. Podilchuk, and K. Ramchandran. Capacity issues in digital image watermarking. In *Proc. Int. Conf. on Image Processing*, volume 1, pages 445–449, Chicago, IL, Oct. 1998.

[9] J. K. Su, J. J. Eggers, and B. Girod. Analysis of digital watermarks subjected to optimum linear filtering and additive noise. *IEEE Trans. Signal Proc.: Special Issue on Information Theoretic Issues in Digital Watermarking*, 81(6), Jun. 2001.

[10] J. K. Su and B. Girod. Power-spectrum condition for energy-efficient watermarking. *submitted to IEEE Trans. Multimedia*, Jul. 1999.