MULTI-BIT INFORMED EMBEDDING WATERMARKING WITH CONSTANT ROBUSTNESS

Joceli Mayer and José Carlos M. Bermudez

LPDS: Digital Signal Processing Research Laboratory
Department of Electrical Engineering - Federal University of Santa Catarina - UFSC - Brazil
E-mail: {mayer,bermudez}@eel.ufsc.br

ABSTRACT

This paper proposes an informed spread spectrum watermarking technique for the embedding of multi-bits into images using blind detection. The new technique exploits the information available at the embedder to eliminate all the interferences from the host, patterns and perceptual masking. A statistical analysis leads to the minimum embedding strength required by each pattern to achieve a specified bit error probability for a given additive noise distortion. As a result, each message bit will present the same degree of robustness. Experimental results illustrate the performance achieved for a set of typical valumetric attacks.

1. INTRODUCTION

Recent research on watermarking has stressed the importance of exploiting the available information at the encoder during the watermark embedding [1, 2, 3]. Informed embedding systems are designed to embed watermark patterns constrained by robustness and fidelity specifications while considering the sources of interference on the detection [3]. Informed coding systems based on the dirty paper concept [4] are designed to produce a watermark represented by a codeword which depends on the host signal [5]. Recently, [1] proposed an informed watermarking system that exploits both informed embedding and informed coding paradigms. The resulting system is able to provide a very high payload with perceptual quality tuned by Watson's metric. Moreover, their results clearly indicate that the informed embedding scheme is the main responsible for the achieved performance. Reference [1] discusses the difficulties in achieving an optimal embedding algorithm using both paradigms. They propose a suboptimal iterative embedding algorithm, combined with a message coding based on a trellis code.

In this paper, we propose an informed spread spectrum watermarking approach that provides a non-iterative embedding considering additive noise attack. Analysis results lead to the value of the minimum watermark energy required to achieve a specified BER (Bit Error Rate) while compensating for the interferences from the channel noise, the host signal, the watermark patterns and the perceptual shaping mask. Currently, we only exploit informed embedding due to the difficulties of achieving an optimal solution including some informed coding approach. However, as discussed in [5], it is possible to extend the embedder by including a dirty paper code. According to [5], which extended the embedders provided in [3], the embedder needs to be modified to include a preliminary step which selects the best among the watermark patterns representing the same message. In [1] the informed coding and the informed embedding are complementary approaches designed separately.

Some basic definitions are presented in the Section 2. Section 3.1 presents our multi-bit embedding solution. Section 3.2 determines the required watermark energy to achieve a given specified BER. Section 3.3 discusses the transparency provided by the technique. Section 4 provides discussions, numerical and visual results to illustrate the robustness and transparency performance achieved for a set of typical valumetric attacks.

This work was supported by CNPq (Brazilian National Council for R&D) Grants Nos. 552164/01-1, 550658/02-5, 308095/2003-0, 472762/2003-6.

2. DEFINITIONS

Consider a message encoded by a sequence of N bits, $\hat{B} = \{\hat{b_1}, \hat{b_2}, \ldots, \hat{b_N}\}$, $\hat{b_i} \in \{0, 1\}$. We map it into an antipodal sequence B where $b_i = 2 \cdot \hat{b_i} - 1$, resulting in $b_i \in \{-1, 1\}$. Consider a set P of N patterns to be used for spread spectrum watermarking of the host image $\hat{C_0}$, $P = \{\hat{P_1}, \hat{P_2}, \ldots, \hat{P_N}\}$, $\hat{P_i} = \{p_{i1}, p_{i2}, \ldots, p_{iM}\}$. Each pattern $\hat{P_i}$ is a sequence of length M. The host image $\hat{C_0} = \bar{C_0} + C_0$, where $\bar{C_0}$ is the image average, is also organized as a sequence of length M.

The sequence B is spread into a watermark sequence W with dimension M:

$$W = \sum_{j=1}^{N} b_j \cdot \hat{P_j} \tag{1}$$

In the traditional spread spectrum watermarking, the watermark is added to the host image $\hat{C_O}$, yielding $C_W = \hat{C_O} + \alpha W$, where α is a gain factor and C_W is the watermarked image, also known as the stegoimage. Watermark detection can be implemented using correlation. Assuming no transmission errors or distortions in the channel path, a decision variable d_i is computed by evaluating the zero-lag spatial cross-covariance function:

$$d_i = \left\langle \hat{P_i}, C_W \right\rangle = \left\langle P_i + \bar{P_i}, C_W \right\rangle \tag{2}$$

where $\hat{P_i}$ has two terms, a zero average pattern P_i and the average $\bar{P_i}$. The average $\bar{S}$ of a sequence $\hat{S}$ with elements s_k, $k = 1, \ldots, M$ is computed as $\bar{S} = \frac{1}{M}\sum_{k=1}^{M} s_k$. The zero-lag cross-correlation of two sequences S and R with elements s_k and r_k, respectively, $k = 1, \ldots, M$, is given by:

$$\langle S, R \rangle = \frac{1}{M}\sum_{k=1}^{M} s_k r_k \tag{3}$$

Disregarding the occurrence of false positives [6], the bit $\hat{b}_i$ is detected as zero if $d_i < 0$ and as one otherwise.

3. WATERMARK EMBEDDING

3.1. Efficient Embedding

The traditional spread spectrum watermarking approach adds a scaled watermark W to the host signal, $C_W = \hat{C_O} + \alpha W$ where W is given by (1). This approach is inefficient because it is limited to use a single factor to adjust the energy of all patterns. Given a fixed gain factor α designed to minimize some cost function, many patterns $\hat{P}_i$ can be introduced with more energy than the minimum necessary to satisfy the robustness or fidelity constraints. Moreover, the designed patterns must incorporate the properties necessary to mitigate the interferences caused by the host image, by the cross correlation among sequences and by the perceptual shaping mask. Watermarking systems lacking these properties will provide sub-optimal embedding, resulting in losses in capacity, transparency and robustness. An analysis of these properties and alternative pattern generating methods can be found in [7]. We address these problems by allowing a different gain factor α_j for each pattern [8]. Thus, we use

$$C_W = \hat{C_O} + \sum_{j=1}^{N} \alpha_j b_j \hat{P}_j * X \tag{4}$$

In (4), the operator $*$ means an element by element vector multiplication and X is a perceptual shaping mask. Recall that $\langle \lambda, V \rangle = 0$, for any constant λ whenever V is a zero average vector, and let us assume that $\bar{P}_i = 0$. Considering an additive noise $\hat{\eta} = \eta + \bar{\eta}$ in the transmission channel, the decision variable d_i, relative to bit b_i, is computed at the detector using (2):

$$d_i = \langle P_i, C_O \rangle + \left\langle P_i, \sum_{j=1}^{N} \alpha_j b_j P_j * X \right\rangle + \langle P_i, \eta \rangle$$

$$d_i = R_i^{C_O} + R_i^{\eta} + \left\langle P_i, \sum_{j=1}^{N} \alpha_j b_j P_j * X \right\rangle$$

$$= R_i^{C_O} + R_i^{\eta} + \sum_{j=1}^{N} \alpha_j R_{ij} \tag{5}$$

where $R_i^{C_O}$, R_i^{η} and $R_{ij} = b_j \langle P_i, P_j * X \rangle$ are, respectively, the correlation of P_i with the host image, the correlation of P_i with the noise and the cross correlation between P_i and the pattern P_j multiplied, element by element, by the mask X. For the noiseless case, $R_i^{\eta} = 0$, we can guarantee a specified detection level $d_i = \beta b_i$, for $i = 1, \cdots, N$, by solving (5) for the optimal gain factor vector $\underline{\alpha} = [\alpha_i, \cdots, \alpha_N]^T$:

$$\begin{bmatrix} R_{11} & R_{12} & \cdots & R_{1N} \\ R_{21} & R_{22} & & \vdots \\ \vdots & & \ddots & \\ R_{N1} & \cdots & & R_{NN} \end{bmatrix} \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} \beta \cdot b_1 - R_1^{C_O} \\ \beta \cdot b_2 - R_2^{C_O} \\ \vdots \\ \beta \cdot b_N - R_N^{C_O} \end{bmatrix} \tag{6}$$

This approach simultaneously compensates for the interferences from the host image, patterns and shaping mask. Disregarding false positives, clipping and round-off effects, we would reliably detect all bits choosing any $\beta > 0$ in this case. Notice that, for all pseudo-random generators used in practice, $R_{ij} << R_{ii}$, assuring that the matrix in Eq. (6 has rank N. Considering an additive noise with known power but with unknown correlations R_i^{η}, the parameter β can be determined to compensate for the effect of these correlations, as will be explained in the following.

3.2. Determining β for Additive White Noise Attacks

In the following, we estimate the parameter β to attain a given specified BER by considering interferences R_i^{η} generated by an additive noise. Recall that using $\underline{\alpha}$ obtained from (6) for the noiseless case, $d_i = \beta b_i$. Considering now the additive noise with the same $\underline{\alpha}$, d_i becomes $d_i = \beta b_i + R_i^{\eta}$ from (5). In this case, a detection error occurs whenever: a) $b_i = 1$ and $d_i = \beta + R_i^{\eta} \leq 0$; b) $b_i = -1$ and $d_i = -\beta + R_i^{\eta} \geq 0$. Thus, the resulting error probability Pr_{error_i} for the bit i is given by:

$$Pr_{error_i} = Pr(R_i^{\eta} \geq \beta, b_i = -1) + \\ + Pr(R_i^{\eta} \leq -\beta, b_i = 1) \tag{7}$$

Assuming that the message B is independent of the noise source, results:

$$Pr_{error_i} = Pr(R_i^{\eta} \geq \beta) Pr(b_i = -1) + \\ + Pr(R_i^{\eta} \leq -\beta) Pr(b_i = 1) \tag{8}$$

Since η and P_i are random quantities, R_i^{η} is a random variable. Thus, we must determine the statistics of R_i^{η} to estimate β for a given BER specification. Assuming $\hat{P}_i$ to be zero-mean, $E[R_i^{\eta}] = 0$ where $E[\cdot]$ stands for statistical expectation. To determine the variance of R_i^{η}, we assume that we have binary patterns $p_{ij} \in \{-P_{max}, P_{max}\}$. Also, assuming that η is white noise, $E[\eta_i \eta_j] = 0$ for $i \neq j$. Hence, the variance of R_i^{η} is given by:

$$Var(R_i^{\eta}) = E\left[(R_i^{\eta} - E(R_i^{\eta}))^2\right] = E\left[(R_i^{\eta})^2\right] =$$

$$= E\left[\left(\frac{1}{M}\sum_{k=1}^{M} P_{ik}\eta_k\right)^2\right] = \frac{1}{M^2}\sum_{k=1}^{M} E\left[P_{ik}^2 \eta_k^2\right] =$$

$$= \frac{P_{max}^2}{M^2}\sum_{k=1}^{M} E\left[\eta_k^2\right] = \frac{P_{max}^2}{M}\sigma_{\eta}^2 \tag{9}$$

Eq. (9) provides a relationship between R_i^{η} and η:

$$\sigma_{R_i^{\eta}} = \frac{P_{max}}{\sqrt{M}}\sigma_{\eta} \tag{10}$$

Since $\sigma_{R_i^{\eta}}$ does not depend on the bit value or on the pattern i, $Pr_{error_i} = Pr_{error}$ represents the average bit error probability. Assuming an even probability density function (pdf) for η, $Pr(R_i^{\eta} \geq \beta) = Pr(R_i^{\eta} \leq -\beta)$. Using this property and recalling that $Pr(b_i = 1) + Pr(b_i = -1) = 1$, from (8):

$$Pr_{error} = Pr(R_i^{\eta} \geq \beta) \tag{11}$$

The Chebyshev's inequality [9], guarantees that, for any $k > 0$:

$$Pr\left(|R_i^{\eta}| \geq k\sigma_{R_i^{\eta}}\right) \leq \frac{1}{k^2} \tag{12}$$

Thus, from (11) and (12) the Pr_{error} for $\beta = k\sigma_{R_i^{\eta}}$ is bounded by $\frac{1}{2k^2}$ since $Pr(|x| \geq A) = 2Pr(x \geq A)$ for any x with even pdf. Notice that R_i^η is computed as a weighted sum of independent, identically distributed (iid) disturbances η_k with even pdf, with $p_{ij} \in \{-P_{max}, P_{max}\}$. Therefore, according to the Central Limit Theorem [10], the distribution of R_i^η tends to a Gaussian for large M and we are able to find a tighter bound from (8):

$$Pr_{error} = Pr(b_i = 1)\int_{-\infty}^{-\beta} G_{R_i^\eta}(x)dx +$$

$$+Pr(b_i = -1)\int_{\beta}^{\infty} G_{R_i^\eta}(x)dx = \int_{\beta}^{\infty} G_{R_i^\eta}(x)dx \qquad (13)$$

where $G_{R_i^\eta}(x)$ is $N(0, \sigma^2_{R_i^\eta})$. Hence, given a desired BER we can determine β using a normalized table of the Gaussian integral or using some numerical procedure. For example, given an acceptable average bit error probability $Pr_{error} = 1 - 0.9987 = 0.0013 = 0.13\%$, by looking at a Gaussian table we find that $\beta = 3\sigma_{R_i^\eta} = 3\frac{P_{max}}{\sqrt{M}}\sigma_\eta$. For most applications, it is not difficult to estimate the standard deviation of the noise. Given a specified BER and an estimate of the channel noise variance, we determine β to compensate for the noise correlation, as explained above, and then compute the gain factor vector $\underline{\alpha}$ using (6).

3.3. Transparency

In the absence of noise, (6) provides a transparent embedding by choosing β as close as possible to zero. In practice, however, the parameter β cannot be too close to zero because of the round-off and clipping effects. Under noisy conditions, transparency will be limited by the noise variance. The proposed approach compensates for the projections of R_i^{Co} and R_{ij} onto the direction of the vector P_i weighted by the perceptual shaping mask X. In both the noiseless and noisy cases, the proposed embedding approach provides the required embedding energy for the sequences given a specified BER and noise variance. Perceptual transparency is considerably improved by using a proper shaping mask X. Notice that the mask interferences are also compensated by our approach.

4. EXPERIMENTS

Many watermarking applications require multi-bit message lengths of at least 70 bits. In this experiment we embed a 70-bit message in the spatial domain of the Lena image using a wavelet-based shaping mask X. Considering that the Human Visual System is less sensitive to the active regions in an image, the perceptual shaping mask was designed to embed more watermark energy into the regions presenting edges and textures. Other masks can be used, such as those based on the Watson metric [1]. Fig. 1(a) shows the watermarked image using $\beta = 0.5$ and Fig. 1(b) shows (after scaling for visibility) the distortion introduced by the watermark.

Fig. 2 shows the 70-bit binary message, the values of R_i^{Co} and R_{ij} for each bit b_i, the computed values of α_i and the correlation results d_i. Notice that, for the noiseless case ($R_i^\eta = 0$), we achieve optimal embedding, where for all bits, $d_i \simeq \beta b_i$. Notice that all bits have the same robustness. The very small deviations observed for d_i around the ideal value, βb_i, occur due to round-off and clipping effects. For this noiseless case, we only need to set β to a small value around 0.05 to achieve zero bit error and a stegoimage with PSNR of 47 dB.

We evaluate the method's robustness for valumetric distortion sources, by choosing AWGN (additive White Gaussian Noise) with $\sigma_\eta = 85$, histogram equalization, high-pass linear filtering and lossy compression using JPEG-DCT with quality factor of 50. Fig. 3 shows the distorted watermarked images and Fig. 4 shows the interference of R_i^n on the decision variable d_i for $\beta = 0.5$. For this particular experiment, all bits were detected perfectly ($BER = 0$). The resulting stegoimage has PSNR $= 33.7$ dB.

		Specified BER_1 0.0013			Specified BER_2 0.1587
σ_η	β	BER	σ_η	β	BER
21	0.125	0.00128	64	0.125	0.1577
43	0.25	0.00114	128	0.25	0.1538
85	0.5	0.00171	256	0.5	0.1663
170	1	0.00114	512	1	0.1587
256	1.5	0.00128	768	1.5	0.1630

Table 1. Monte Carlo Simulation for AWGN Attacks.

Table 1 shows a Monte Carlo simulation with 100 runs each using messages of 70 bits, considering AWGN and the same perceptual mask. In this experiment we specified two bit error probabilities: $BER_1 = 0.13\% \Rightarrow \beta = 3\sigma_{R_i^\eta} = 3\frac{P_{max}}{\sqrt{M}}\sigma_\eta$ and $BER_2 = 15.87\% \Rightarrow \beta = \sigma_{R_i^\eta} = \frac{P_{max}}{\sqrt{M}}\sigma_\eta$ for various noise variances with $P_{max} = 1$ and $M = 512 \times 512$. The experimental bit error rates (BER) achieved agree very well with the specified BER_1 and BER_2.

Using the same shaping mask, we evaluated the robustness for high payload by embedding messages of 200, 300 and 400 bits in the above image. We achieved PSNR $= 29.59$, 28 and 27.0 dB, respectively, with very high perceptual quality due to the shaping mask chosen. The resulting experimental bit error rates are very close to the specified $BER = 0.13\%$ for the 100 simulations using $\beta = 0.25$ and considering an AWGN attack with $\sigma_\eta = 43$.

5. CONCLUSIONS

We presented a novel approach for informed multibit embedding watermarking. We determine the exact energy required by each pseudo random sequence to achieve a specified BER considering interferences from sequences, host, noise and shaping mask. As a result, the technique provides a constant robustness for all bits. Results illustrated the robustness to some valumetric distortion sources such as AWGN, histogram equalization, high-pass linear filtering and lossy compression using JPEG-DCT. Monte Carlo simulations illustrated the accuracy of the analysis used to determine β according to the channel noise variance. Examples illustrated the robustness and transparency for high payload embedding.

6. REFERENCES

[1] Matt L. Miller, Gwenaël J. Doërr, Ingemar J. Cox, "Applying informed coding and embedding to design a robust high-capacity watermark," *IEEE Transactions on Image Processing*, vol. 6, no. 13, pp. 792–807, June 2004.

[2] M. Barni, N. Memon, T. Kalker, P. Moulin, I.J. Cox, M.L. Miller, J.J. Eggers, F. Bartolini, F. Pérez-González, "Signal processing forum: What is the future for watermarking ?

(a) (b)

Fig. 1. (a) C_W with $\beta = 0.5$ and (b) Difference $10 \cdot (C_W - C_O)$.

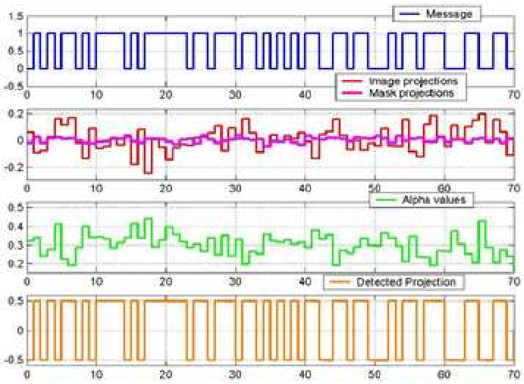

Fig. 2. Noiseless case. Message, host and mask projections, α_i and d_i values for $\beta = 0.5$ with the same robustness for each bit.

(part 2)," *IEEE Signal Processing Magazine*, vol. 20, no. 6, pp. 53–57, November 2003.

[3] I. J. Cox, M. L. Miller, A. L. Mckellips, "Informed embedding: Exploiting image and detector information during watermark insertion," *in IEEE International Conference on Image Processing*, vol. 3, pp. 1–4, 2000.

[4] Max Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 439–441, 1983.

[5] Matt L. Miller, "Watermarking with dirty-paper codes," in *IEEE Int. Conf. Image Processing*, Thessaloniki, Greece, vol. 2, pp. 538–541.

[6] I. J. Cox, M. L. Miller, J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann, 2002.

[7] J. Mayer, A. V. Silverio, J. C. M. Bermudez, "On the design of pattern sequences for spread spectrum image watermarking," *Int. Telecommunications Symposium (ITS2002)*, 2002.

[8] Joceli Mayer, Rafael Araujo da Silva, "Efficient informed embedding of multi-bit watermark," in *IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP*, 2004, vol. 1, pp. 389–392.

[9] D.G. Manolakis, V.K. Ingle, S.M. Kogon, *Statistical and Adaptive Signal Processing*, McGraw-Hill, 2000.

[10] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, Inc., 1991.

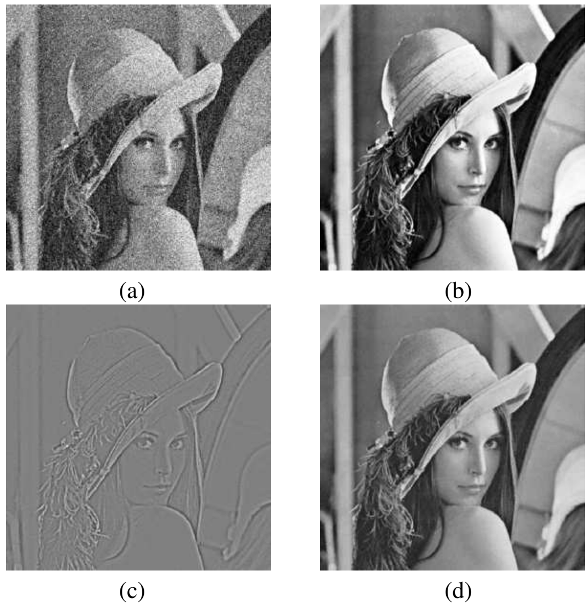

Fig. 3. Attacked watermarked images: (a) AWGN; (b) Histogram Equalization; (c) High-pass filtering; (d) JPEG lossy compression.

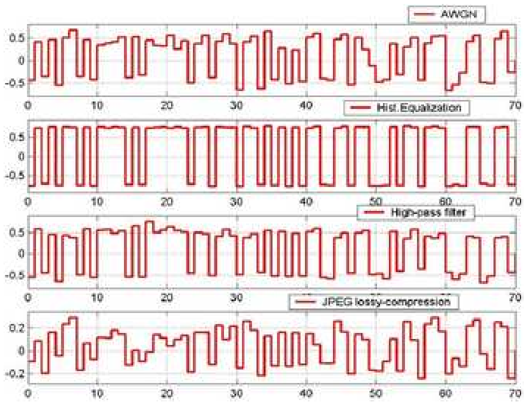

Fig. 4. Effects of the valumetric attacks on the correlation d_i.