OPTIMUM WATERMARK DETECTION AND EMBEDDING IN DIGITAL IMAGES

Josep Vidal, Elisa Sayrol

Dept. Teoría de la Señal y Comunicaciones. Universidad Politécnica de Cataluña.
Campus Nord, Módulo D5, c/ Jordi Girona 1-3. 08034 Barcelona SPAIN
Email: {pepe,elisa}@gps.tsc.upc.es

Abstract - One of the problems arising from the use of digital media is the ease of identical copies of digital images or audio files, allowing manipulation and unauthorized use. Copyright is an effective tool for preserving intellectual property of those documents but authors and publishers need effective techniques that prevent from copyright modification, due to the straightforward access to multimedia applications and the wider use of digital publications through the www. These techniques are generally called watermarking and allow the introduction of side information (i.e. author identification, copyrights, dates, etc.) [2], [3], [6].

This work will concentrate on the problem of watermarking of still images using the luminance component, through the use of spread spectrum techniques, both in space (Direct Sequence Spread Spectrum or DSSS) and frequency (Frequency Hopping or FH), following the guidelines of [1]. The system described below is able to embed watermarks and recover them with zero probability of error. The problem is faced from a statistical detection point of view through the analysis of the density function of the image to be marked. A Cauchy model is found to be very accurate and some tests are performed in order to assess improved detection quality. The resulting system turns out to be easy to encrypt and very robust to filtering and JPEG compression.

1. DIGITAL WATERMARKS

It is interesting to attack the problem by considering the watermark as a signal to be buried in noise, that is the image. The signal design may be obtained as a compromise between the following factors:

a) The watermark has to be difficult to detect by a non-authorized user, therefore some kind of encryption has to be done, if possible both in space and frequency. Spread spectrum techniques in space (DSSS) and in frequency (FH) adapt specifically to the requirement.

a) Visual quality of the marked image should be indistinguishable from the original. The contribution in [1] is a pioneering work on the use of psycovisual criteria in the watermark embedding process, by modeling the behavior of human visual system with Gabor filters [4]. The well known masking effect is used there: Any watermark whose bandwidth is less than or equal to the Gabor filter bandwidth will be invisible provided that its energy be lower than the image energy in that band. With this regard, the instantaneous Gabor filter output is used to modulate the amplitude of the watermark.

b) The amount of information this signal can convey: large amounts might increase the signal bandwidth beyond the Gabor filters bandwidth which implies visual noticing of the watermark.

c) The probability of error in the detection of each symbol constituting the watermark should be as low as possible, implying high power for the mark and, at the same time, noticeable effect on the marked image. DSSS techniques again allow the use of low power signals while maintaining probability of error in reasonable levels.

d) The watermark should be robust enough to low-pass filtering, compression, or any other not noticeable modification of the image. In particular the central frequency of the watermark should be placed at frequencies that are generally preserved by a low compression JPEG procedure.

Having those conditions in mind, the watermark to be included in the image consists in a series of K=31 orthogonal symbols being each of them a pseudorandom minimum length sequence (MLS). Each chip in the MLS is sized to a block of 8x32 pixels in order to accommodate to the Gabor filter bandwidth [1] (see figure 1.1).

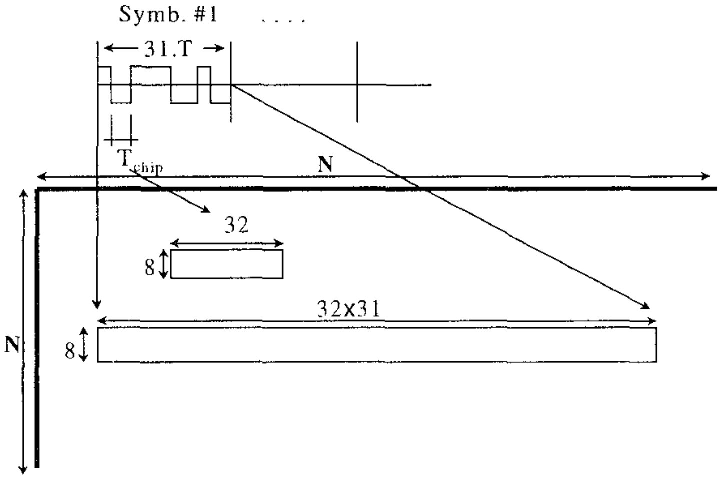

Figure 1.1. Watermark structure and embedding

Each series of symbols is modulating in amplitude a bidimensional carrier whose frequencies are randomly chosen. The set of available frequencies has to be such that the carriers are orthogonal in the integration interval of size 8x992 pixels. Horizontal normalized frequencies of values $k_x/992$ (k_x=0,1,...,991) fit the requirements. The value of k_x cannot be too low to give noticeable results nor too high to be eliminated in a JPEG compression. In practice, the values chosen are [1] in the interval 0,1 y 0,2 in which we can accommodate around 100 different frequencies. In the vertical sense the value for k_y is not chosen at random and it is fixed to 1/8.

2. OPTIMUM DETECTION

It is required that the authorized user be able to recover with low probability of error the watermark. Good detection schemes allow the watermark embedding with low power and hence, low visual impact. Before deriving the detector, let us formulate a model for the watermark: if we do represent each block of the marked image in vector notation, as $\mathbf{r} = \mathbf{y} + A\mathbf{s}_i$ with $\mathbf{s}_i = \mathbf{f} \otimes \mathbf{a}_i$, where $A\mathbf{f}$ stands for the amplitude which modifies the marking symbol $\mathbf{a}_i$ following the output of the Gabor perceptual filter, and the symbol $\otimes$ represents a term-by-term product between two vectors.

2.1. Optimum linear detector

The optimum detector has to take into account the density function of the noise, that is, the image $\mathbf{y}$. The conventional and computationally simple approach is to consider the noise to be Gaussian and stationary. In this case, the log-likelihood function of $\mathbf{r}$ is given by:

$$\begin{aligned} \Lambda_i &= (\mathbf{r} - A\mathbf{s_i} - m\mathbf{1})^T \mathbf{C}^{-1} (\mathbf{r} - A\mathbf{s_i} - m\mathbf{1}) = (\mathbf{r} - \mathbf{H_i}\theta)^T \mathbf{C}^{-1} (\mathbf{r} - \mathbf{H_i}\theta) \\ \mathbf{H_i} &= [\mathbf{s_i} \quad \mathbf{1}] \qquad \theta^T = [A \quad m] \end{aligned} \tag{2.1}$$

that has to be minimized over i, m and A. It is easy to show that this is completely equivalent to maximize the decision function over i:

$$\Psi_i = \mathbf{r}^T \mathbf{C}^{-1} \mathbf{H}_i \hat{\theta}_i = \mathbf{r}^T \mathbf{C}^{-1} \mathbf{H}_i \left(\mathbf{H}_i^T \mathbf{C}^{-1} \mathbf{H}_i \right)^{-1} \mathbf{H}_i^T \mathbf{C}^{-1} \mathbf{r} \tag{2.2}$$

The computation of (2.2) does not present problems if, as usual, a first-order Markov model is assumed for the image. In this case the inverse of **C** has a closed form and is sparse [5]. Moreover, the correlation coefficient can be chosen to be 1, yielding very low complexity matrix-vector products even for such large size of vector **y**.

However, it is more convenient from implement (2.2) using a previous whitening filter (instead of using C-1) for r and the symbols to be used in the maximization si. A conventional FIR 3x3 filter B[.] for prediction error generation may be chosen:

0	-0,25	0
-0.25	1	-0,25
0	-0,25	0

which plays the role of $\mathbf{C}^{-1/2}$. In this way the decision function is simplified to:

$$\Psi_i = \frac{\left|\mathbf{r}_b^T \mathbf{s}_{b,i}\right|^2}{\mathbf{s}_{b,i}^T \mathbf{s}_{b,i}} \qquad \mathbf{r}_b = B[\mathbf{r}] \qquad \mathbf{s}_{b,i} = B[\mathbf{s}_i] \tag{2.3}$$

Since the power of the whitened symbols is the same, the metrics is reduced to the numerator of (2.3). This scheme appears in figure 2.1.

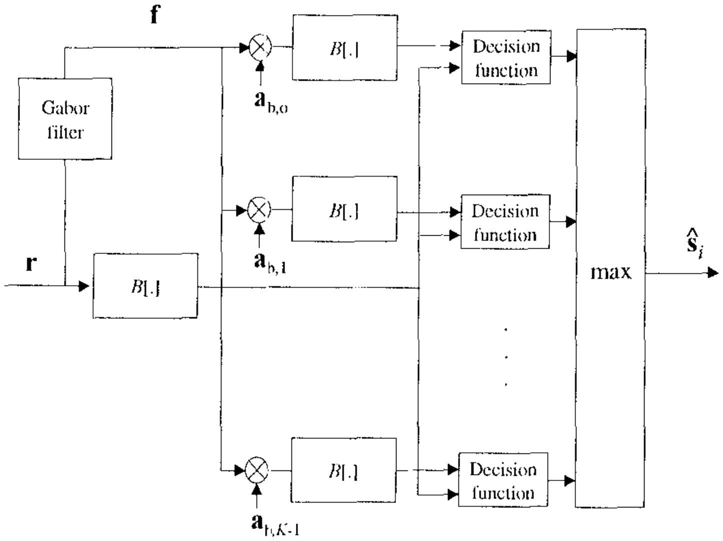

Figure 2.1. Detection of watermarks built using *K*-ary signaling.

2.2. Cauchy detector

Although a Gaussian model yields to reasonable solutions, the distribution of the whitened image tends to exhibit a slower decay in the tails of the distribution. We can model this behavior with alpha-stable distributions [7], which concentrate around the mean but are also characterized by heavier tails. These distributions include the Gaussian, as a limiting case. A simple way to describe a symmetric alpha-stable (SαS) probability density function is from the Inverse Fourier Transform of its characteristic function:

$$f_\alpha(\gamma,\delta,x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \exp\left(j\alpha\omega - \gamma|\omega|^\alpha\right)\exp(-j\omega x)d\omega \tag{2.4}$$

which is itself characterized by three parameters. The characteristic component, α ($0 < \alpha \leq 2$), accounts for the heaviness of the tails. A small value of α indicates severe presence of outliers whereas α close to 2 indicates a nearly normal behavior. The location parameter, δ (taking values $-\infty<\delta<\infty$) is the point of symmetry of the SαS pdf. Finally the dispersion parameter γ ($\gamma>0$), describes the spread of the values around its median. It is similar to the

variance of a Gaussian pdf. Although there is no closed-form expression for (2.4), except for some particular distributions, it can be expanded into convergent series [7].
Several images have been tested observing that alpha-stable distributions are able to characterize the distribution of the whitened images. As an example, in figure 2.2 we represent the histogram of a whitened image. The pdf of the Gaussian distribution is also shown as well as the pdf of the Cauchy distribution (α=1). The dispersion parameter has been estimated using the methods described in [8]. We can observe that the Cauchy distribution is a better model than the Gaussian distribution. In general, the characteristic component can be estimated to obtain more accurate models of the distribution.

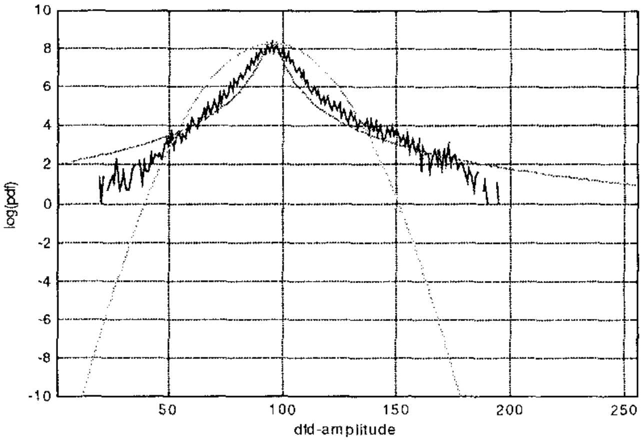

Figure 2.2. Histogram of a whitened image and fitting of a Gaussian and Cauchy pdf

An optimum receiver can be derived in the maximum likelihood sense to decide which symbol is present in a region of the marked image. In particular, considering that the whitened data follows a Cauchy distribution the decision function becomes:

$$\underset{s_i}{max} \sum_{k=1}^{N} \log\left[\frac{\gamma}{\gamma^2 + \left(r_b(k) - s_{b,i}(k)\right)^2}\right] \qquad (2.5)$$

As it is shown in [9] this decision function is robust even for distributions where α is different form 1 and lies in a broad range between 0.5 and 2. Note that the final detection scheme in figure 2.1 also holds.

2.3. Probability of error: simulations

In order to compare the performance of the different detectors, the error rate has been computed by marking several images with a set of characters. Tables 1 and 2 show the rate between misreceived characters and total number of detections. The Cauchy detector gives the best results compared to the optimum linear detector and the correlator used in [1] which is the linear detector without whitening. The global amplitude A that affects the whole watermark has been lowered from value 1.0 to 0.6. As in [1] a correcting factor lowers the amplitude of the mark on sharp edges. Figure 2.3 shows an original image, its marked version and the watermark image. The original image and the marked image are visually equivalent.

	A=1.0	A=0.8	A=0.6
Correlator	12/248	51/248	97/248
Opt. Linear	0/248	6/248	39/248
Cauchy	0/248	0/248	2/248

Table 1: Error rate for Lena

	Lena	Pepper	Camman
Correlator	51/248	41/248	75/248
Opt. Linear	6/248	3/248	15/248
Cauchy	0/248	0/248	0/248

Table 2: Error rate for A=0.8

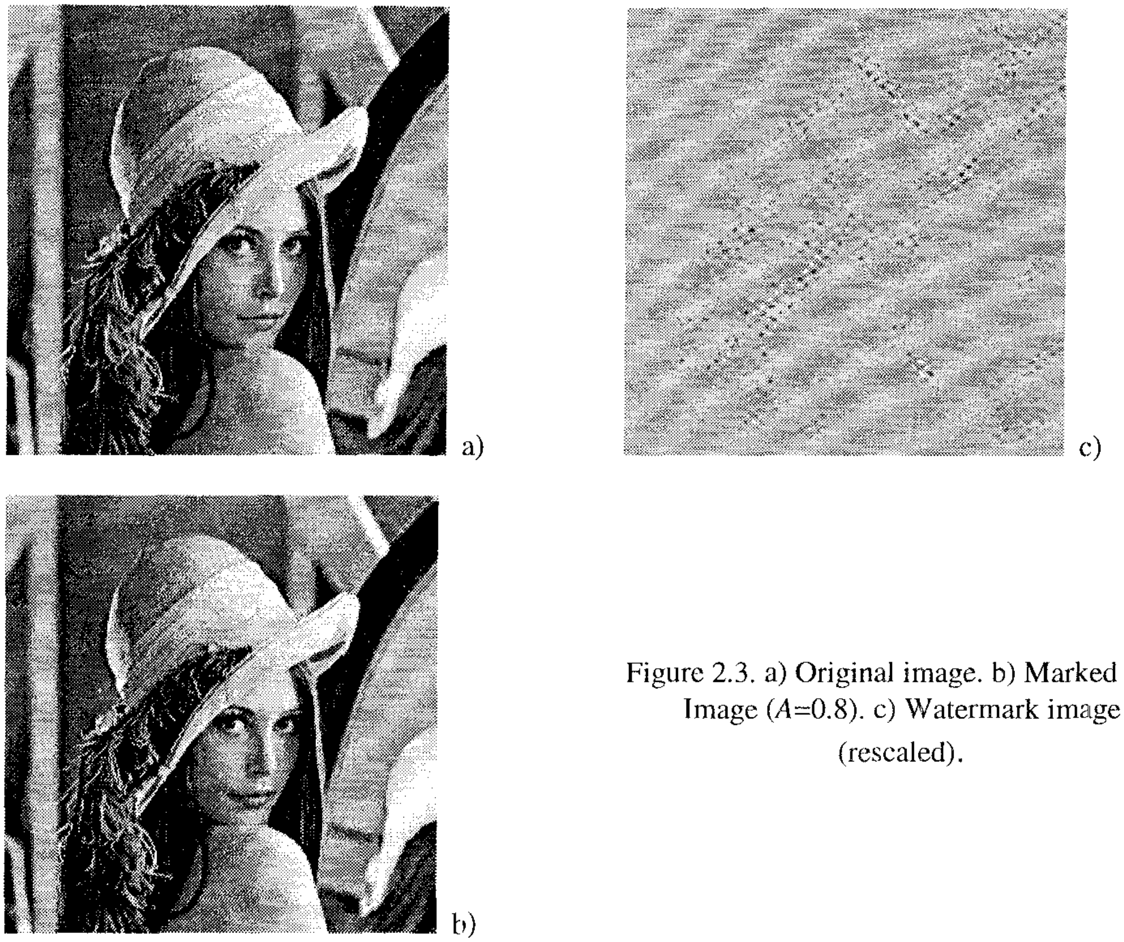

Figure 2.3. a) Original image. b) Marked Image (A=0.8). c) Watermark image (rescaled).

3. WATERMARK EMBEDDING

The amplitude modulation of the symbols which constitute the watermark using the Gabor filter output **f** contributes to increase the correlation among the symbols but it is an unavoidable step if one wants unnoticeable visual impact. However, the probability of error can be reduced to zero if we consider the very nature of the problem, which is in fact different from the problem found in detection for digital communications. The watermark embedding scheme knows exactly which is the noise pattern that the detector will face, that is, the original image. Henceforth it can act in the following two ways.

3.1. Correlation increase in detection

Assume we are using the linear detector. The metrics given in (2.3) takes into account the correlation between the whitened image and the whitened symbols:

$$\Psi_i = \left|\mathbf{r}_b^T \mathbf{s}_{b,i}\right|^2 = \left|B[\mathbf{y}]^T \mathbf{s}_{b,i} + A\mathbf{s}_{b,i}^T \mathbf{s}_{b,i}\right|^2 \qquad (3.1)$$

If the first term in the r.h.s. of (3.1) is negative, it will decrease the value of the metric for the right symbol, thus impairing the detection process. Since this term can be computed at the time of marking, it can be used to change the sign of the mark $\mathbf{s}_{b,i}$ thus increasing the value of the metric [1]. The watermark generation and embedding scheme for the linear receiver is very similar to the one found in [1], and it is plotted in figure 3.1.

3.2. Gain adjustment for zero probability of error

Since the marking scheme knows the original image, it is able to determine exactly which symbol among the K possible will produce the error. In consequence it is able to increase the power of the mark to be embedded accordingly in such a way that no error occurs in detection. The importance of the optimum Cauchy detector resides in the fact that, since it lower drastically the probability of error, the increase in the power of the mark happens very seldom and, when it does, the increase in the watermark power is moderate.

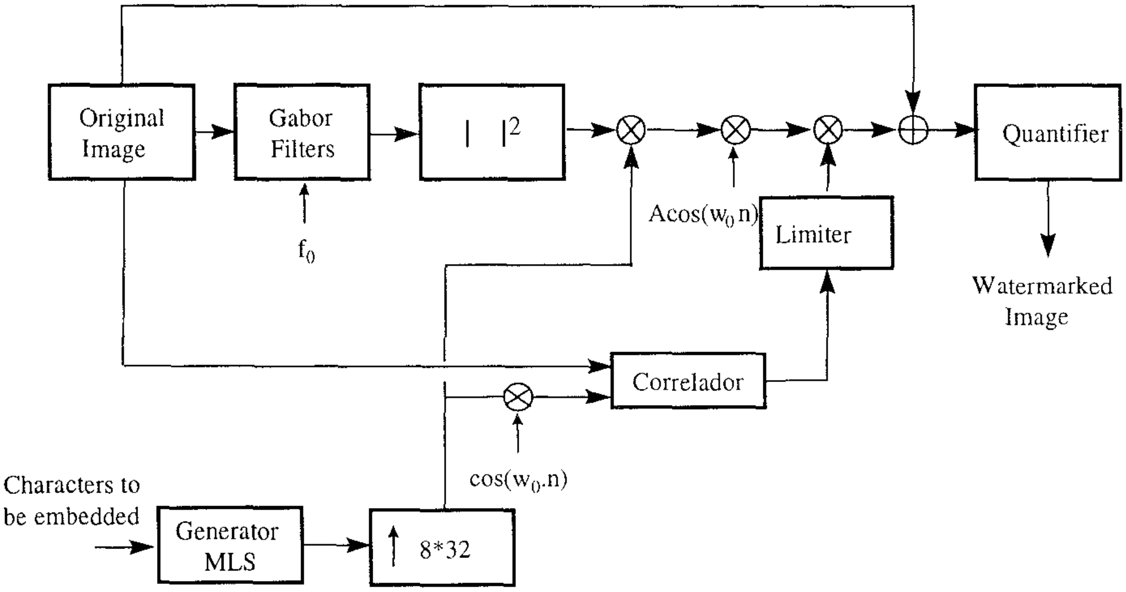

Figure 3.1. Watermark generation scheme.

4. CONCLUSIONS

A watermark system for still images that relies on optimum detectors has been proposed. The scheme is general enough to be applied, with minor modifications, to digital watermarking of audio or speech signals. The system allows zero probability of error in detection. A comparison between the original and the watermarked image shows imperceptible differences by the human eye. Moreover, we can encrypt easily the watermark thanks to the large number of degrees of freedom to include randomness: in pseudorandom DSSS sequences, in frequency if we do use FH, and by randomizing the initial phase of each symbol embedded. The problem, far from being solved, needs further study to assess robustness in conditions of image cropping.

References

[1] J.F. Delaigle, et al., “Watermarking algorithm based on a human visual model”, *Signal Processing*, Vol. 66, No. 3, pp. 319-336, May 1998.

[2] Jian Zhao.Look, “It’s Not There”, *Byte,* January 1997.

[3] A. H. Tewfik, M. Swanson, “Data Hiding for Multimedia Personalization, Interaction, and Protection” *IEEE Signal Processing Mag.*, July 1997.

[4] Stephane Mallat “Multifrequency Channel Decompositions of Images and Wavelet Models”, *IEEE Trans. on ASSP*. Vol 37.no 12, pag 2091-2094, Dic. 1989

[5] Kay, *Modern Spectral Analysis*, Prentice-Hall.

[6] S. Burgett, el al., “Copyright Labeling of Digitized Image Data”, *IEEE Comm. Magazine,* March 1998.

[7] M. Shao and C. L. Nikias, ”Signal Processing with fractional Lower Order Moments: Stable Processes and their Applications”, *Proc. of IEEE,* V-81, No. 7, July 1993.

[8] G. A. Tsihrintzis and C. L. Nikias, “Fast Estimation of the Parameters of Alpha-Stable Impulsive Interference”, *IEEE Trans. on Signal Processing,* V-44, No. 6 June 1996.

[9] G. A. Tsihrintzis and C. L. Nikias, “Performance of Optimum and Suboptimum Receivers in the Presence of Impulsive Noise Modeled as an Alpha-Stable Process”, *IEEE Trans. on Comm.,* V-43, No. 2/3/4, February 1995.