DATA HIDDING IN COLOR IMAGES USING PERCEPTUAL MODELS[1]

Josep Vidal, Elisa Sayrol, Maribel Madueño

Dept. Teoría de la Señal y Comunicaciones, Universitat Politècnica de Catalunya
Campus Nord, Módulo D5, c/ Jordi Girona 1-3
08034 Barcelona, SPAIN
Email: {elisa,pepe}@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.). This work concentrates on the problem embedding and optimum blind detection of data in color images through the use of spread spectrum techniques, both in space (Direct Sequence Spread Spectrum or DSSS) and frequency (Frequency Hopping). It is applied to RGB and opponent color component representations. Perceptive information is considered in both color systems. Some tests are performed in order to ensure imperceptibility and to assess detection quality of the optimum color detectors.

Keywords: watermarking, CIE-lab models, direct sequence spread spectrum.

1. INTRODUCTION

The watermark system described in [2] was successfully applied to gray scale images [1] and could be easily extended to color images by embedding the watermark in the luminance component or in each of the three components. Some efforts have been done to derive watermark systems specifically considering color images. Thus, in [3] the watermark is added in the blue channel motivated by the fact that the human visual system is less sensitive to this component.

In [4] a model of human color vision based on the CIELAB standard is used and the hidden information is embedded in the yellow-blue opponent component. Nevertheless, there is no need to limit the system to watermark only one component, the perceptual model will correctly weight the amplitude of the embedded signal in each component in order to preserve imperceptibility. The objectives may be the introduction of more information in the mark or the decrease in the probability of error by the diversity of including the mark in three components.

In [1][8] optimum detectors were derived in the ML sense for the case of gray-scaled images. However the extension to color images is not straightforward when the watermark is added to each component. In this work we derive optimum detectors for color images departing from an experimental model for the density function of the images that has been found to fit well in all studied images. Perceptual models are also used to ensure the invisibility of the watermark, in particular the perceptual models described in [3] and [4] are considered.

2. DIGITAL WATERMARKS

There are some techniques that successfully embed hidden information in an image. In particular, spread spectrum techniques in space (DSSS) and in frequency (FH) adapt specifically to the different requirements of a watermarking system [5]. It is interesting to attack the problem by considering the watermark as a signal 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-authorised user, therefore some kind of encription 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.

b) Visual quality of the marked image should be indistingeable from the original. The paper [2] 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 [9]. The well known masking effect is used there: a 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. On the other hand the S-CIELAB system is an extension of CIELAB which is based on

[1] This work was partially supported by the European Commission under ACTS, AC347 SUNBEAM, the Spanish National Plan of Research, through the projects CICYT, TIC98-0412 and TIC98-0703, the AECI and Generalitat de Catalunya, through the project CIRIT, 1998SGR-00081.

psychophysical studies of color discriminability and takes spatial structure also into account [3]. This system will be used to measure and reduce perceptibility in watermarked color images.

c) The amount of information this signal can convey: large amounts might increase the signal bandwidth, that implies either an increase in the probability of error or a noticeable watermark.

d) The probability of error in the detection of each symbol constituting the watermark should be as low as possible, conveying 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 thanks to the processing gain.

e) 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, a possible space-based watermarking scheme is illustrated in figure 1: it consist in a series of K=31 orthogonal symbols being each of them a pseudorandom minimum length sequence (MLS) (see figure 1).

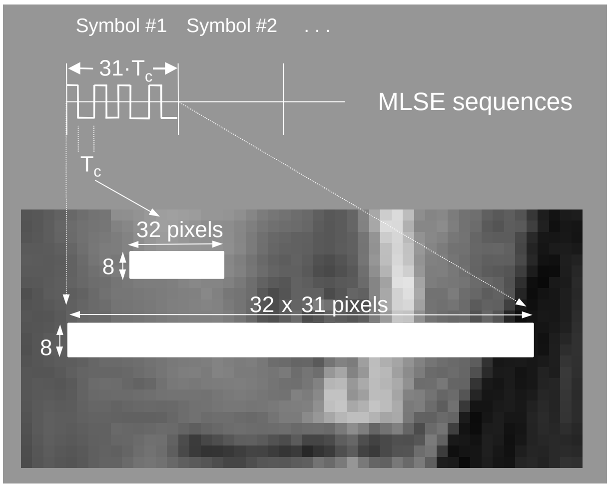

Figure 1. Watermarking on the spatial domain using DSSS sequences.

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 be orthogonal in the integration interval of size 8x992 pixels. Horizontal normalized frequencies of values $k_x/992$ (k=0,1,…,991) fit the requirements. The value of k_x cannot be too low to give noticieable 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 accomodate around 100 different frequencies.

This scheme might be reproduced for each color component, thus obtaining a system in which either three times the information can be added, or the same symbols are encountered in each component so as to obtain color-diversity and hence reduction in probability of error. The use of optimum detectors exclusively designed for a model of image and for color images will also reduce the errors with respect to the conventional detector based on the correlation.

3. OPTIMUM WATERMARK DETECTION IN COLOR IMAGES

It is required that the authorized user be able to recover the watermark with low probability of error. 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 the watermarked color image in vector notation, as $\mathbf{r} = \mathbf{p} + \mathrm{m} \circ \mathbf{q}_i$ where

$$\mathbf{r} = \begin{bmatrix} \mathbf{r}_R \\ \mathbf{r}_G \\ \mathbf{r}_B \end{bmatrix} \quad \mathbf{p} = \begin{bmatrix} \mathbf{p}_R \\ \mathbf{p}_G \\ \mathbf{p}_B \end{bmatrix} \quad \mu \circ \mathbf{q}_i = \begin{bmatrix} \mu_R \mathbf{q}_{Ri} \\ \mu_G \mathbf{q}_{Gi} \\ \mu_B \mathbf{q}_{Bi} \end{bmatrix} \qquad (1)$$

and $\circ$ stands for element-to element vector product.

r : Watermarked image with three components. In the following derivations, RGB components are used although the same derivations apply when other color components are used, for example opponent components.

p : Original three components image.

m : Amplitude that controls the total power for each component.

$\mathbf{q}_i$: Weighted symbol, that is, for each component ***X*** we have: $\mathbf{q}_{Xi} = \mathbf{f}_x \circ \mathbf{s}_i$ where $\mathbf{f}_x$ corresponds to the perceptual mask and $\mathbf{s}_i$ stands for the original symbol to code, which is a pseudorandom minimum length sequence [1].

3.1 *Optimum linear detector*

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

$$\Psi = (\mathbf{r} - \mathbf{H}_i ?)^T \mathbf{C}_{RGB}^{-1} (\mathbf{r} - \mathbf{H}_i ?) \qquad (2)$$

The detectors derived in the following make the approximation that the $\mathbf{f}_x$ amplitudes are constant, (not space dependant) which is a rough approximation if a perceptual mask is used (see sections below). This translates into 3-components for the vector q:

$$\mathbf{H}_i = \begin{bmatrix} \mathbf{s}_i & 0 & 0 \\ 0 & \mathbf{s}_i & 0 \\ 0 & 0 & \mathbf{s}_i \end{bmatrix} \quad ?^T = \begin{bmatrix} A_R & A_G & A_B \end{bmatrix} \qquad (3)$$

$$\mathbf{C}_{RGB} = \Lambda \otimes \mathbf{C}$$

$\mathbf{C}$ represents the covariance matrix that takes into account spatial correlation, and L is the correlation matrix between the three-color components. The symbol ⊗ represents kronecker product between matrices. Note that spatial correlation is assumed equal in the three components.

The decision function has to be minimized over the possible symbols $\mathbf{s}_i$, and q. It is easy to show that this is completely equivalent to maximize the decision function over *i*:

$$\begin{aligned}\Psi_i &= \mathbf{r}^T \mathbf{C}_{RGB}^{-1} \mathbf{H}_i \hat{?}_i = \\ &= \mathbf{r}^T \mathbf{C}_{RGB}^{-1} \mathbf{H}_i \left(\mathbf{H}_i^T \mathbf{C}_{RGB}^{-1} \mathbf{H}_i\right)^{-1} \mathbf{H}_i^T \mathbf{C}_{RGB}^{-1} \mathbf{r}\end{aligned} \quad (4)$$

A first-order Markov model is assumed for $\mathbf{C}$ (the covariance of the original image) and although a closed form of the inverse can be derived, it is more convenient to use a pre-whitening filter playing the role of $\mathbf{C}^{-1/2}$. Analogously $\mathrm{L}^{-1/2}$ represents the pre-whitening among the RGB components. Thus, the decision function is simplified to:

$$\begin{aligned}\Psi_i &= \frac{\left|\mathbf{r}_{wR}{}^T \mathbf{s}_{swi}\right|^2 + \left|\mathbf{r}_{wG}{}^T \mathbf{s}_{swi}\right|^2 + \left|\mathbf{r}_{wB}{}^T \mathbf{s}_{swi}\right|^2}{\mathbf{s}_{swi}^T \mathbf{s}_{swi}} \\ \mathbf{r}_{wR,G,B} &= (? \otimes \mathbf{C})^{-1/2} \mathbf{r}_{R,G,B} \\ \mathbf{s}_{swi} &= \mathbf{C}^{-1/2} \mathbf{s}_i\end{aligned} \quad (5)$$

$\mathbf{r}_{wX}$ is a whitened version of the *X* component of the watermarked image in space and color dimensions and $\mathbf{s}_{swi}$ is the symbol $\mathbf{s}_i$ that is whitened in the spatial dimension only.

3.2 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 [6], which concentrate around the mean but are also characterized by heavier tails. In particular we consider a Cauchy distribution. Figures 2 to 4 show the distribution of the whitened RGB components for a certain image. As it can be seen the Cauchy distribution is closer to the histogram than the Gaussian distribution. This result has been found to be general for all tested real images.

Considering the Cauchy distribution, we derive an optimum receiver in the maximum likelihood sense to decide which symbol is present in a region of the watermarked image, that is:

$$\Psi_i^C = \min_{s_i} \sum_{k=1}^{N} \log\left[\gamma^2 + z_i(k)^2\right] \quad (6)$$

where *N* is the number of pixels in the block in which a symbol is present, γ is the distribution dispersion (which can be estimated according to the lines in [8] on the whitened components) and $z_i(k)$ are the *N* components of the vector:

$$\begin{aligned}\mathbf{z}_i &= \mathbf{C}_{RGB}^{-1/2}\left(\mathbf{r} - \mathbf{H}_i^D ?\right) = \\ &= \mathbf{r}_w - \frac{1}{\mathbf{s}_{wsi}^T \mathbf{s}_{wsi}} \begin{bmatrix} \mathbf{s}_{wsi} \mathbf{s}_{wsi}^T \mathbf{r}_{wR} \\ \mathbf{s}_{wsi} \mathbf{s}_{wsi}^T \mathbf{r}_{wG} \\ \mathbf{s}_{wsi} \mathbf{s}_{wsi}^T \mathbf{r}_{wB} \end{bmatrix}\end{aligned} \quad (7)$$

This detector greatly improves the probability of error with respect to the Gaussian.

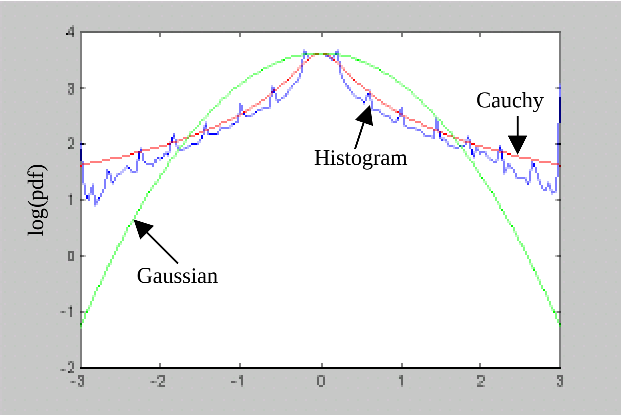

Figure 2: Histogram of the whitened R component, Gaussian pdf and Cauchy pdf for a given image

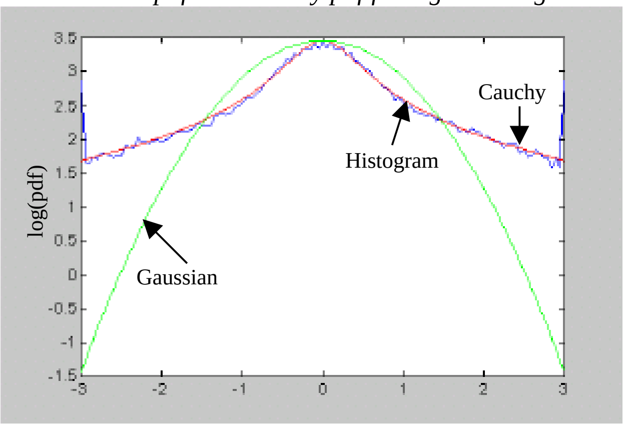

Figure 3: Histogram of the whitened G component, Gaussian pdf and Cauchy pdf for a given image

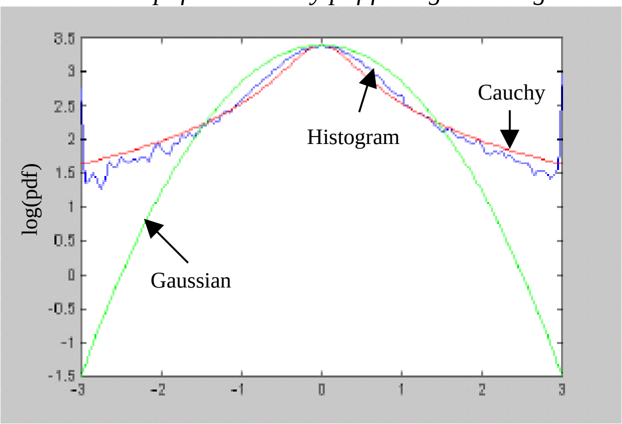

Figure 4: Histogram of the whitened B component, Gaussian pdf and Cauchy pdf for a given image

4. COLOR PERCEPTUAL MODELS

For a watermark to be really imperceptible it has to be spatially windowed in a way that accounts for the perceptual characteristics of the human visual system. A straightforward approach is to the use the Gabor filter model used in [2] for each color component. A more rigurous approach is to use the advanced perceptual model for color images given by the S-CIELAB. The interest of this model is twofold: it takes into account the spatial information of the image, and it translates the three color components to a basis in which a linear increment is linearly perceived as a color change. The watermark generation scheme based on S-CIELAB [4] is shown in figure 5.

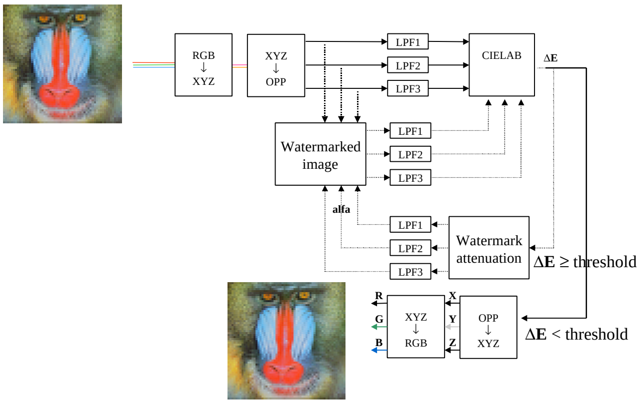

Figure 5: Watermark Embedding using S-CIELAB

The watermark is applied to the opponent color components, which are yellow-blue (YB), red-green (RG) and luminance (L). Nevertheless numerical differences that correspond to perceptual differences are measured in the Lab space. Thus, for each pixel the perceptual difference between the original image and the watermarked image is given by :

$$\Delta E = \sqrt{\Delta L^2 + \Delta a^2 + \Delta b^2} \qquad (8)$$

Although usually *DE* should be lower than 3 to be unnoticeable, a more restrictive measure of *DE*<1 is sometimes used. Those pixels that are above the selected threshold are attenuated until a high percentage of pixels, usually 99%, are under the threshold. Figure 6 shows how the perceptual measure is computed.

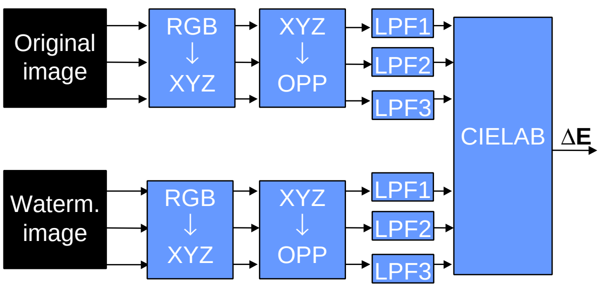

Figure 6: Computation of the error measure in the S-CIElab model

5. RESULTS

In order to assess the performance of the different detectors using different perceptual models, the error rate has been computed by marking several color images with a set of symbols. The images were obtained from the Petitcolas' benchmark database [10], where one can find different synthetic and real images with diverse spatial and luminance characteristics. First, Gabor models are considered and two tests have been made: luminance-only watermarking and RGB components watermarking, using the same info in the three components. This allows some kind of diversity that will surely be used by the detector to decrease the probability of error in the symbol detection. Additional and significant gain is obtained from the use of the Cauchy detector with respect to the conventional Gaussian (with whitening), as seen in table 1. 7500 symbols were added to the set of images, so reliable estimations of the probability of error are above 10^{-3} .

The three LAB components have been also marked using the S-CIELAB model with a perceptual *DE*=1. Somewhat better visual results were obtained. The watermark exhibited structural differences as shown in figure 7. However, the probability of error showed minor differences with respect to the RGB and have been associated to the first column in table 1.

Table 1: Error rate when watermarking the RGB/LAB and luminance components, for the two detectors

	RGB/LAB	Luminance
Gaussian	2,6e-3	1,4e-2
Cauchy	1,7e-3	9,6e-3

Robustness with respect to the JPEG compression has been tested for the luminance and the three components watermarking. Results in table 2 also show that in general, it is better to watermark the RGB components than the luminance component, specially under JPEG compression. On the other side, the Cauchy detector gives better results compared to the optimum linear detector. In all cases the original image and the marked image were visually equivalent.

Table 2: Error rate when watermarking the RGB/LAB and luminance components for the two detectors when image is compressed

JPEG	RGB/LAB		Luminance	
	Cauchy	Gaussian	Cauchy	Gaussian
Q=50	9,5e-2	5,8e-2	1,6e-1	1,9e-1
Q=70	2,9e-2	5,5e-2	1,2e-1	1,5e-1
Q=90	3,7e-2	7,8e-2	5,8e-2	6,6e-2

6. CONCLUSIONS

A watermark embedding and detecting system for color images that relies on perceptual models has been proposed. Consequently, comparison between the original and the watermarked image shows imperceptible differences by the human eye. An optimum detector has been developed showing lower probability of error with respect to: 1) optimum linear detector thanks to a better adaptation to the image model, and 2) luminance watermarking, due to the diversity allowed by the use of three color components. These observations are reproduced, although less evidently, when the image suffers high degradation via JPEG compression. It has also been assesed that the S-CIELAB model gives slightly better visual results.

Work is in progress to use redundant coding to reduce the probability of error and modulations in the frequential domain so as to avoid synchronization problems when the image is cropped.

7. REFERENCES

[1] Josep Vidal, Elisa Sayrol, "Optimum Watermark Detection and Embedding in Digital Images", *Proc. of IEEE Workshop on Multimedia Signal Processing*, Los Angeles, CA, December 1998, pp. 285-290.

[2] J.F. Delaigle, et al., "Low Cost Watermarking Based on a Human Visual Model", *Proc. ECMAST 97*, 1997.

[3] M. Kutter, F. Jordan, F. Bossen, "Digital watermarking of color images using amplitude modulation", Journal of Electronic Imaging 7(2), pp. 326-332, April 1998.

[4] David J. Fleet, David J. Heeger, "Embedding Invisible Information in Color Images", *Proc. of ICIP '97*, Santa Barbara, October 1997, pp 532-535

[5] I. J. Cox, et al., "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. on Image Processing*, vol. 6, no 12, Dec. 1997

[6] 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 93.

[7] 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.

[8] J.R. Hernández, F. Pérez-González, "Statistical Analysis of Watermarking Schemes for Copyright Protection of Images", *Proc. of IEEE*, vol. 87, no. 7, July 1999, pp. 1142-1166.

[9] S. Mallat "Multifrequency Channel Decompositions of Images and Wavelet Models", *IEEE Trans. on ASSP*. Vol 37, No 12, pag 2091-2094.

[10]http://www.cl.cam.ac.uk/~fapp2/watermarking/benchmark/image_database.html

Figure 7. Original image (top) and the watermarks obtained using the Gabor perceptual ponderation (middle) and the S-CIElab (bottom). Most of the watermark information is placed on the image contours.