A M.A.P. IDENTIFICATION CRITERION FOR DCT-BASED WATERMARKING

M. Barni, F. Bartolini, V. Cappellini, A. Piva, F. Rigacci
Dipartimento di Ingegneria Elettronica, Università di Firenze,
Via Santa Marta 3,
50139 Firenze, ITALY
Tel: +39 55 4796380; fax: +39 55 494569
e-mail: barto@cosimo.die.unifi.it

ABSTRACT

For reliably protecting the rights of multimedia data owners, digital watermarking techniques appear to be the best solution. A digital watermark is a code which is hidden into the multimedia data for carrying information regarding the copyright. In this paper the problem of the reliable identification of the watermark, in absence of the original unmarked image, is addressed. An optimum (based on a MAP, Maximum A Posteriori probability, criterion) watermark identificator is designed, for extracting watermarks inserted in the DCT domain. The watermark identificator is based on the knowledge of the probability density function of the DCT coefficients. The results support the optimality of the identificator and prove the robustness of the approach.

1 INTRODUCTION

Images are maybe the most powerful media the man can communicate by. All around the world, a huge and rich pictorial patrimony is available, for example in museums and photographic archives, and most of it is already in a digital form. Nevertheless multimedia products, such as CD-ROMs or WEB sites, supply often very low quality pictures, and this happens despite the wide market that could be interested by these productions. The primary contributing factor to the limited development of the commerce of electronic images is the unavailability of effective means to protect the rights of the owners. Once a digital image has been sold, the purchaser could, in fact, reproduce as many identical copies of it as he wants, modify them and, for example, sell them again. What it could be useful is to tightly attach to the digital image some information for granting the rights of the original owner.

This is the aim of image watermarking techniques [6], that hide into the image some perceptually invisible codes (signatures), usable for carrying information related to legal or commercial properties of the data. Such a code should be easily and reliably identifiable, its insertion should not visibly deteriorate the image, and its identification should be possible also after the image has been processed (e.g. by JPEG compression) [8]. Recently also the non cancelability of the watermark is emerging as an important requirement [14] to be satisfied. During the last few years many watermarking techniques have been proposed. Watermarking data are embedded either in the spatial [5, 7], or in the frequency domain [2, 13]; the properties of the Human Visual System are, sometimes, exploited for decreasing watermark visibility and enhancing robustness [11].

In this paper a novel technique for identifying watermarks embedded in the DCT domain is presented. The technique, based on a MAP criterion, is mainly aimed to optimize watermark identifiability. The considered watermarking technique modifies, proportionally to their values, some coefficients of the image full frame DCT. An optimum identificator is thus designed, which exploits the knowledge of the probability density function (pdf) of the full frame DCT coefficients to minimize the error probability. Results are presented that support the optimality of the proposed identificator, and demonstrate its robustness.

2 OPTIMUM DETECTION BASED ON THE MAP CRITERION

Given that robustness of frequency domain based watermarking techniques has been already demonstrated [3], we choose to embed the signature into a subset of the image full frame DCT coefficients. The watermark encoding/decoding process can be modeled as a communications process: the watermark is the transmitted signal and the image is the channel noise. An optimum receiver (identificator) is, thus, designed which minimizes the identification error probability.

In order to evaluate how the noise affects the transmitted signal, the watermark casting procedure has to be specified. Given an image to be watermarked, its full frame DCT is first computed; the coefficients of the DCT are, then, zig-zag reordered, and a subset in the mid frequency range is selected in the following way: N are skipped and the next L are put in a vector $\vec{x} = \{x_j\}_{j=0,\dots L-1}$. The elements of vector $\vec{x}$ are modified producing the vector $\vec{y} = \{y_j\}_{j=0,\dots L-1}$

$$y_j = x_j + \alpha m_{ij} x_j \qquad j = 0, \dots, L-1 \tag{1}$$

where α is a weighting factor, and $\vec{m}_i = \{m_{ij}\}_{j=0,\ldots L-1}$ is the i^{th} watermark of the M available. The modulation law in (1) is designed to take into account the frequency masking characteristics of the Human Visual System [12]. In fact, the perceptibility threshold of a sinusoidal grating depends on the amplitude of the isofrequential signal to which it is superimposed. The modified vector $\vec{y}$ is then inserted, in place of vector $\vec{x}$, in the full frame DCT, the inverse transformation is applied to obtain the watermarked image. From equation (1) it is apparent that, in our channel model, the noise (i.e. the image) affects the signal (i.e. the watermark) in an additive and multiplicative way.

The first step of watermark identification is the extraction of the subset of modified coefficients from the full frame DCT of the watermarked image. By supposing that the signed image has not been modified, the vector $\vec{y}$ is obtained. The mark, among the M available, which maximizes the posterior probability is then searched for, i.e.:

$$\max_{i=0,\ldots M-1} Pr(\vec{m}_i/\vec{y}). \tag{2}$$

By applying the Bayes rule, this equation can be rewritten as:

$$\max_{i=0,\ldots M-1} \frac{p_Y(\vec{y}/\vec{m}_i)Pr(\vec{m}_i)}{p_Y(\vec{y})} \tag{3}$$

by observing that the marginal pdf $p_Y(\vec{y})$ does not depend on $\vec{m}_i$, and by supposing that all marks are equiprobable (i.e. $Pr(\vec{m}_i) = \text{constant}$), the problem reduces to find the signature for which is

$$\max_{i=0,\ldots M-1} p_Y(\vec{y}/\vec{m}_i). \tag{4}$$

It is well known that the DCT is a quasi-optimal transformation for real images [4], in the sense that the transformed coefficients are uncorrelated; we will also assume they are independent. With this hypothesis and from (1) it follows that also the element of vector $\vec{y}$ are independent, so that equation (4) becomes:

$$\max_{i=0,\ldots M-1} \prod_{j=0}^{L-1} p_{Y_j}(y_j/\vec{m}_i) \tag{5}$$

furthermore each element y_j depends only on the corresponding element m_{ij} of the signature vector; thus, the expression to be maximized is:

$$\max_{i=0,\ldots M-1} \prod_{j=0}^{L-1} p_{Y_j}(y_j/m_{ij}). \tag{6}$$

Now, the conditional pdf in this equation can be easily computed by considering the modulation law (1) and the theory of the functions of random variables [9]:

$$p_{Y_j}(y_j/m_{ij}) = \frac{1}{1+\alpha m_{ij}} p_{X_j}\left(\frac{y_j}{1+\alpha m_{ij}}\right). \tag{7}$$

By inserting this last equation into the (6) and by using a logarithmic formulation, a cost function is obtained which has to be maximized to find the embedded watermark:

$$\max_{i=0,\ldots M-1} \sum_{j=0}^{L-1} \log\left(p_{X_j}\left(\frac{y_j}{1+\alpha m_{ij}}\right)\right) - \log\left(1+\alpha m_{ij}\right). \tag{8}$$

For actually designing the watermark identificator defined by (8), the pdf of the full frame DCT coefficients X_j needs to be known. This requirement is a consequence of the fact that, in our model, the noise affecting the channel is not only additive but also multiplicative. A statistical analysis has been carried out to estimate the pdf of the coefficients of the full frame DCT of a large set of images [1]. A good approximation results to be the Laplacian function:

$$p_{X_j}(x_j) = \frac{\lambda_j}{2} e^{-\lambda_j |x_j|} \tag{9}$$

which, inserted into the (8), allows to obtain the optimum watermark identificator

$$\max_{i=0,\ldots M-1} \sum_{j=0}^{L-1} \log\left(\frac{\lambda_j}{2}\right) - \lambda_j \left|\frac{y_j}{1+\alpha m_{ij}}\right| - \log\left(1+\alpha m_{ij}\right). \tag{10}$$

By observing the last equation it is noted that the term $\log\left(\frac{\lambda_j}{2}\right)$ of the sum does not depend on index i, a more compact formulation can, thus, be obtained by eliminating it.

3 EXPERIMENTAL RESULTS

Some experiments have been carried on for supporting the statement of optimality of the identificator. In a previous work of the authors [10] another DCT-based watermarking scheme is presented, where the modulation law is:

$$y_j = x_j + \alpha m_{ij} |x_j| \qquad j = 0, \ldots, L-1. \tag{11}$$

The absolute value is needed for the correlation identificator, proposed there, to work properly. An optimum identificator can be designed also for this modulation law, following the steps described in previous section. A comparison is thus performed among the two optimum identificators based on modulation laws (1) and (11) and the correlation identificator proposed in [10]. The performances are compared in the following way: 1000 (i.e. $M = 1000$) marking vectors, whose element are uncorrelated each other and have a normal distribution, are generated; for each one of the 3 methods, one of the marking vectors is embedded and successively identified; the embedding/identification step is repeated by decreasing the weighting factor α, until the identificator fails. The other parameters have been chosen $N = 16000$ and $L = 16000$. In Figure 1 the mini-

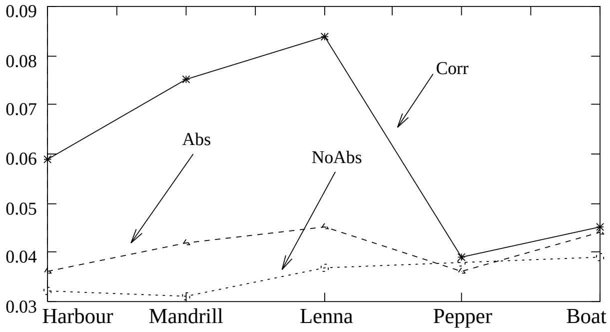

Figure 1: Minimum values of the α parameter which can be successfully used with the three different identificators, plotted with respect to the 5 different images used for testing. "Corr" refers to the correlation identificator, "NoAbs" to the optimum identificator proposed, and "Abs" to the optimum identificator designed for the modulation law in (11).

mum values of α which can be successfully used with the three different identificators are plotted with respect to 5 standard images used for testing. From the plot it is evident that the identificator proposed in the previous section is (almost always) the best. Furthermore the optimum identificator for the modulation law in (11), always outperforms that one based on the correlation function, thus confirming the validity of the approach.

Robustness of the identificator is tested against some common signal processing algorithms and geometric distortions by using some standard images. Here some preliminary results are shown regarding image "Lenna". The weighting factor is $\alpha = 0.1$ for granting watermark invisibility. In Figure 2 the watermarked image is shown which confirms watermark invisibility; in Figure 3 the responses of the identificator to the 1000 marks are plotted, it is evident the maximum value which is achieved for the embedded watermark (no. 444).

In Figure 4 the watermarked image compressed by the JPEG algorithm with a 10% quality factor, is depicted: the image is visibly deteriorated. Nevertheless the proposed algorithm is still able to identify the watermark (in Figure 5 the responses of the system to the 1000 marks are plotted).

The algorithm has demonstrated to be resistant also to low-pass and median filtering, to histogram stretching and to image dithering. With regard to geometric distortions, thanks to the properties of DCT transform the algorithm is resistant to image resizing (the spatial sampling step is enlarged, and aliased spectra approaches each other, but also the number of frequency samples reduces by the same factor, so that the medium range frequencies, where the watermark is embedded, remains unchanged), but is resistant to image cropping only if the cropped portion can be replaced in the same position it has in the original image. Further investigations will be needed to solve this last problem.

Figure 2: Image "Lenna" watermarked with weighting factor $\alpha = 0.1$.

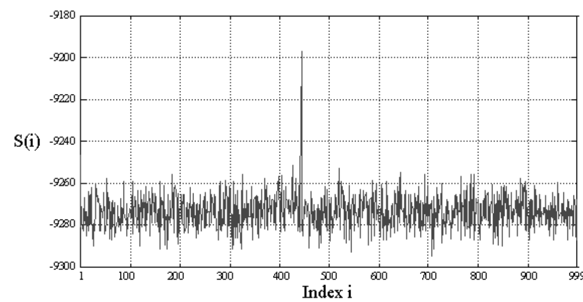

Figure 3: Plot of responses of the optimum identificator to the 1000 marks.

4 CONCLUSIONS AND FUTURE DEVELOPMENTS

In the paper a new identificator has been designed, based on MAP criterion, for extracting watermarks embedded in the DCT domain. The identificator has been demonstrated to be optimum and robust with respect to common signal processing techniques and geometric distortions.

Future research will be devoted to investigate the use of DFT instead of DCT, in such a way to allow the watermarking system to resist to geometric translations. Furthermore, in the present state, the masking characteristics of the Human Visual System are exploited only in the frequency domain, spatial effects are neglected. We are confident that a spatial weighting procedure, similar to that one proposed in [10], will reduce visibility and enhance robustness of the system.

Figure 4: Image "Lenna" watermarked with weighting factor $\alpha = 0.1$ and compressed by JPEG with a 10% quality factor.

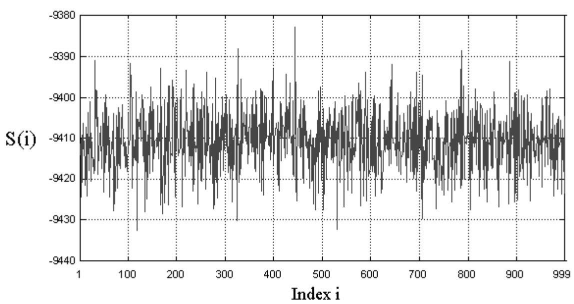

Figure 5: Plot of responses of the optimum identificator to the 1000 marks in the case of the JPEG compressed image.

5 ACKNOWLEDGEMENTS

This work was partially supported by the "Progetto Finalizzato Beni Culturali" (Finalized Project for Cultural Heritage) of the Italian National Research Council (CNR).

References

[1] M. Barni, F. Bartolini, A. Piva, and F. Rigacci. Statistical modelling of full frame DCT coefficients. In *Proc. EUSIPCO '98*, Rhodes, Greece, 1998.

[2] A. Bors and I. Pitas. Image watermarking using DCT domain constraints. In *Proc. IEEE Internat. Conf. Image Processing '96*, pages 231–234, Lausanne, Switzerland, September 16-19 1996.

[3] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. Technical Report 95-10, NEC Research Institute, 1995.

[4] A. K. Jain. *Fundamentals of Digital Image Processing*. Prentice Hall, Englewood Cliffs, New Jersey, USA, 1989.

[5] G. C. Langelaar, J. C. A. Van der Lubbe, and J. Biemond. Copyright protection for multimedia data based on labeling techniques. In *17th Symp. Information Theory in the Benelux*, Enschede, The Netherlands, May 1996.

[6] B. M. Macq and J. J. Quisquater. Cryptology for digital TV brodacasting. *Proceedings of the IEEE*, 83(6):944–957, June 1995.

[7] N. Nikolaidis and I. Pitas. Copyright protection of images using robust digital signatures. In *Proc. IEEE Internat. Conf. Acoustics, Speech & Signal Processing '96*, pages 2168–2171, Atlanta, GA, May 7-10 1996.

[8] J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland. Watermarking digital images for copyright protection. *Proc. of the IEE - Vis. Image Signal Processing*, 143(4):250–256, August 1996.

[9] A. Papoulis. *Probaility, Random Variables, and Stochastic Processes*. McGraw Hill, third edition, 1991.

[10] A. Piva, M. Barni, F. Bartolini, and V. Cappellini. DCT-Based watermark recovering without resorting to the uncorrupted original image. In *Proc. IEEE Internat. Conf. Image Processing '97*, pages 520–523, Santa Barbara, CA, October 26-29 1997.

[11] C. Podilchuk and W. Zeng. Perceptual watermarking of still images. In *Proc. The First IEEE Signal Processing Society Workshop on Multimedia Signal Processing*, Princeton, New Jersey, June 1997.

[12] C. F. Stromeyer III and B. Julesz. Spatial frequency masking in vision: Critical bands and spread of masking. *Journal of the Optical Soc. of America*, 62(10):1221–1232, October 1972.

[13] B. Tao and B. Dickinson. Adaptive watermarking in the DCT domain. In *Proc. IEEE Internat. Conf. Acoustics, Speech & Signal Processing '97*, Munich, Germany, April 21–24 1997.

[14] W. Zeng and B. Liu. On resolving rightful ownerships of digital images by invisible watermarks. In *Proc. IEEE Internat. Conf. Image Processing '97*, pages 552–555, Santa Barbara, CA, October 26-29 1997.