A Framework for Optimal Adaptive DCT Watermarks

Shelby Pereira and Thierry Pun
University of Geneva - CUI, 24 rue General Dufour, CH 1211 Geneva 4, Switzerland
Email: {Shelby.Pereira,Thierry.Pun}@cui.unige.ch

ABSTRACT

In this paper we address the problem of robustly embedding 64 bits into an image while taking into account the HVS. The proposed method is general in that any mask can be adopted. The main advantage of the framework we present is that we demonstrate how to optimally embed a watermark given the constraints imposed by the mask in the spatial domain. This is in sharp contrast with the bulk of publications which embed a watermark in the DCT domain and then truncate or modulate in the spatial domain in order to satisfy masking constraints. The problem with these approaches is that spatial domain truncation or modulation leads inevitably to the degradation of the watermark in the DCT domain. Results indicate that our proposed approach is robust against JPEG compression at a quality factor of 30images of size 64 by 64.

1 Introduction

The World Wide Web, digital networks and multimedia afford virtually unprecedented opportunities to pirate copyrighted material. Consequently, the idea of using a robust digital watermark to detect and trace copyright violations has therefore stimulated significant interest among artists and publishers. In order for a watermark to be useful it must be robust to a variety of possible attacks by pirates. These include robustness against compression such as JPEG, scaling and aspect ratio changes, rotation, cropping, row and column removal, addition of noise, filtering, cryptographic and statistical attacks, as well as insertion of other watermarks. A discussion of possible attacks is given in [4]. In this publication however, we consider only attacks that do not change the geometry of the image. Our aim is to construct an optimal DCT domain watermark which takes into account the properties of the human visual system (HVS). While we formulate the problem in the DCT domain we note that the approach is easily extendible to other transforms such as the DFT, Hartley or Wavelet transforms.

Much work has been been done in the now relatively mature field of DCT domain watermarking. The most recent work involves sophisticated masking models incorporating brightness, frequency and contrast which have been used in combination with an embedding into 8x8 DCT blocks [5, 8]. With few exceptions, the work in watermarking has involved a one bit watermark. That is, at detection a binary decision is made as to the presence of the watermark most often using hypothesis testing [9]. Barni [1] encodes roughly 10 bits by embedding 1 watermark from a set of 1000 into the DCT domain. The recovered watermark is the one which yields the best detector response. In practice however, many more applications are possible when the watermark length is of the order 60 bits since this allows for a unique identifier specifying the owner and buyer of an image as well as possibly indicating the type of content in the image. Such schemes are much more flexible, but the problem is more challenging.

In this paper we address the problem of robustly embedding 64 bits into an image while taking into account the HVS. The proposed method is general in that any mask can be adopted. The main advantage of the framework we present is that we demonstrate how to optimally embed a watermark given the constraints imposed by the mask in the spatial domain. This is in sharp contrast with the bulk of publications which embed a watermark in the DCT domain and then truncate or modulate in the spatial domain in order to satisfy masking constraints (see [1] for example). The problem with these approaches is that spatial domain truncation or modulation leads inevitably to the degradation of the watermark in the DCT domain.

2 Problem Formulation

We assume that we are given an image to be watermarked denoted $\boldsymbol{I}$. If it is an RGB image we work with the luminance component. We are also given a masking function $\boldsymbol{V}(\boldsymbol{I})$ which returns 2 matrices of the same size of $\boldsymbol{I}$ containing the values $\Delta_{pi,j}$ and $\Delta_{ni,j}$ corresponding to the amount by which pixel $I_{i,j}$ can be respectively increased and decreased without being noticed. We note that these are not necessarily the same since we also take into account truncation effects. That is pixels are integers in the range $0-255$ consequently it is possible

to have a pixel whose value is 1 which can be increased by a large amount, but can be decreased by at most 1. The function $\boldsymbol{V}$ can be a complex function of texture,luminance, contrast, frequency and patterns. We wish to embed $\boldsymbol{m} = (m_1, m_2 ... m_M)$ where $m_i \in \{0,1\}$ and M is the number of bits in the message. In our scheme, the binary message is first coded using the well known BCH codes [6] to produce the message $\boldsymbol{m_c}$ of length $M_c = 128$. Without loss of generality we assume the image $\boldsymbol{I}$ is of size 64×64 corresponding to a very small image. For larger images the same procedure is adopted for each 64×64 large block. To embed the message, we first divide the image into 8×8 blocks. In each 8×8 block we embed 2 bits from $\boldsymbol{m_c}$. In order to embed a 1 or 0 we respectively increase or decrease the value of a DCT coefficient. Once the DCT domain watermark has been calculated, we compute the inverse DCT transform and add it to the image in the spatial domain. At decoding, we take the sign of the DCT coefficient, apply the mappings $(+ \rightarrow 1), (- \rightarrow 0)$ and then decode the BCH codes to correct possible errors.

The central problem with this scheme is that during embedding we would like to increase or decrease the DCT coefficients as much as possible for maximum robustness, but we must satisfy the constraints imposed by $\boldsymbol{V}$ in the spatial domain. In order to accomplish this, we formulate the problem for each 8x8 block, as a standard constrained optimization problem as follows. For each block we select 2 mid-frequency coefficients in which we will embed the information bits. We then have:

$$\min_{\boldsymbol{x}} \boldsymbol{f}'\boldsymbol{x} \qquad ; \qquad \boldsymbol{A}\boldsymbol{x} \leq \boldsymbol{b} \tag{1}$$

$\boldsymbol{x} = [x_{11} \ldots x_{81} x_{12} \ldots x_{82} \ldots x_{18} \ldots x_{88}]^t$ is the vector of DCT coefficients arranged column by column. $\boldsymbol{f}$ is a vector of zeros except in the positions of the 2 selected coefficients where we insert a -1 or 1 depending on whether we wish to respectively increase or decrease the value of the coefficients as determined by $\boldsymbol{m_c}$. $\boldsymbol{A}\boldsymbol{x} \leq \boldsymbol{b}$ contain the constraints which are partitioned as follows.

$$\boldsymbol{A} = \begin{bmatrix} IDCT \\ ---- \\ -IDCT \end{bmatrix}; \quad \boldsymbol{b} = \begin{bmatrix} \Delta_p \\ ---- \\ \Delta_n \end{bmatrix} \tag{2}$$

where IDCT is the matrix which yields the 2D inverse DCT transform of $\boldsymbol{x}$ (with elements of the resulting image arranged column by column in the vector). We also note that we take Δ_p and Δ_n to be column vectors where the elements are taken column wise from the matrices of allowable distortions. Stated in this form the problem is easily solved by the well known Simplex method. Stated as such the problem only allows for spatial domain masking, however many authors [7] suggest also using frequency domain masking. This is possible by adding the following constraints:

$$\boldsymbol{L} \leq \boldsymbol{x} \leq \boldsymbol{U} \tag{3}$$

Here $\boldsymbol{L}$ and $\boldsymbol{U}$ are the allowable lower and upper bounds on the amount we by which we can change a given frequency component. The Simplex method can also be used to solve the problem with added frequency domain constraints.

We note that by adopting this framework, we in fact allow *all* DCT coefficients to be modified (in a given 8x8 block) even though we are only interested in 2 coefficients at decoding. This is a novel approach which has not appeared in the literature. Other publications select a subset of coefficients to mark while leaving the rest unchanged. In words, we are "making space" for the watermark in an optimal fashion by modifying elements from the orthogonal complement of the coefficients we are interested in, while satisfying spatial domain constraints. One important point to note is that in some cases we may not be able to modify a DCT coefficient sufficiently so as to change the sign. In this case, at decoding, the wrong sign will be obtained. However since we have embedded the sequence using error correction codes, several errors will be detected and correctly decoded. Our results indicate that this approach works well in practice.

3 Results

The algorithm was tested on several small images of size 64x64. The simple masking function of luminance and texture proposed in [2] was used. In all cases the watermarked image was indistinguishable from the original. To the 64 bit message was added a 20 bit checksum. The new message was encoded using BCH codes to yield a message of length 128. The 20 bit checksum is essential in determining the presence of the watermark. At detection if the checksum is verified we can safely say (with probability $\frac{1}{2^{20}}$ of error) that a watermark was embedded and successfully decoded. Our results indicate that the algorithm is robust down to a level of 30% quality factor and is resistant as well to low and high pass filtering. Unfortunately, little or no work has been done with small images, so a fair comparison is not possible. Typically publications present results for images of size 256×256. Relative to JPEG, our algorithm shows excellent performance since typically algorithms break down at JPEG 30-50% quality factor. Furthermore the bulk of the literature contains 1 bit watermarks while we encode a much larger payload consisting of 64 bits. We note that the small image case is important in practice since one possible application is the watermarking of logos and thumbnails of images.

Work is currently under way to apply the ideas of [2] so as to make the algorithm resistant to geometric changes as well. This would consist of adding a DFT domain template which consists of peaks at known po-

sitions. The decoding process would then consist of locating the peaks and consequently detecting any affine transformation as described in [3], followed by decoding the DCT domain watermark. The fact that such a multiple domain approach works in practice was shown in [2].

4 Conclusion

In this article we have described a new algorithm for the embedding DCT watermarks in an optimal manner. The algorithm is extremely flexible in that constraints as determined by masking functions can be easily incorporated in the spatial or frequency domain and any linear transform domain may be used although here we considered the special case of the DCT. Furthermore we show how to handle problems with truncation in an optimal way and propose the novel approach of modifying all DCT domain coefficients even though we are only interested in a small subset. The algorithm allows for the recovery of 64 bits of information in a small image even after a significant JPEG compression.

References

[1] M. Barni, F. Bartolini, V. Cappellini, A. Piva, and F. Rigacci. A M.A.P. identification criterion for DCT-based watermarking. In *EUSIPCO'98*, Rhodes, Greece, September 1998.

[2] S. Pereira, J. J. K. Ó Ruanaidh, and T. Pun. Secure robust digital image watermarking using the lapped orthogonal transform. In *IS&T/SPIE Electronic Imaging'99*, San Jose, CA, USA, January 1999.

[3] S. Pereira and T. Pun. Fast robust template matching for affine resistant watermarks. In *3rd International Information Hiding Workshop*, Dreseden, Germany, September 1999.

[4] F. A. P. Petitcolas and R. J. Anderson. Attacks on copyright marking systems. In *2nd International Information Hiding Workshop*, pages 219–239, Portland, Oregon, USA, April 1998.

[5] C. I. Podilchuk and W. Zeng. Perceptual watermarking of still images. In *Proc. Electronic Imaging*, volume 3016, San Jose, CA, USA, February 1996.

[6] C. B. Rorabaugh. *Error Coding Cookbook*. The McGraw-Hill Companies, 1996.

[7] M. D. Swanson, B. Zhu, and A.H. Tewfik. Robust data hiding for images. In *7th IEEE Digital Signal Processing Workshop*, pages 37–40, Loen, Norway, September 1996. G:WM1-A23.

[8] B. Tao and B. Dickinson. Adaptive watermarking in the DCT domain. In *IEEE Int. Conference on Image Processing '96 Proceedings*, Lausanne, Switzerland, September 1996.

[9] G. Voyatzis and I. Pitas. The use of watermarks in the protection of digital multimedia products. *Proceedings of the IEEE*, 87(7), July 1999.