DLT-BASED DIGITAL IMAGE WATERMARKING

S. Asif Mahmood Gilani[1] and A. N. Skodras[1,2]

[1]Electronics Laboratory
University of Patras
GR-26110 Patras
Greece

[2]Computer Technology Institute
PO Box 1122
GR-26110 Patras
Greece

ABSTRACT

The effectiveness of the discrete Laguerre transform (DLT) in digital image watermarking is examined in the present communication. Extensive performance comparisons between the DLT- and DCT-domain watermarking are conducted. It is seen that the quality of the DLT-domain watermarked images is higher than the corresponding DCT-domain watermarked images. From the robustness point of view, it is proved that both the DLT and DCT watermarking approaches have similar performance.

1. INTRODUCTION

Rapidly growing field of digitized images, video and audio has urged the need of copyright protection, which can be used to produce an evidence against any illegal attempt to either reproduce or manipulate them in order to change their identity. Although watermarking has been proved to be an active area of research for some time, it seems that it is still passing through its adolescent age. Many watermarking techniques do exist. These can be divided into two broad categories, those working in the *spatial / time domain* and those working in the *transform (frequency) domain* [1].

There has been a significant recent research into digital *watermarks* (hidden copyright messages) and *fingerprints* (hidden serial numbers); the idea is to exploit these techniques in order to identify copyright violators, and to prosecute them. Copyright marks do not always need to be hidden, as some systems use visible digital marks [1,2]. The concentration though is on invisible or transparent digital watermarks, which have wider applications. Visible digital watermarks are more or less digital counterpart of original paper watermarks, which appeared at the end of thirteenth century to differentiate paper makers of that time. Fragile watermarks that are referred to as *signatures* create confusion with digital signatures used in cryptography. They are destroyed as soon as the object is modified too much, and they are useful in checking if the image is modified intentionally or by chance and can be used as evidence in the court of law. Robust marks have the property that it is difficult to remove them until the host data is degraded enough. This usually means that the mark should be embedded in the perceptually most significant components of the object. There are several types of robust copyright marking systems:

- **Private marking system or incomplete or escrow watermarking** is the system that requires the original and the watermarked versions of images to extract the watermark.

- **Public marking or complete or oblivious or blind watermarking** remains the most challenging problem since neither it requires original image nor the embedded watermark.

In many ways an incomplete watermark is better since the original image or video is available for the recovery process, which makes watermark recovery rather easier and more robust. In fact, the information that is the actual image or video, can be subtracted from the signed version leaving a reasonably pure version of the watermark. On the other hand, complete watermarking makes the watermark recovery process more difficult and less robust.

Digital steganography or information hiding can be studied using communication theory. The parameters of information hiding, such as the number of data bits that can be hidden, the invisibility of message, and resistance to removal can be related to the characteristics of the communication system, i.e. capacity, signal to noise ratio (SNR) and jamming margin. *Capacity* in data hiding represents the maximum number of bits hidden and successfully recovered by the watermarking system. The *SNR* provides a measure of invisibility or detectability. In this paper the message is a *randomly generated gaussian vector* and represents the noise, which is part of every natural digital image or communication system. *Cover image* is the actual information. In compliance with communication theory, where a high SNR is desired, a very high SNR corresponds to lower perceptibility, and therefore greater success is achieved when concealing the embedded signal. *Jamming* resistance is the

This work was supported by the State Scholarships Foundation of Greece and the General Secretariat for Research and Technology (Grant 97YP149).

robustness of the system in resisting to any kind of intentional or accidental attack.

In this work we compare SNR and robustness of DLT-domain watermarking with that of the DCT. In Section 2 the different watermarking approaches are reported, while in Section 3 the DLT is briefly presented. The transform domain watermarking is described in Section 4, and in Section 5 evaluation results are given.

2. WATERMARKING APPROACHES

There is a vast majority of image watermarking approaches. One method of data hiding exploits the least significant bit (LSB) plane, with direct replacement between cover image's LSB and message (watermark) bits by adopting different logical or arithmetic combinations. LSB manipulation programs for a variety of image formats can be found. LSB methods achieve both high payload (high information rate) and low perceptibility. However, because information is hidden in LSB, it is fragile to any data processing, which results in loss of information from these LSB bits [3].

Approaches of perceptual masking to exploit characteristics of human visual system (HVS) for data hiding have been also utilized [4]. Perceptual masking means, information in certain regions of an image is occluded by perceptually more prominent information from the other parts of the image. Masking can be performed either in frequency or spatial domain.

Most of recent research is mostly based on frequency domain techniques for still images [5-14]. In particular Cox et al. described a method where the watermark is embedded in large DCT coefficients using an idea borrowed from spread spectrum in communications theory [11].

Zhu et al. [12] applied the same technique of spread spectrum for a unified approach for digital watermarking of images and video based on two and three dimensional discrete wavelet transform (DWT). The hierarchical nature of wavelet representation was adopted for the detection purpose. Watermark was added to all the high pass bands in the wavelet domain, using a nonlinear insertion procedure.

Xia et al. [13] also use a multiresolution watermarking method using the DWT. Gaussian random noise is added to the largest coefficients of all subbands except in the lowest frequency subband. They also used a masking formula in order to suppress the artifacts generated by the high energy of the embedding watermark.

3. THE DISCRETE LAGUERRE TRANSFORM

Mandyam and Ahmed introduced the DLT in 1996 [15]. It is based on the Laguerre functions, which constitute an orthonormal set of functions in the (0, ∞) interval. The n^{th} Laguerre function (starting from n = 0) is defined as

$$l_n(p,x) = (-1)^n \sqrt{2p}\,\phi_n(2px) \qquad (1)$$

where $\phi_n(x) = e^{-x/2} L_n(x)$, $L_n(x) = \frac{e^x}{n!}\frac{d^n}{dx^n}(x^n e^{-x})$ and p is a nonzero constant. Due to exponential term e^{-px}, the Laguerre functions are not polynomials. By some minor modifications to the Gauss-Jacobi orthogonalisation procedure one gets the desired DLT transform matrix. As an example, the 4x4 DLT transform matrix (quantised to four digits) is

$$L_{4x4=}\begin{bmatrix} 0.7766 & 0.5978 & 0.1972 & 0.0232 \\ -0.5261 & 0.4458 & 0.6974 & 0.1950 \\ 0.3160 & -0.5785 & 0.4372 & 0.6118 \\ -0.1420 & 0.3303 & -0.5325 & 0.7663 \end{bmatrix} \qquad (2)$$

A drawback of the DLT is the increase in the computational burden as the order of the DLT increases, due to the difficulty in finding the roots of the corresponding high-order Laguerre polynomial. There are two remarkable points about the DLT: (a) Referring to eq. (1), one can see that the Laguerre basis polynomials are all subject to an exponential decay, and therefore, for x sufficiently large, $l_n(x)$ approaches zero for all possible n. One can therefore conclude that signals that can be best represented by DLT are those that have some sort of exponential decay. (b) It can be observed that the DLT has no "DC basis vector," as is the case with the DCT and DFT. As such, signals with a DC offset are not suitable for efficient representation by the DLT.

4. DLT DOMAIN WATERMARKING

The process for the transform domain embedding and detecting the watermark is depicted in Fig. 1. This scheme is general and can be applied for any escrow transform domain watermarking approach. The original image, which is assumed to be continuous-tone grey scale of 2^P pixel accuracy, is first DC shifted by subtracting the value 2^{P-1} from each pixel value. Thus, all pixel values are shifted from unsigned integers in the range of $[0, 2^P-1]$ to signed integers in the range of $[-2^{P-1}, 2^{P-1}-1]$. Then, the discrete transform is applied to the image as a whole, and the N largest coefficients are selected for watermark embedding. Each of the selected coefficients X_k is modified (watermarked) according to the formula [4,5,11]

$$X_k^* = X_k + a w_k |X_k|, \quad k=1,2,\ldots,N \qquad (3)$$

where X_k^* is the watermarked coefficient, a the watermark strength and w_k the k^{th} element of a pseudo-random discrete Gaussian signal w with zero mean and unit variance. Applying the inverse transform and inverse DC shifting the final watermarked image is produced, as shown in Fig. 1a.

For the detection of the watermark, the original image and the watermarking sequence w are needed. The whole process is illustrated in Fig. 1b. Both the original and the watermarked images are DC shifted and forward transformed. Then, the N largest coefficients for the original image are selected. Each of these coefficients X_k is subtracted from the corresponding

watermarked coefficient X_k^* and a new sequence is generated according to the formula

$$w_k^* = \frac{X_k^* - X_k}{a|X_k|} \quad , \qquad k=1,2,\ldots,N \qquad (4)$$

The produced sequence w^* is cross-correlated with the watermark sequence w. If a peak occurs at the center of the correlation result, then we can say that the watermark w has been detected, i.e. the sequences w^* and w are similar. The higher the peak is, the greater is the similarity.

5. EVALUATION RESULTS

The watermarking process described in section 4 has been implemented and evaluation results are reported in the present section for different images and different attacks. The test images are grey scale of size 256x256 with pixel accuracy of 8 bits, i.e. P=8. The number of coefficients selected for watermarking is N=500. The watermarking strength a has been set equal to 0.08. For comparison purposes we conducted the same simulations for the DLT and the DCT. In other words, we implemented the processes of Fig. 1 for the DLT and the DCT, using the same values for a and N.

In Fig. 2 the original *peppers* image (of size 256x256) is shown, and in Figures 3 and 4 the corresponding watermarked images by means of the DLT and the DCT are illustrated. It is seen that subjectively and objectively the images watermarked in the DLT-domain are better than those watermarked in the DCT-domain (PSNR difference of approximately 3 dB). The detection (extraction) of the watermark is achieved by calculating the cross-correlation peak, as shown in Fig. 5. In order to test the robustness of the DLT and DCT watermarking techniques, we performed various attacks on the watermarked images, as for example addition of Gaussian and uniform noise, median filtering, downscaling and compression. It was seen that the DLT-based watermarking approach is more robust than the DCT-based one, in the case of noise addition. It is, however, less robust to downscaling, (images were downscaled by 2 in each direction and then up-scaled by interpolation to the original size). Both watermarking approaches were of the same robustness in the case of JPEG compression.

6. CONCLUSIONS

A DLT-domain watermarking technique has been presented in this communication. Comparisons between the DLT- and the DCT-based watermarking have shown that the achieved image quality is better in the case of the DLT watermarking. This technique is also more robust than the DCT-based, in the case of attacking images by additive noise. In most of the other attacks, both behave almost the same, except for the downscaling case, where the DLT-based is inferior to the DCT-based watermarking.

ACKNOWLEDGEMENTS

The authors would like to express their sincere thanks to Dr. Nasir Ahmed and Dr. Giridhar Mandyam for providing the DLT matrices.

REFERENCES

[1] S. Katzenbeisser and F.A.P. Petitcolas (eds): "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House Books, Dec. 1999.

[2] F.A.P.Petitcolas, R.J.Anderson and M.G.Kuhn: "Information Hiding – A Survey," Proc. of the IEEE, Vol. 87, No. 7, pp.1062-1078, July 1999.

[3] N. Nikolaidis and I. Pitas, "Robust Image Watermarking in the Spatial Domain," Signal Processing, Vol. 66, No. 3, pp. 385-403, May 1998.

[4] R.B. Wolfgang, C.I. Podilchuk and E.J. Delp: "Perceptual Watermarks for Digital Images and Video", Proc. of the IEEE, Vol. 87, No. 7, pp.1108-1126, July 1999

[5] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT Domain System for Robust Image Watermarking," Signal Processing, Vol. 66, No. 3, pp. 357-372, May 1998.

[6] D. Kunder and D. Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition," Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP), Vol. 5, pp. 2969-2972, Seattle, WA, 1998.

[7] G. Nicchiotti and E. Ottaviano, "Non-Invertible Statistical Wavelet Watermarking," Proc. 9th Europ. Signal Processing Conf. (EUSIPCO' 98), pp. 2289-2292, Rhodos, Greece, Sept. 8-11, 1998.

[8] M.L. Mora and J.M. Martinez: " Orthogonal Watermarks for Digital Images", Proc. Of the IASTED Int. Conf. Signal and Image Processing (SIP'98), pp. 469-472, Las Vegas, Nevada, USA, Oct. 28-31, 1998.

[9] G.C.M. Silvestre and W.J. Dowling: "A Data-Embedding Technique for Digital Images", Proc. IEE Colloquium on Secure Images and Image Authentication, Savoy Place, London, April 10, 2000.

[10] P. Loo and N. Kingsbury: "Digital Watermarking with Complex Wavelets", Proc. IEE Colloquium on Secure Images and Image Authentication, Savoy Place, London, April 10, 2000.

[11] I.J. Cox and J. Kilian and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. Image Processing, Vol. 6, No. 12, pp. 1673-1687, 1997.

[12] W. Zhu, et al. “Multiresolution Watermarking for Images and Video,” IEEE Trans. on Circuits and Systems for Video Technology, Vol. 9. No. 4, June 1999.

[13] X-G Xia, C.G.Boncelet, and G. R. Arce, “Wavelet Transform Based Watermark for Digital Images,” Optics Express, Vol. 3, No. 12, Dec. 1998.

[14] L. M. Marvel, C. G. Boncelet and C. T. Retter, “Spread Spectrum Image Steganography,” IEEE Trans. Image Processing, Vol. 8, No. 8, Aug. 1999.

[15] G. Mandyam and N. Ahmed, “The Discrete Laguerre Transform: Derivation and Applications,” IEEE Trans. Signal Processing, Vol. 44, No. 12, pp. 2925-2931, Dec. 1996

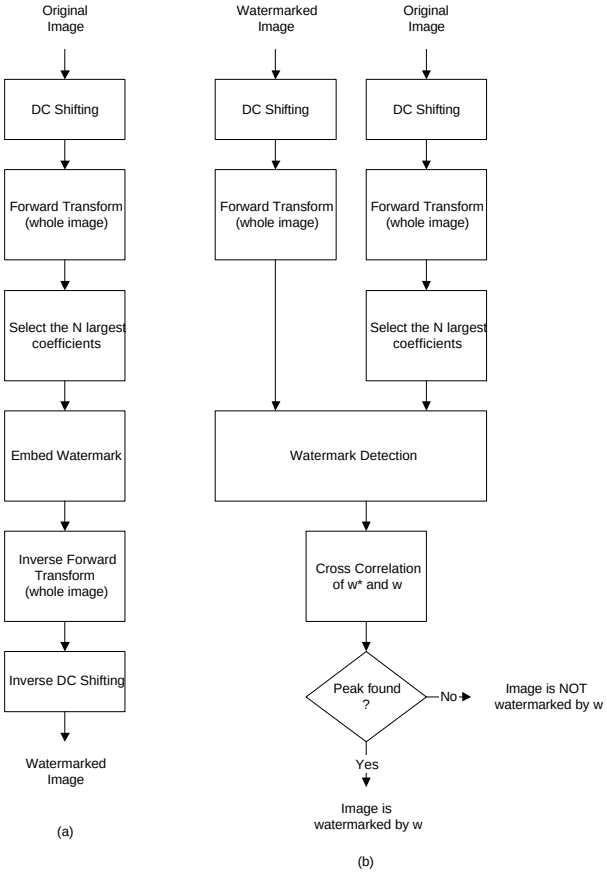

Figure 1. Transform domain watermarking: (a) watermark embedding, (b) watermark detection.

Figure 2. Original grey scale image of size 256x256

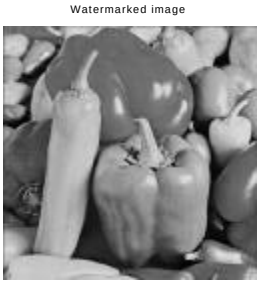

Figure 3. DLT watermarked image (PSNR 40.55dB).

Figure 4. DCT watermarked image (PSNR 36.26dB).

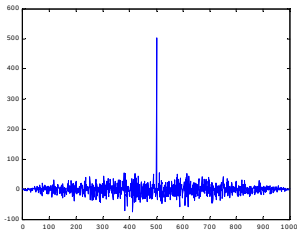

Figure 5. A high cross-correlation peak denotes that the watermark is present.