CIRCULARLY SYMMETRIC WATERMARK EMBEDDING IN 2-D DFT DOMAIN

V. Solachidis and I.Pitas

Department of Informatics
University of Thessaloniki
Thessaloniki 54006, Greece
Tel,Fax: +3031-996304
e-mail: pitas@zeus.csd.auth.gr

ABSTRACT

This paper presents an algorithm for rotation and scale invariant watermarking of digital images. An invisible mark is embedded in magnitude of the DFT domain. It is robust to compression, filtering, cropping, translation and rotation. The watermark introduces image changes that are invisible to the human eye. The detection algorithm does not require the original image.

1. INTRODUCTION

Digital products can be easily copied and reproduced in a network enviroment. Therefore the watermarking of the multimedia products has been essential for copyright protection. A digital watermark is a digital signal carrying information about the copyright owner and it is expected to be permanently embedded into the digital products. In the following, we shall limit our presentation to digital image protection.

The watermark should be robust to distortions (such as image processing and lossy image compression) and statistically undetectable. In order to be robust, it must be associated to the most significant components of the image that do not change with image distortions.

Watermark invisibility preserves image data quality. Furtheremore, if the watermark is visible, then its illegal removal could be very easy in the digital domain. The watermark should also be statistically undetectable, otherwise the watermark can be localized or destroyed.

Robustness against image processing is also required. Image processing does not modify only the image but also may modify the watermark. A pirate may try through image processing manipulations to render the watermark undetectable.

Several watermarking methods have been proposed in the literature. In some of them the watermark is embedded in the spatial domain [1] [2] [3] whereas in others it is embedded in the DCT [4] [5] [6] [7][8] [9] or DFT domain [10], [11].

In the proposed algorithm the watermark is embedded in DFT domain. The original image is not required in the watermark detection procedure.

2. WATERMARK EMBEDDING

Let I be a grayscale $N \times N$ original image. The Fourier transform of I is:

$$I(k_1,k_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} i(n_1,n_2) e^{-j2\pi n_1 k_1/N_1 - j2\pi n_2 k_2/N_2} \tag{1}$$

Let $M(k_1,k_2) = |I(k_1,k_2)|$ be the magnitude and $P(k_1,k_2)$ be the phase of the Fourier transform of I. Let also $W(k_1,k_2)$ be the watermark, $M^{'}(k_1,k_2)$ the modified magnitude and $I^{'}(k_1,k_2)$ the watermarked image.

The watermark is embedded in the DFT domain and consists of a 2-D circularly cymmetric sequence taking values 1 or -1. It has zero mean value.

The watermark should affect neither the low frequencies of the transform (in order to be invisible) nor the high frequencies (in order to be robust against compression) [5]. By assuming that the zero frequency term $I(0,0)$ is in the center of the transform domain, the region in which the watermark is embedded should be a ring covering the middle frequencies. Thus,

$$W(r,\theta) = \begin{cases} 0, & \text{if } r < R_1 \text{ and } r > R_2 \\ \pm 1, & \text{if } R_1 < r < R_2 \end{cases} \tag{2}$$

where $r = \sqrt{k_1^2 + k_2^2}$, $\theta = \arctan(\frac{k_2}{k_1})$

The ring is separated in S sectors and in homocentric circles of radius $r \in [R_1, R_2]$ We assign the same value 1 or -1 in each watermark circlular sector.

Then the coefficients of the watermarked magnitude $M^{'}$ are:

$$M^{'}(k_1,k_2) = M(k_1,k_2) + aW(k_1,k_2) \tag{3}$$

a is a factor which determines the strength of the watermark. Such an embedding is shown in Figure 1 for the 512×512 image LENNA. We used a large factor a for illustative purposes. If the magnitude becomes negative, it is rounded to 0. Watermark embedding can become image-dependent by using an embedding function $af(M(k_1, k_2), W(k_1, k_2))$ instead of simple addition in (3).

The DFT of a real 2-D signal has certain conjugate symmetry properties. The addition of a watermark to the magnitude of the DFT of the image does not ensure that the inverse DFT will produce a real image. To ensure that the IDFT is real, the watermark must possess the following summetry [10]:

$$W_{k,l} = W_{N-k,N-l}, \quad \forall k,l \in [1, N] \tag{4}$$

The watermarked image is given by the inverse DFT:

$$i' = IDFT(I^{'}), \quad I^{'} = (M^{'}, P) \tag{5}$$

The watermark can also be casted in the spatial domain as follows:

$$W^{'} = IDFT(W, P), i^{'} = i + W^{'} \tag{6}$$

In order to increase watermark invisibility local image masking can be used.

3. WATERMARK DETECTION

Let $I^{'}$ be the DFT of a possibly watermarked image and $M^{'}$ its magnitude. The correlation c between the possibly watermarked coefficients $M^{'}$ and the watermark W can be used to detect the presence of the watermark:

$$c = \sum_{i=1}^{N} \sum_{j=1}^{N} W(k_1, k_2) M^{'}(k_1, k_2) \tag{7}$$

If the image $I^{'}$ is watermarked with $W_j^{'}$. $W \neq W_j^{'}$, then the correlation c is given by:

$$c = \sum_{i=1}^{N} \sum_{j=1}^{N} (W(k_1, k_2) M(k_1, k_2) + aW(k_1, k_2) W^{'}(k_1, k_2)) \tag{8}$$

If the image $I^{'}$ is watermarked with W the correlation c is:

$$c = \sum_{i=1}^{N} \sum_{j=1}^{N} (W(k_1, k_2) M(k_1, k_2) + aW^2(k_1, k_2)) \tag{9}$$

Assuming that W, M, are independent and identically distributed random variables and W has zero mean value, the mean value of c is:

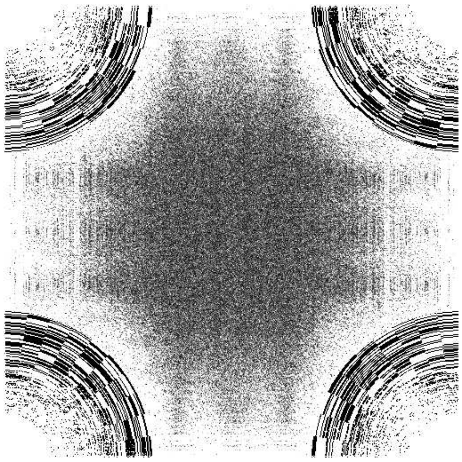

Figure 1: Watermarked DFT magnitude of image LENNA 512×512

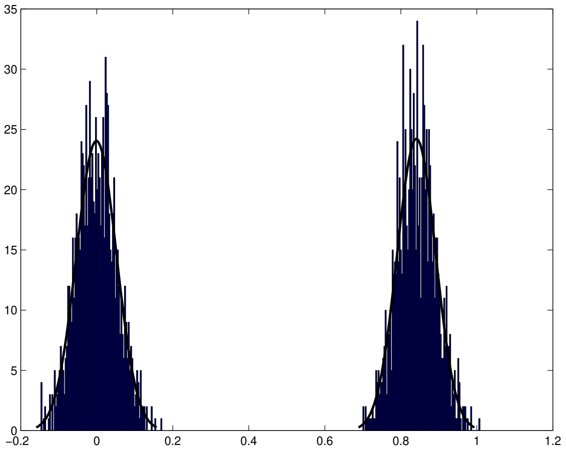

Figure 2: Distribution

$$\mu_c = \begin{cases} \pi(R_2^2 - R_1^2)a & \text{if } W = W^{'} \\ 0 & \text{if } W \neq W^{'} \\ 0 & \text{if no watermark is present} \end{cases} \tag{10}$$

The value of the correlator can also be expressed as $c^{'} = c/\mu_c$. The sample mean value of the normalized correlator $c^{'}$ should be 1 for every watermarked image.The empirical pdf of $c^{'}$ that has been obtained by watermarking the 512×512 'LENNA' with 1000 different watermarks is shown in Figure 2.

The detection could be of the form:
H_0: $I^{'}$ is watermarked by $W^{'}$ if $c \geq T$
H_1: $I^{'}$ is not watermarked by $W^{'}$ if $c < T$

Considering that T is the threshold, two probabilities must be estimated. First, the false alarm probability which is the probability to detect a watermark in an unmarked image. False rejection probability is the probability of not detecting the watermark in a marked image. Since the empirical pdf of c' can be approximated by a normal distribution false alarm and false rejection can be computed using the error function $erf(x)$:

$$P_F = 1 - \frac{1}{2}erf(\frac{T}{\sqrt{2\sigma_c^2}}). \qquad (11)$$

Our method is simpler than that reported in [11], because we do not employ Fourier-Melin transform.

4. ROBUSTNESS TO GEOMETRICAL TRANSFORMATIONS

The proposed method is robust to translations, since they do not affect the DFT magnitude. Rotation in the spatial domain causes rotation of the Fourier domain by the same angle. [11]. Since the watermark consists of S sectors having identical values, this construction of the watermark allows its detection even after a rotation in the range $[-\frac{\pi}{S}, \frac{\pi}{S}]$of the watermarked image. The maximum angle of rotation depends on the size (or the number) of the sectors. If a search of optimal rotation is performed that maximizes c', the detection algorithm can be robust to any rotation angle. Rotation, translation invariance is very useful because the copies from printing, scanning or xeroxing maybe rotated or translated in comparison with the initial image. From geometrical transformation point of view, rotation around an arbitrary center is equivalent with rotation around the center of the image and translation. Thus, out method is robust to rotation around an arbitrary center.

Scaling in the spatial domain causes inverse scaling in the frequency domain (if $f(x_1, x_2) \overset{DFT}{\rightarrow} F(k_1, k_2)$ then $f(ax_1, ax_2) \overset{DFT}{\rightarrow} \frac{1}{a}F(\frac{k_1}{a}, \frac{k_2}{a})$)[11]. Thus, if $N \times M$ is the size of the initial image and $[R_1, R_2]$ is the size of the watermark ring (in the frequency domain), the size of the scaled image is $aN \times aM (a > 0)$ and the size of the watermark of the scaled image in the frequency domain remains unaltered. Thus, the mean value of the correlation c of the watermark and the ring of any scaled image whose dimensions are R_1 and R_2 is $\pi(R_2^2 - R_1^2)a$. Furthermore, normalized correlation output does not depend on a.

Cropping changes the frequency sampling step. If the size of the initial image is known then the correlation can be done between the cropped image (in the frequency domain) and the watermark, which should be changed to the same frequency sampling step of the cropped image. If the size of the initial image is not known then the correlation should be done for many frequency sampling steps by searching the maximal detector output. Let I' be an $M' \times N'$ image which is possible scaled and cropped. The detection algorithm is applied to the watermark and to a ring of the

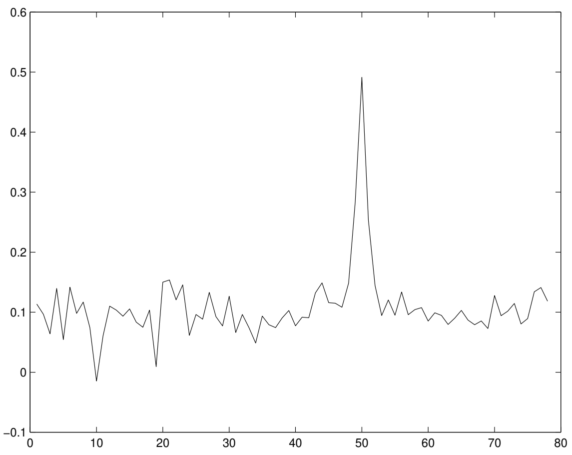

Figure 3: Correlator for several frequencies sampling steps

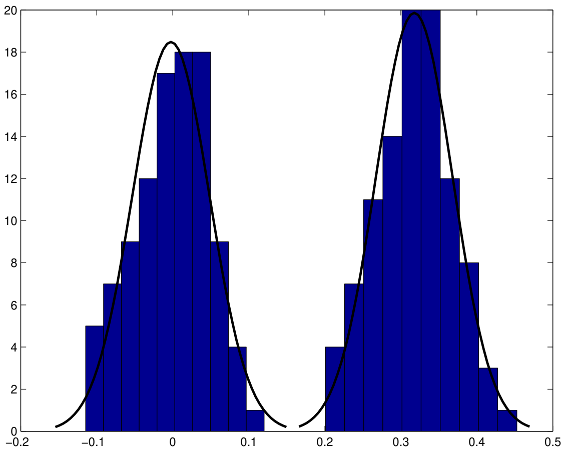

Figure 4: Pdf of one dimension cropping and scaling

frequency domain of I' whose size is bR_1 (inside radius) and bR_2 (outside radius) for every b $(0 < b < 1)$. The normilized correlation c' is shown (in Figure 3) for several frequencies sampling steps. We get a maximum c' for $b = 50 = \frac{400}{512}64$ (where $R_1 = 64$ in this experiment on the 512×512 LENNA) that manifests the existance of the watermark. The initial image was cropped from 512×512 to 400×400 and scaled to 512×512.

The proposed method is also robust to anisotropic cropping and scaling distortions. The pdf of c' of 100 non-watermark images (left) and 100 watermarked (right) is shown in Figure 4. The size of the initial image is 512×512. The detection was performed after cropping to 512×505 and scaling to 512×512. If we use threshold $T = 0.18$ the method is robust to such attacks.

5. NUMBER OF WATERMARKS

The length (number of samples) of the 2-D watermark sequence W is:

$$L = (R_2 - R_1)\frac{S}{2}$$

where $R_2 - R_1$ is the number of the homocentric circles of the ring, S is the number of the sectors. This product is divided by 2 because the watermark preserves positive summetry. In our experiments for 512×512 images, the length L of the watermark sequence is $L = 2304$.
The number of the L-length sequences is 2^L and the number of L-length sequences with mean value 0 is

$$\binom{L}{L/2}$$

The number of the watermarks for L=2304 is

$$\binom{2304}{1152} = 10^{691.7938} = 6.22 \;\; 10^{691}$$

For every watermark there are some other similar watermarks that can produce positive detector output. In order to avoid this problem, a set of watermark sequences should be constructed such that their correlation is small. In this set of vectors w_i for every pair of W_k, W_j, should be $< W_k, W_j > \leq a$, where $a < L$ (L is vector dimension (length of the sequence)). We have devised an algorithm for creating such watermark vectors.

6. SIMULATION RESULTS AND CONCLUSIONS

We have tested our algorithm on a number of digital images. It's overall performance was very good. We present here it's use on image LENNA 512×512. The parameters which have been used in this experiment are: N=512, a=0.3, $R_1 = 51$, $R_2 = 166$, $S = 40$, $R = 11$, $T_2 = 0.0002$. If we set the threshold $T = 0.18$ then the false alarm is $1.8663 \;\; 10^{-6}$ and the false rejection is: $9.8916 \;\; 10^{-5}$ (Figure 3). The PSNR of the watermarked image (Lenna) is about 42. In all these experiments, the watermark is robust in JPEG compression up to 1:25, scaling, cropping, rotation (up to 3 degress), histogram equalization, Gausian noise, median 3×3 and moving average 3×3 filtering. It is also robust to StirMark. Furthermore, it is robust to rotation at any angle and to combined cropping/scaling if search maximizing correlation c' is used. We cannot present experimental pdfs of c' for all these cases due to lack of space. We have used the same threshold $T = 0.18$ for all rpeviously mentioned processing attacks.

7. REFERENCES

[1] Martin Kutter, Frederic Jordan, and Frank Bossen. Digital watermarking of color images using amplitude modulation. *Journal of Electronic Imaging*, 7(2):326–332, 1998.

[2] G. Voyatzis and I. Pitas. Embedding robust watermarks by chaotic mixing. In *Proceedings of 13th International Conference on Digital Signal Processing*, volume 1, pages 213–216, Santorini, Greece, July 2-4 1997.

[3] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. *Signal Processing, sp.issue on Copyright Protection and Access control*, to appear in 1998.

[4] M. D. Swanson, B. Zhu, and A. H. Tewfik. Transparent robust image watermarking. In *Proceedings of ICIP'96*, volume III, pages 211–214, Lausanne, Switzerland, September 1996.

[5] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 12 1997.

[6] A. G. Bors and I. Pitas. Image watermarking using dct domain constraints. In *Proceedings of ICIP'96*, volume III, pages 231–234, Lausanne, Switzerland, September 1996.

[7] A. Piva, M.Barni, and F. Bartolini. Dct-based watermark recovering without resorting to the uncorrupted original image. In *Proceedings of ICIP'97*, volume I, pages 520–523, Atlanta, USA, October 1997.

[8] M.Barni, F.Bartolini, V.Cappelini, and A.Piva. A blind dct-domain system for robust image watermarking. *to appear in IEEE Journal of Selected Areas of Communications*.

[9] C. T. Hsu and J.L. Wu. Hidden signatures in images. In *Proceedings of ICIP'96*, volume III, pages 223–226, Lausanne, Switzerland, September 1996.

[10] J. Ó Ruanaidh, W. J. Dowling, and F. M. Boland. Phase watermarking of digital images. In *Proceedings of ICIP'96*, volume III, pages 239–242, Lausanne, Switzerland, September 1996.

[11] J. Ó Ruanaidh and T. Pun. Rotation, scale and translation invariant digital image watermarking. In *Proceedings of ICIP'97*, volume I, pages 536–539, Atlanta, USA, October 1997.