Self-similar ring shaped watermark embedding in 2-D DFT domain

V. Solachidis and I.Pitas
Department of Informatics, Aristotle University of Thessaloniki,
Box 451, Thessaloniki 540 06, GREECE
Tel,Fax: +3031-996304
e-mail: [vasilis, pitas]@zeus.csd.auth.gr

ABSTRACT

A new watermarking algorithm for still images is presented in this paper. The watermark is embedded in magnitude of the DFT domain and introduces image changes that are invisible to the human eye. It is robust to compression, filtering, cropping, translation, rotation and scaling. The detection algorithm does not require the original image. The watermark has a self-similar structure that accelerates the detection procedure.

1 INTRODUCTION

Digital products can be easily copied and reproduced in a network environment. Therefore copyright protection of multimedia products using watermarking techniques has emerged as an important research topic. 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 copyright protection.

The watermark should be robust to image processing operations and lossy image compression. Furthermore it should be able to withstand intentional attacks that aim to render the watermark undetectable. It must be associated to the most significant components of the image that do not change with image distortions in order to be robust.

Watermark invisibility is necessary to guarantee preservation of image data quality. Furthermore, 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 and destroyed.

Several still image watermarking methods have been proposed in the literature. The watermark is embedded in the spatial domain [1] - [3], the DCT domain [4] -[8] or the DFT domain [9], [10]. In the proposed algorithm the watermark is embedded in DFT domain. The original image is not required in the watermark detection procedure. This method is an extension of [11]. The watermark selfsimilarity accelerates its detection in a geometrically transformed image.

2 Watermark embedding

Let $I(n_1, n_2)$ be a grayscale $N \times N$ image. The Fourier transform of I is:

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

Let $M(k_1, k_2) = |I(k_1, k_2)|$ be the magnitude and $P(k_1, k_2)$ the phase of the Fourier transform of $I(n_1, n_2)$. Let also $W(k_1, k_2)$ be the watermark, $M'(k_1, k_2)$ the modified Fourier magnitude and $I'(k_1, k_2)$ the Fourier transform of the watermarked image.

The watermark is embedded in the DFT domain and consists of a 2-D ring shaped chaotic 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 located at the center of the transform domain, the region in which the watermark is embedded should be a ring covering the middle frequencies. Thus, the watermark signal can be expressed in a polar coordinate system in the following way:

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

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

The ring consists of several sub-rings. Each sub-ring is a scaled version (by a factor of 2) of its inward neighbor sub-ring. Thus, the thickness of its ring is twice the thickness of each inward neighbor. Also, the rings are separated in S identical sectors. Such a watermark can be seen in Figure 1. The pattern of image Lenna was used in this case, instead of a random signal, in order to exemplify the self-similar structure of the watermark.

The Fourier magnitude $M^{'}$ of the watermarked image is given by:

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

where a is a factor which determines the strength of the watermark. If the magnitude becomes negative,

Figure 1: Example of a self-similar watermark

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 DFT magnitude 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 symmetry [9]:

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

The watermarked image $I'(n_1,n_2)$ is given by the inverse DFT:

$$I'(n_1,n_2) = IDFT(I'(k_1,k_2)) \tag{5}$$

$$I'(k_1,k_2) = M'(k_1,k_2)e^{P(k_1,k_2)} \tag{6}$$

The above procedure is equivalent to spatial domain embedding using the following embedding function:

$$I'(n_1,n_2) = I(n_1,n_2) + W(n_1,n_2) \tag{7}$$

$$W(n_1,n_2) = IDFT(W(k_1,k_2),P(k_1,k_2)) \tag{8}$$

In order to increase watermark invisibility distortion masking utilizing the local image properties can be used [12].

3 Watermark detection

Let $I'(k_1,k_2)$ be the DFT of a possibly watermarked image and $M'(k_1,k_2)$ its magnitude. The correlation c between $M^{'}$ and the watermark W can be used to detect the presence of the watermark:

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

If the image I is watermarked with W', $W \neq W'$, then the correlation c is given by:

$$c = \sum_{i=1}^{N}\sum_{j=1}^{N}(W(k_1,k_2)M(k_1,k_2) + aW(k_1,k_2)W^{'}(k_1,k_2)) \tag{10}$$

If the image I is watermarked with W the correlation c is:

$$c = \sum_{i=1}^{N}\sum_{j=1}^{N}(W(k_1,k_2)M(k_1,k_2) + aW^2(k_1,k_2)) \tag{11}$$

Assuming that $W(k_1,k_2), M(k_1,k_2)$, are independent and identically distributed random variables and W has zero mean value, the mean value of c is:

$$\mu_c = \begin{cases} \pi(R_2^2 - R_1^2)a & \text{if } W = W^{'} \\ 0 & \text{if } W \neq W^{'} \\ 0 & \text{if no watermark is present} \end{cases} \tag{12}$$

The normalized correlator output $c^{'} = c/\mu_c$ is used for watermark detection. The mean value of the normalized correlator $c^{'}$ should be 0 for images that are not watermarked or watermarked with another watermark (W') and 1 for watermarked images (with the right watermark).

The detection rule could be of the form:
$I^{'}$ is watermarked by W if $c \geq T$
$I^{'}$ is not watermarked by W if $c < T$
where T is an appropriately selected threshold. Two probabilities must be estimated: the false alarm probability which is the probability to detect a watermark in an unmarked image or in an image that is marked with a different watermark and the false rejection probability which 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 can be computed using the error function $erf(x)$.

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 on the Fourier domain by the same angle [10]. Since the watermark consists of S sectors having identical values, watermark detection is possible even after a rotation $\frac{2k\pi}{S}$ degrees of the watermarked image, where $k = 0,1,...,S-1$. Thus, a search for the angles $0,1,2,...,\frac{2k\pi}{S} - 1$ suffices to perform detection for every rotation angle. Rotation and translation invariance is a very useful property because printed, scanned or xeroxed copies of an image might be rotated or translated in comparison with the initial image. Our method is also robust to rotation around an arbitrary center, since rotation around an arbitrary

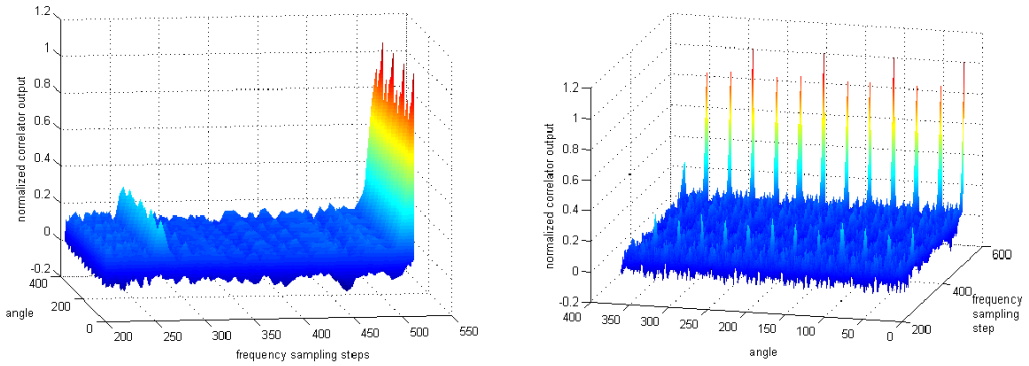


Figure 2: Normalized correlator output for several frequency sampling steps and rotation angles (two different view angles)

Table 1: Detection percentage for median and moving average filtering

	Window size	*Threshold 0.1*		*Threshold 0.15*		*Threshold 0.2*	
		SNR 35 db	SNR 30 db	SNR 35 db	SNR 30 db	SNR 35 db	SNR 30 db
Moving Average	3×3	99.6	100	98.8	100	96.6	100
	5×5	98.4	100	95.6	100	91.2	100
Median	3×3	99.6	100	98.6	100	95.8	100
	5×5	97.6	100	94.2	100	86.8	100

center is equivalent with rotation around the center of the image and translation.

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 $f(sx_1, sx_2) \overset{DFT}{\rightarrow} \frac{1}{s}F(\frac{k_1}{s}, \frac{k_2}{s})$)[10]. Thus, if $N \times N$ 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 $sN \times sN (s > 0)$ and the size of the watermark of the scaled image in the frequency domain remains unaltered. Furthermore, normalized correlation output does not depend on s.

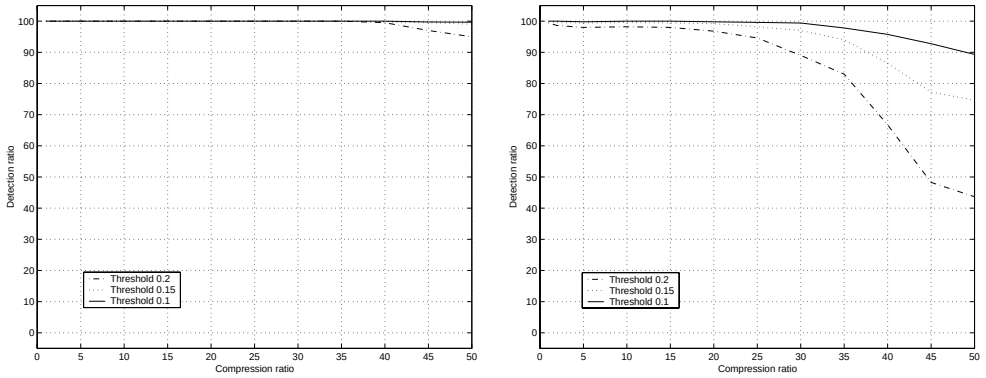
Cropping changes the frequency sampling step. If the size of the initial image is known, the correlation can be performed between the cropped image (in the frequency domain) and the watermark, which should be adapted to the frequency sampling step of the cropped image. If the size of the initial image is not known then the correlation should be performed for many frequency sampling steps.

The method is also robust to combined cropping and scaling. Let $I^{'}$ be an $M^{'} \times N^{'}$ image which is possibly scaled and cropped. The detection algorithm is applied using a watermark to a ring of the frequency domain of $I^{'}$ whose size is bR_1 (inner radius) and bR_2 (outer radius) for every b $(0 < b < 1)$. For example, if the size of the original image is 512×512 and the size of the cropped watermarked image is 400×400 then we get a maximum $c^{'}$ for $b = 0.78125 = \frac{400}{512}$ that manifests the existence of the watermark. However the watermark is self-similar, thus we have to search only for $0.5 < b < 1$. Therefore, the number of the different frequency sampling steps where the search should be performed is halved (in out case reduced from 512 to 256). In Figure 2 the normalized correlator output for several frequency sampling steps and rotation angles for a watermarked image that has not been distorted is depicted. The multiple peaks due to the self-similarity of the watermark can be clearly seen.

5 Simulation results and conclusions

We have tested our algorithm on a number of digital images using several different keys. Its overall performance was very good. We present the percentage of the correlator values that is above the selected threshold. Three thresholds have been chosen, $T = 0.1$, $T = 0.15$ and $T = 0.2$. The probability of false alarm for these thresholds is $4 \cdot 10^{-2}$,$4 \cdot 10^{-3}$ and $2 \cdot 10^{-4}$ respectively. Having set the threshold T, the performance criterion used for comparing the performance of the algorithms under image processing operations was the detection ratio defined as : $P = \frac{N_{detect}}{N_{total}}$ where N_{detect} is the number of the correctly detected watermarks in N_{total} experiments. By fixing the strength parameter a, watermarked images distorted to 30 and 35 db SNR were generated.

The experiments prove that the watermark is ro-



SNR 30 db SNR 35 db

Figure 3: Detection percentage for several JPEG compressions

bust to JPEG compression, scaling, cropping, rotation, histogram equalization, Gausian noise, median and moving average filtering. It is also robust to StirMark. Furthermore, it is robust to rotation at any angle and to combined cropping/scaling if the search procedure described in Section 4 is used.
The resistance of the watermark method to JPEG compression is depicted in Figure 3. The compression ratios are from 5 to 50 with step 5. The detection ratio for median and moving average filtering is shown in Table 1.

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*, 66(3):385–403, 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] 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.*

[8] 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.

[9] 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.

[10] 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.

[11] V. Solachidis and I.Pitas. Circularly symmetric watermark embedding in 2-d dft domain. In *Proceedings of ICASSP99*, volume 6, pages 3469–3472, Phoenix, Arizona, USA, March 15-19 1999.

[12] N. Nikolaidis and I.Pitas. Digital image watermarking: an overview. In *Proceedings of ICMCS99*, volume I, pages 1–6, Florence, Italy, June 7-11 1999.