WAVELET-BASED SELF-SIMILAR WATERMARKING FOR STILL IMAGES

S. Tsekeridou and I. Pitas

Dept. of Informatics, Aristotle University of Thessaloniki
Box 451, Thessaloniki 54006, Greece
e-mail: {sofia,pitas}@zeus.csd.auth.gr

ABSTRACT

This paper presents a wavelet-based watermarking method for copyright protection of still images. Watermarks are structured in such a way to attain spatial self-similarity with respect to a cartesian grid. Embedding and detection are performed in the wavelet domain allowing thus multiresolution detection. The novelty of the current approach is the use of self-similar watermarks (quasi scale-invariant), which are expected to be robust against geometric transformations, especially scaling. The approach proves rather efficient against many kinds of distortions, such as linear and nonlinear filtering, JPEG compression, scaling, cropping and rotation.

1. INTRODUCTION

Copyright protection of multimedia content is nowadays an all-increasing demand especially with the drastic expand of Internet and web-based services. To address this demand, watermarking methods have been developed. They are distinguished in two classes according to the domain where embedding is performed: the spatial-domain methods [1, 2] and the transform domain methods [3]-[9]. All methods aim at satisfying two basic requirements: watermark perceptual invisibility and watermark robustness against image modifications while preserving a desired image quality.

A wavelet domain watermarking method is proposed in this paper that exploits the spatial localization and frequency spreading of the wavelet transform to embed spatially self-similar watermarks to selected subbands of the transform, resulting in implicit visual masking and thus watermark perceptual invisibility. Due to the hierarchical structure of the transform, multiresolution embedding and detection is possible. No use of the original image is attempted during detection. Detection is performed by initially evaluating the normalized correlation between the watermarked image and the watermark and then thresholding it with a threshold derived under a desired false alarm probability constraint. Experimental results prove the efficiency of the current approach against various image distortions, such as filtering, compression, cropping, scaling and rotation. For the geometric distortions, search ranges have to be defined for detection but, as it will be shown, these are much limited due to the watermark structure.

The outline of the paper is the following. In section 2, we discuss the process of generating pseudorandom self-similar watermarks with zero mean value. Sections 3 and 4 present the embedding and detection methods in the wavelet domain. In section 5, simulation results are discussed and in section 6 conclusions are drawn and potential extensions of the method are presented.

This work has been funded by the LTR-ESPRIT European Project 31103 - INSPECT

2. WATERMARK GENERATION

A major drawback of many watermarking methods that have appeared to date is their sensitivity to geometric distortions inflicted on an image. Usually extensive search regions have to be defined thus increasing the computational complexity of the detection phase. Few attempts have been reported to deal with geometric transformations satisfactorily [3, 9]. Bearing this in mind, the concept of spatial self-similarity, that would ideally reduce search ranges in cases of cropping and scaling, has been incorporated in our watermark generation process. In more detail, the circularly-symmetric watermark presented in [3] is used as the so-called, from here on, mother signal, $W_M(r,\theta)$:

$$W_M(r,\theta) = \begin{cases} 0, & \text{if } r < r_{min} \text{ or } r > r_{max} \\ \pm\alpha, & \text{if } r_{min} < r < r_{max} \end{cases} \tag{1}$$

where $r = \sqrt{n_1^2 + n_2^2}$ with (n_1, n_2) representing the spatial coordinates and $\theta = \arctan(\frac{n_2}{n_1})$. r_{min} and r_{max} are the minimum and maximum radii that define the watermark's circular or ring-like support and α is an integer representing the embedding level. In order for $W_M(r,\theta)$ to attain sufficient lowpass characteristics and thus be more robust to compression or filtering, the mother signal's cyclic or ring-like spatial support is additionally divided to a total number of s sectors having an extend of $\frac{s}{360}^0$. All the pixels inside a sector for a constant radius are set equal to $-\alpha$ or $+\alpha$ according to a pseudorandom generator initialized with a prespecified key k. An example of the mother signal can be seen in Figure 2(a). Such a choice for W_M has been made in order to deal with rotation cases. Detection after rotation by angles smaller than $\frac{s}{360}^0$ is possible without rotating the watermark. When rotation angles are bigger, detection is performed faster since watermark rotation is only needed for multiples of $\frac{s}{360}^0$.

The next step is to incorporate spatial self-similarity with respect to the cartesian grid. This is accomplished in the way shown in Figure 1. $W_M(n_1, n_2)$ is scaled (using nearest neighbour interpolation) and shifted with respect to its center $r = 0$ 4 times, thus allowing possibility of watermark detection for scaling factors ranging from $\frac{1}{8} - 8$ as it will be explained later on. The final watermark $W(n_1, n_2)$ consists thus of 4 layers and it is evaluated by:

$$\begin{aligned} W(n_1,n_2) \quad = \quad & \sum_{f=0}^{3} \sum_{i=0}^{2^f-1} \sum_{j=0}^{2^f-1} W_M(2^f n_1 + i\lceil \frac{r_{max}}{2^f} \rceil, 2^f n_2 \\ & + j\lceil \frac{r_{max}}{2^f} \rceil) \end{aligned} \tag{2}$$

It is evident that the watermark dimensions are $2r_{max} \times 2r_{max}$ and are totally independent of the image size. The parameters that are necessary for the watermark generation and which present the final key for detection are: $\{k, \alpha, r_{min}, r_{max}, s\}$ Its center is used as a reference point in the detection phase. An example of the final watermark is given in Figure 2(b).

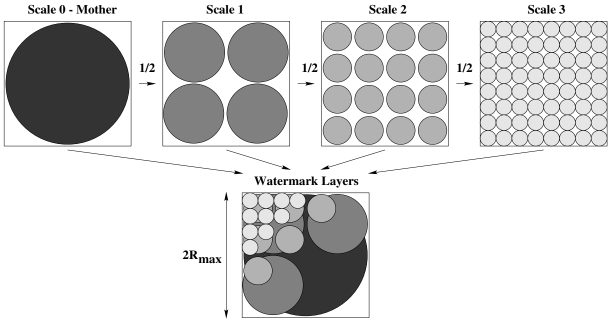
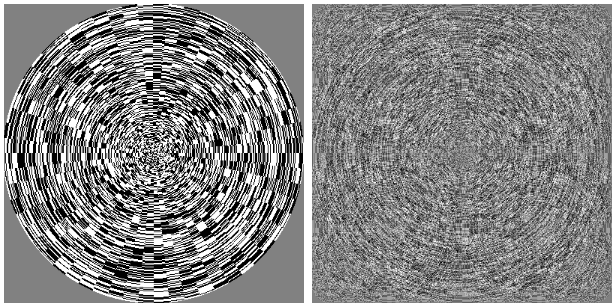


Figure 1: Illustration of the self-similarity in the watermark generation process.



(a) (b)

Figure 2: Example of (a) mother signal, (b) self-similar watermark.

3. WATERMARK EMBEDDING

Embedding is performed in the wavelet domain in an additive manner. The image is decomposed in 4 levels using the Haar wavelet basis. $W(n_1, n_2)$ is superimposed on the detail subbands of the highest and the second highest levels of the decomposed original image $I(n_1, n_2)$ as shown in Figure 3, i.e.:

$$I'_{f_l} = I_{f_l} \oplus W(2^{l-1}n_1, 2^{l-1}n_2), f \in \{LH, HL, HH\}, l \in \{1, 2\} \quad (3)$$

where $\oplus$ is a superposition operator. I_{f_l} and I'_{f_l} stand for the detail subband components of the original image and the watermarked image respectively, f for the subband index and l for the level index of the wavelet decomposition, where embedding is performed. It is noted that the watermark size must be smaller or equal to half of the size of the image to be watermarked. If it is smaller, it is added in the center of the detail subband component. Furthermore, in order to perform embedding in the second highest level of the wavelet decomposition, watermark scaling by 1/2 is initially performed using nearest neighbour interpolation. No embedding is performed to lower levels of the DWT, since they are considered unreliable especially when detection for wrong watermarks is to be tested. After watermark addition, inverse DWT is performed to obtain the watermarked image $I'(n_1, n_2)$. Due to the inherent spatial localization and frequency spread of DWT, implicit visual masking is accomplished leading to watermark perceptual invisibility. Embedding is additionally performed in the second highest level of the transform to ensure watermark detection after distortions such as filtering or compression which tend to remove high frequency components of the image (1st level of DWT). Multiplicative embedding might lead to better performance and it is to be experimented on in future.

4. WATERMARK DETECTION

Watermark detection is accomplished in a statistical way without the use of the original image. Initially, the watermarked image $I'(n_1, n_2)$ is DWT transformed and the correlations between the watermark (or scaled watermark) and the detail subband components of the 1st and 2nd levels are calculated, as shown in Figure 3. Thus, the following normalized correlation expressions are evaluated [4]:

$$\rho(l, f) = \frac{I'_{f_l}.W_{2^{l-1}}}{W_{2^{l-1}}.W_{2^{l-1}}}, \qquad l \in \{1, 2\}, f \in \{LH, HL, HH\} \quad (4)$$

for each frequency orientation f (subband component) and for each level l. . denotes inner product. It is $W_1(n_1, n_2) = W(n_1, n_2)$ and $W_2(n_1, n_2) = W(2n_1, 2n_2)$. Since I_{f_l} and W are statistically independent and uncorrelated, it is obvious that $\rho(l, f)$ will be equal to 1 under watermark presence and equal to 0 under watermark absence. In order to estimate the overall correlator response, average values along each frequency orientation f are initially estimated and then the maximum value of all frequency orientations f is estimated:

$$\rho = max_f\{E_l[\rho(l, f)]\} \quad (5)$$

Average values along each frequency orientation aid in enhancing the correlation value especially after filtering or compression, where higher levels of the decomposition tend to be more affected. The final correlator response has been chosen as the maximum value of all subbands in order to exploit any strong structure existent in the image (e.g. many vertical edges) where the watermark is better retained.

The correlator of (4) works satisfactorily under image distortions such as filtering or compression where spatial supports are not changed. In order to detect the watermark under geometric transformations, the following correlator has been defined where the mother signal $W_M(n_1, n_2)$ instead of the entire watermark is employed to exploit its self-similar structure:

$$\rho_M(l, f) = \frac{I'_{f_l}.W_{M,2^{l-1},\lceil r_{max}/2^{l-1}\rceil}}{W_{M,2^{l-1},\lceil r_{max}/2^{l-1}\rceil}.W_{M,2^{l-1},\lceil r_{max}/2^{l-1}\rceil}} \quad (6)$$

$W_{M,2^{l-1},\lceil r_{max}/2^{l-1}\rceil}$ defines the mother signal scaled by $1/2^{l-1}$ and shifted with respect to the watermark center by $\lceil r_{max}/2^{l-1}\rceil$ in both dimensions. This correlator behaves in the same way as the one of (4) even for other kinds of distortions. It is easily proven that when a watermark exists, the correlator's value is 1, and when a watermark does not exist, its value is 0.

Detection is further performed by comparing the final normalized correlator response ρ against a predefined threshold. The latter is estimated in such a way to attain a very small false alarm

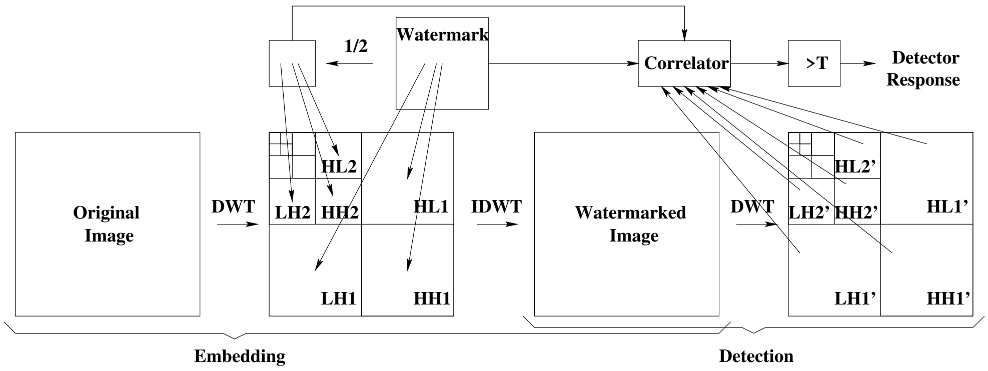


Figure 3: Presentation of the watermark embedding and detection methods in the wavelet domain.

probability (probability of detecting a watermark when it does not exist in the image).

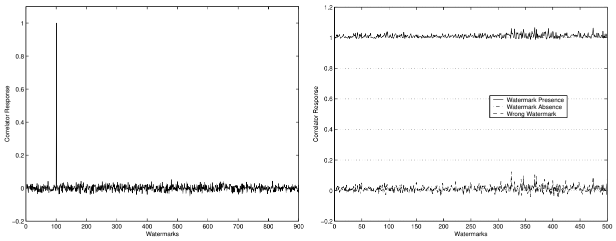
5. SIMULATION RESULTS

During performance evaluation, 5 different greyscale images of size 960×960 have been used. The embedded watermark power has been varied to produce watermarked images with SNR of 30, 35 and 40dB. The stronger the embedded watermark, the more visible it tends to be. An example of part of the original and watermarked image ($SNR = 30$dB) is given in Figure 4. It is noted that the watermark can hardly be distinguished. In order to experimentally prove that different-keyed watermarks are uncorrelated with each other, the correlations between a watermark with index 100 and 900 watermarks, differing only in the key parameter k, have been calculated and shown in Figure 5(a). It is obvious that our assumption holds.

(a) (b)

Figure 4: Part of (a) original image and (b) watermarked image, $SNR = 30$dB.

In order to evaluate the overall thresholds for the three cases of SNR considered, the correlator response for 500 watermarks (5 images, 100 watermarks) has been calculated (shown in Figure 5(b)), when the watermark is present, when the watermark does not exist and when the wrong watermark is attempted to be detected. From these probability distributions and in order to attain a false alarm probability of 10^{-4}, a threshold of 0.05 has been employed for detection when $SNR = 30$ dB, a threshold of 0.085 when $SNR = 35$ dB and a threshold of 0.15 when $SNR = 40$ dB for all distortion cases.

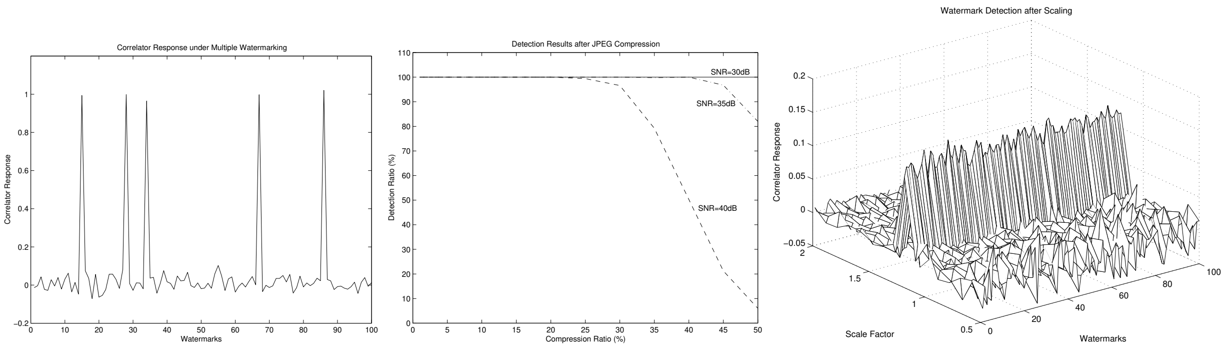


(a) (b)

Figure 5: (a) Correlator response between 900 different watermarks and watermark no 100, (b) Correlator Outputs under watermark presence, watermark absence and wrong watermark detection cases for 100 different watermarks and 5 images.

The detection ratio of the method has been calculated when no distortion or when various distortions have been inflicted on the watermarked images. When no distortions are present, the watermark is detected in all cases (100%). Multiple watermarking has also been tested. Five different watermarks have been embedded to an image and detection has been attempted for 100 watermarks including these five ones. The results are illustrated in Figure 6(a). It is seen that all five watermarks are detected. Filtering with a mean and a median filter of size 3×3 and 5×5 has also been tested. The detection ratios attained are illustrated in Table 1. It is seen that the method is robust against mean and median filtering of size 3×3 even when the embedded watermarks are not sufficiently strong. However, for greater size windows, its performance deteriorates. JPEG compression for a wide range of compression ratios has further been experimented on. The method proves remarkably robust even for weak watermarks (40dBs) which can stand up to 1:30 compression ratio as shown in Figure 6(b).

Geometric distortions have been further introduced to the watermarked images. Detections have been performed using the mother signal and its scaled by 2 version. A detection ratio of 95% has been calculated after rotation by 2^0 without initializing any search range. Non-uniform cropping has led to 100% detection. The original image size is preserved. The opposite case remains to



(a) (b) (c)

Figure 6: (a) Correlator Output in the case of Multiple Watermarking in a single image. The correct watermarks are: 15, 28, 34, 67 and 86, (b) Watermark Resistance to JPEG Compression for different $SNRs$: 30, 35 and 40 dB, (c) Watermark Detection after Scaling for 100 different Watermarks ($SNR = 30$dB).

Table 1: Detection Ratios (%) after Moving Average and Median Filtering of size 3×3 and 5×5. Three SNR cases are considered.

SNR	Filter Type			
	Moving Average		Median	
	3×3	5×5	3×3	5×5
30	100	92.4	100	100
35	100	16.2	100	98.4
40	99	1	100	34.2

be tested. Finally, scaling of the watermarked images by a factor of 1.2 has also led to 100% detection. The correlator response in this case is shown in Figure 6(c). A search range in the scale parameter has been defined as $[0.5 : 2.0]$ and peaks appear, as it is seen, when the scale factor is 1.2.

6. CONCLUSIONS AND FUTURE WORK

A wavelet-based watermarking method has been presented that embeds self-similar watermarks in the detail subbands of the highest and second highest levels of the decomposed images. The incorporation of self-similarity in the watermark structure proves useful for watermark detection under geometric distortion cases. The method is robust against filtering, JPEG compression and geometric distortions. Multiplicative embedding is expected to lead to better performance making use of the implicit visual masking of the wavelet transform and it will be pursued. More experiments will also be conducted to test the robustness of the method under combinations of geometric or other kinds of distortions and wavelet coding.

7. REFERENCES

[1] I. Pitas, "A method for watermark casting in digital images,", *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 8, no. 6, October 1998.

[2] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain", *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 385–403, May 1998.

[3] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-d dft domain", in *Proc. of ICASPP'99*, Phoenix, Arizona, USA, 15-19 March 1999.

[4] R.B. Wolfgang, C.I. Podilchuk, and E.J. Delp, "Perceptual watermarks for digital images and video", *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108–1126, July 1999.

[5] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication", *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1167–1180, July 1999.

[6] C.-T. Hsu and J.-L. Wu, "Multiresolution watermarking for digital images", *IEEE Trans. on Circuits and Systems II*, vol. 45, no. 8, pp. 1097–1101, August 1998.

[7] X.-G. Xia, C.G. Boncelet, and G.R. Arce, "A wavelet transform based watermark for digital images", *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 540–550, May 1998.

[8] M.D. Swanson, B. Zhu, and A.H. Tewfik, "Multiresolution scene-based video watermarking using perceptual models", *IEEE Journal of Selected Areas of Communications*, vol. 16, no. 4, pp. 540–550, May 1998.

[9] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, and A. Piva, "A DWT-based technique for spatio-frequency masking of digital signatures", in *Proc. of SPIE Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, 25-27 January 1999, vol. 3657.