Journal of Electronic Imaging

SPIEDigitalLibrary.org/jei

Discrete Fourier transform–based watermarking method with an optimal implementation radius

Ante Poljicak
Lidija Mandic
Darko Agic

SPIE

IS&T
imaging.org

Discrete Fourier transform–based watermarking method with an optimal implementation radius

Ante Poljicak
Lidija Mandic
Darko Agic
University of Zagreb
Faculty of Graphic Arts
Zagreb, 10000 Croatia
E-mail: ante.poljicak@grf.hr

Abstract. *In this paper, we evaluate the degradation of an image due to the implementation of a watermark in the frequency domain of the image. As a result, a watermarking method, which minimizes the impact of the watermark implementation on the overall quality of an image, is developed. The watermark is embedded in magnitudes of the Fourier transform. A peak signal-to-noise ratio is used to evaluate quality degradation. The obtained results were used to develop a watermarking strategy that chooses the optimal radius of the implementation to minimize quality degradation. The robustness of the proposed method was evaluated on the dataset of 1000 images. Detection rates and receiver operating characteristic performance showed considerable robustness against the print-scan process, print-cam process, amplitude modulated, halftoning, and attacks from the StirMark benchmark software. © 2011 SPIE and IS&T.*
[DOI: 10.1117/1.3609010]

1 Introduction

With today's availability of digital images, the immense leap forward in the computational power of an average computer and new technologies that enable misuse of digital images, there is a growing need for watermarking methods. This need has been met with limited success by scientists and researchers, and there are many different approaches to the problem of digital image protection.

A very common technique is the implementation of the watermark in the frequency domain using some discrete transform. Thus, the energy of the watermark is distributed over the entire image after the transformation back to the spatial domain, which enables the implementation of stronger watermarks with less perceptual impact. The most popular transforms are discrete cosine transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT). Each approach has its advantages and disadvantages. DWT-based methods[1–6] enable good spatial localization and have multiresolution characteristics, which are similar to the human visual system.[6] In addition, this approach shows robustness to low-pass and median filtering. However, it is not robust to geometric transformations. The DCT approach[6–10] is very robust to JPEG compression, since JPEG compression itself uses DCT. However, DCT methods lack resistance to strong geometric distortions.

The DFT approach[10–15] has one advantage in comparison with the spatial domain methods. First, it is translation invariant and rotation resistant, which translates to strong robustness to geometric attacks. On the other hand, according to Raja *et al*., fast Fourier transform (FFT) methods introduce round-off errors, which can lead to loss of quality and errors in watermark extraction.[16] However, Cheddad *et al*. states that this disadvantage is much more important for hidden communication than for watermarking.[17]

Because of its resistance to geometric attacks and the distribution of energy, FFT watermarking methods are developed to create robust watermarking schemes resistant to the degradation attacks of the watermarked image in the transmission channel such as print-scan process (PS process). The robustness of the watermarking method to the PS process would enable the use of the method in the protection of the printed images, thus enabling the use of digital watermarks in the protection of analog media. However, the PS process is very difficult to model. It engenders a number of linear (translation, rotation, and scaling) and nonlinear attacks (pixel distortions and noise addition). These attacks are not only user and equipment dependent, but also time-variant.[11,18,19] For this reason, there are few watermarking methods robust to the PS process all of which use the Fourier transform domain. Examples can be found in He and Sun,[11] Kang *et al*.,[12] Pereira and Pun,[13] and Lee and Kim.[14] There are also some multiple domain methods that use the advantages of different domains to create a very robust watermarking scheme. A good example of a multiple domain method is presented in Al-Haj[6] and Pramila *et al*.[15]

Methods described in Refs. 11–15, are similar in the way they use the Fourier transform domain to implement a watermark. The common property of these methods is the implementation of the binary vector of length l, which is acquired by a pseudorandom generator. This vector is embedded in the magnitude of the Fourier transform of a cover work, as a circle of radius r around the center of the cover work. To control the strength of the implementation, the implementation factor α is used.

Paper 10168R received Oct. 12, 2010; revised manuscript received Mar. 31, 2011; accepted for publication Jun. 17, 2011; published online Aug. 16, 2011.

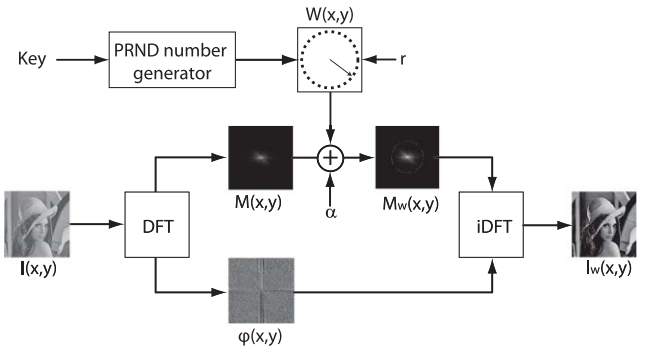

Fig. 1 Block diagram of the encoder.

However, no one gave the methodological evaluation of the influence of the watermark embedding. A search for existing publications on the subject showed that there are no papers that show the influence of this kind of watermark embedding on the overall perceptual quality of an image. Since FFT methods are very popular in the watermarking community, a need exists for this kind of research.

This research has two parts. In the first part, we propose a watermarking method, define the parameters of a watermark, and investigate the influence of the defined parameters on the overall perceptual quality of an image. In the second part, we use the results of the investigation to modify the encoder of the proposed watermarking method and test its robustness to various attacks such as cropping, blurring, PS process, Print-Cam (PC) process, etc.

The rest of the paper is organized as follows. Section 2 describes the watermarking method. Section 3 defines the parameters of the watermark and evaluates how they affect the quality of a watermarked image. Section 4 explains the modification of an encoder for our watermarking method. Section 5 gives the results of the robustness test of the proposed method and its comparison with other similar methods. A conclusion is given in Sec. 6.

2 Watermarking Method

2.1 *Encoding*

The watermark is embedded in a cover work in the magnitude coefficients of the Fourier domain. The block diagram of the encoder is shown in Fig. 1.

First, luminance values of the cover work are transformed in the Fourier domain. For color images luminance (Y) is obtained by transformation from RGB to YCbCr color space. Then, the low frequency magnitude coefficients of the transform are moved to the center. This enables the control in what frequencies the watermark will be embedded by controlling the radius of the implementation. Third, using the secret key k that represents the seed of the pseudorandom generator, the row vector v with l binary elements is obtained. After that, according to the radius of the implementation r, elements of the watermark matrix are calculated using the following [Eq. (1)]:

$$W(x_i, y_i) = v(j)\left[\frac{1}{9}\sum_{s=-1}^{1}\sum_{t=-1}^{1} M(x_i + s, y_i + t)\right], \tag{1}$$

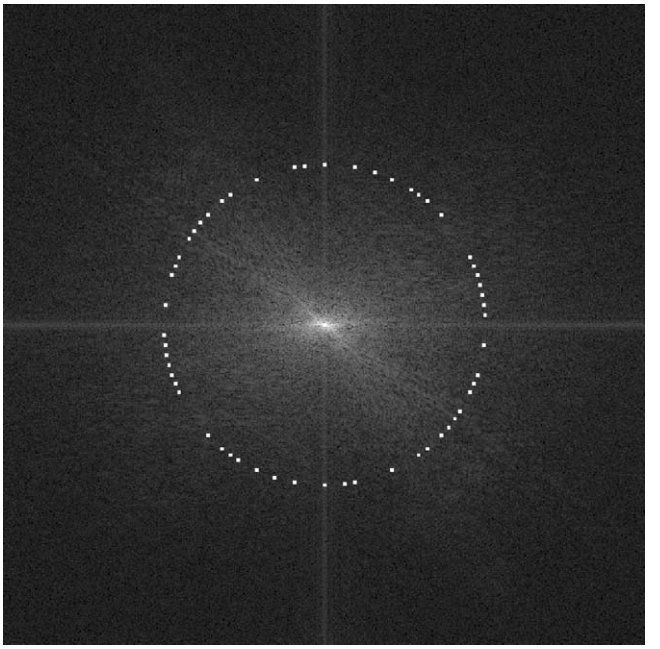

Fig. 2 Embedded watermark in the magnitude coefficients of the Fourier domain (intensities of the watermark coefficients are exaggerated to be visible).

where $W(x_i,y_i)$ are elements of the watermark matrix, $v(j)$ is the j'th element of the row-vector v; and $M(x_i,y_i)$ are the elements of the magnitude of the cover image.

Coordinates (x_i,y_i) are defined as:

$$x_i = \left(\frac{m}{2} + 1\right) + \left\lfloor r\cos\left(\frac{j\cdot\pi}{l}\right)\right\rfloor \tag{2}$$

$$y_i = \left(\frac{n}{2} + 1\right) + \left\lfloor r\sin\left(\frac{j\cdot\pi}{l}\right)\right\rfloor, \tag{3}$$

where m and n denote size of the matrix M, r is implementation radius, l denotes the length of the row-vector, and $\lfloor\cdot\rfloor$ denotes a floor operator.

The elements of the watermark are equally spaced around the center of the watermark matrix, and the watermark matrix is then embedded in the magnitude coefficients of the cover work using the equation:

$$M_w(x, y) = M(x, y) + \alpha * W(x, y), \tag{4}$$

where x and y are image coordinates, M is the magnitude of the cover image, W is the watermark matrix, α is the implementation factor, and M_w is the magnitude of the watermarked image.

Finally, the watermarked magnitude coefficients $M_{w(x,y)}$ (Fig. 2) are combined with unaltered phase coefficients $\varphi(x,y)$ and transformed back to the spatial domain. For color images, Y component is concatenated with chromaticity components. The result is the watermarked image I_w.

2.2 *Decoding*

A decoder makes a blind iterative search for the implemented watermark. Therefore, for detection, the original image is

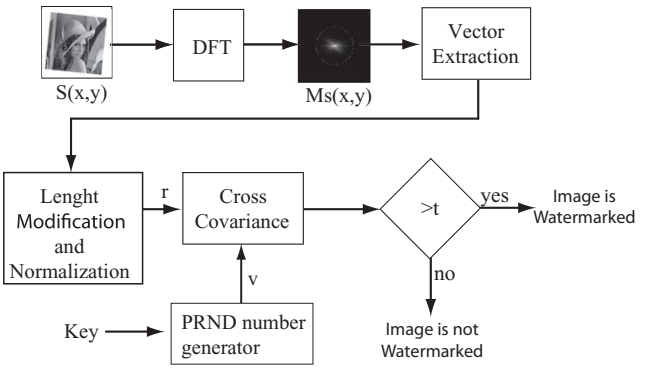

Fig. 3 Block diagram of the decoder

not required. The only requirement is the key used for the generation of the watermark. A block diagram of the decoder is shown in Fig. 3.

To test for the existence of a watermark in an image, the image is first resized to 512×512 pixels using bilinear interpolation. After scaling, the image is transformed to the Fourier domain. Then, row-vectors are extracted from the magnitude coefficients of the image from radii $r_{\min}$ to $r_{\max}$. Each extracted vector is then resized to length l defined by Eq. (5):

$$l = r_{\max} * \pi. \tag{5}$$

Then, its values are normalized to interval [0 1]. After normalization, cross covariance is calculated between the extracted vector r, and the row-vector v generated with a pseudo-random generator using the original key as a seed. The cross-covariance of two vectors is actually a cross-correlation of the vectors with removed mean value. It is defined as:

$$C_{rv}(m) = \begin{cases} \sum_{n=0}^{N-|m|-1} \left(r(n-m) - \frac{1}{N}\sum_{i=0}^{N-1} r_i \right) \left(v_i^* - \frac{1}{N}\sum_{i=0}^{N-1} v_i^* \right), & m \geq 0 \\ C_{rv}^*(-m), & m < 0 \end{cases}, \tag{6}$$

where C_{rv} is the cross covariance of vectors r and v, and * denotes complex conjugation.

The watermark detection is positive if the maximum value of cross-covariance exceeds a predefined threshold t.

3 Influence of Watermark Parameters on the Peak Signal-to-Noise Ratio

In the first part of the research, we evaluate the influence of the watermark on the overall quality of an image and develop a watermarking method that takes into account the influence on an image. This approach, in comparison with other similar methods, gives a more robust watermark while maintaining the same level of degradation of a watermarked image.

The influence of the watermark on the quality of the image depends on the length of a vector, the radius of an implementation, and the implementation factor. Furthermore, these parameters will have a different influence on the overall quality of the watermarked image.[9] To determine how each parameter affects the quality, we designed an experiment where two parameters are constant while one varies. For the experiment, we used the encoder described in Sec. 2, and shown in Fig. 1. We used five images, "Lena," "Mandrill," "Peppers," "Kiel," and "Lighthouse" (Fig. 4). All images are bitmaps with a resolution of 512×512 pixels.

Fig. 4 Pictures used for the experiment.

The quality of a watermarked image is evaluated by the peak signal-to-noise ratio (PSNR), which is, albeit old, still a very common metric for quality assessment in image processing. It is defined as:

$$\mathrm{PSNR} = 10 * \log\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right), \tag{7}$$

where MAX is the highest possible value in an image (usually 255), and MSE denotes mean squared error, which is given as:

$$\mathrm{MSE} = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} \|I_w(x,y) - I(x,y)\|^2, \tag{8}$$

where m and n are the dimensions of an image, x and y are the image coordinates, $I_{w(x,y)}$ is the watermarked image, and $I(x,y)$ is the cover work. The PSNR is often given in decibels. Values above 40 dB indicate low degradation, while values below 30 dB indicate low quality.[17]

Three parameters were controlled in the experiment: an implementation factor α, the radius of the implementation r, and the length of the row vector l. The PSNR was calculated for the different values of each parameter, while the other two were held constant. In the first part of the experiment, the influence of the implementation factor α was tested. The factor varied from 0 to 30, while the radius was set to 128 and a row-vector had 50 elements. With the increase of the implementation factor α, a watermarked image is more robust to attacks, and the watermark is easier to detect; however, its impact on the overall quality of the image increases.

For the second part of the experiment, the radius was varied in an interval from 25 to 250, the implementation

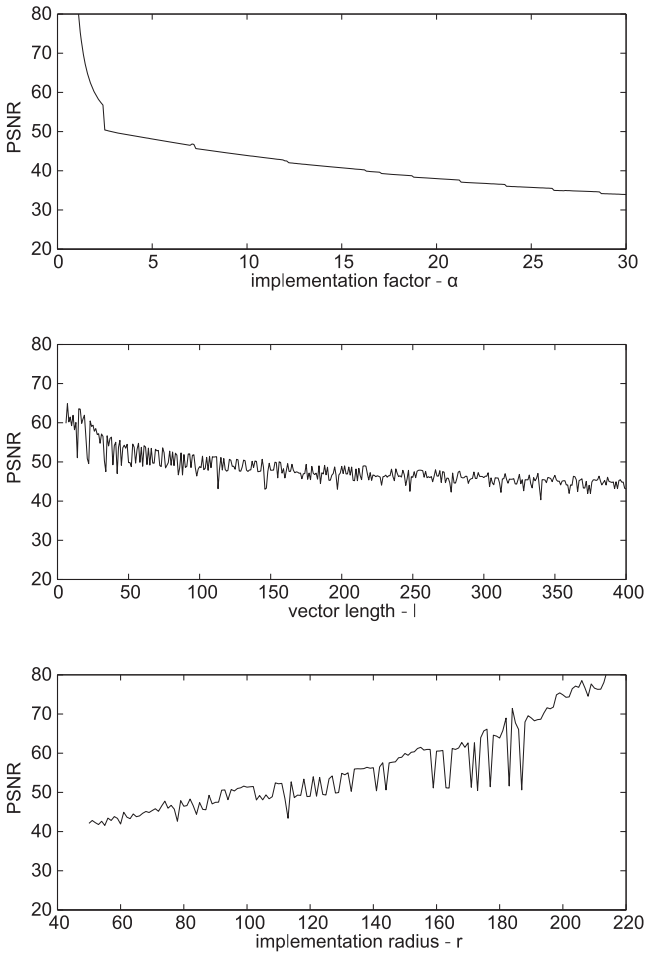

Fig. 5 Influence of the watermark properties on PSNR (Lena).

factor α was 3, and the row-vector length was 50. The radius of the implementation is very important since the frequencies of the magnitude coefficients in the Fourier domain increases as the radius increase. The manipulation of the lower frequency magnitudes (smaller radius) has more impact on the quality of the watermarked image than the manipulation of the higher frequency magnitudes (bigger radius). PSNR values depend on the radius much more unpredictably. Even though there is a general rule of thumb that a smaller radius means a bigger degradation, for some radii the degradation is smaller, while for other radii it is bigger than expected.

In the third part, the length of the row-vector varied between 1 and 400 elements, the implementation factor α was 3, and the radius was set to 128. The length of the vector also has a significant influence on the quality of the watermarked image. With the increase of the number of bits implemented, the quality deteriorates.

Results for Lena are shown in Fig. 5. Results for other images were similar.

With the change of the implementation factor, the PSNR decreases monotonously. For the small values of an implementation factor, the PSNR first falls rapidly, and then the fall rate decreases. For some images the curve is continuous and has a logarithmic shape, while for other images, there is a discontinuity, a drop in the PSNR value.

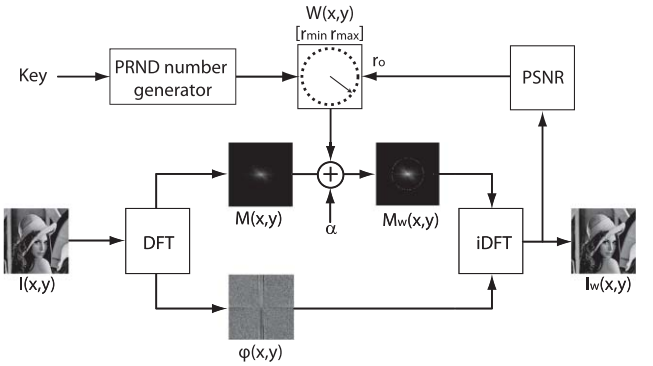

Fig. 6 Block diagram of the modified encoder

The length of the watermark affects the PSNR in a less predictable way than the implementation factor. In general, the PSNR decreases as the number of implemented bits increases; however, for small intervals of vector length, there is the local maximum of the PSNR. As the vector length increases, local maximums are less and less salient.

With the increase of the implementation radius, the PSNR value increases. Same as with the watermark length, the influence on the PSNR is not predictable, and there are some radii that are much more suitable for implementation. We use this fact to modify the encoder of the proposed method to achieve the adaptability of the method to different cover works.

The quality of a watermarked image heavily depends on the properties of the cover work. Some images are more affected with the implementation of the watermark than other images.

4 Modification of the Encoder

From the results of the previous experiment, we see that the quality degradation of an image due to watermark embedding can be mitigated by carefully tuning the parameters of the watermark. By tuning any of the three parameters, we can improve the overall quality of an image. However, the best way to minimize the quality degradation is to modify the radius of the implementation, since some radii of implementation affect the overall quality of a watermarked image much less than other radii.

We modified the encoder from Fig. 1 to search for the optimal radius r_o (Fig. 6). The optimal radius is the radius for which the PSNR value is maximized; it is determined by calculating the PSNR for each r_i in an interval $[r_{\min}\ r_{\max}]$. When the optimal radius is found, the encoder uses it for the implementation of the watermark.

The search for the optimal radius enables adaptation of the watermark to an individual image. In this way, the robustness of the watermark in an image is increased while the PSNR value is maximized.

Comparison of the original and modified encoder is given in Table 1. The results in the table were acquired by watermark implementation in the dataset of 1000 different color and grayscale images. The implementation factor α was 5 and vector length l was 200. The modified encoder searched for optimal radius in interval [140 180] (mean optimal implementation radius was 175.4). The original encoder had

Table 1 Comparison of the watermarking of 1000 images using the original and the modified encoder.

	Mean implementation radius r	Mean PSNR value
Original encoder	175 (fixed)	49.2
Modified encoder	175.4	53.3

a fixed implementation radius r set to 175 (this value was chosen to be comparable with the results of the modified encoder). While using the modified encoder, the mean PSNR value of the watermarked images was 53.3, which is a significant improvement over 49.2 when the original encoder was used.

Another advantage of the modified approach is that the radius of the implementation is different for different images. In this way, the security of the method is further improved, since a possible attacker is unable to find out the exact radius of the implementation. Therefore, even if the attacker has access to key and length of the row-vector, it would be extremely difficult to remove the watermark without seriously affecting the image quality.

5 Robustness of the Proposed Watermarking Method

5.1 *Experiment*

To evaluate the robustness of the proposed method we embedded a watermark in 1000 different color and grayscale images. The robustness of the watermarking method depends on the strength of implementation. Therefore, to ensure the repeatability of the test, the implementation factor for each image was chosen to produce a watermarked image with the PSNR value around 40 dB. The implementation factor varied from 2.5 to 30 with the mean value for all images around 7. The histogram of PSNRs obtained is shown in Fig. 7. This value was chosen to obtain watermarked images that are perceptually indistinguishable from original images. An example of watermark embedding is shown in Fig. 8.

For the evaluation, the StirMark benchmark was used.[20–22] This program enables testing a watermarking method against

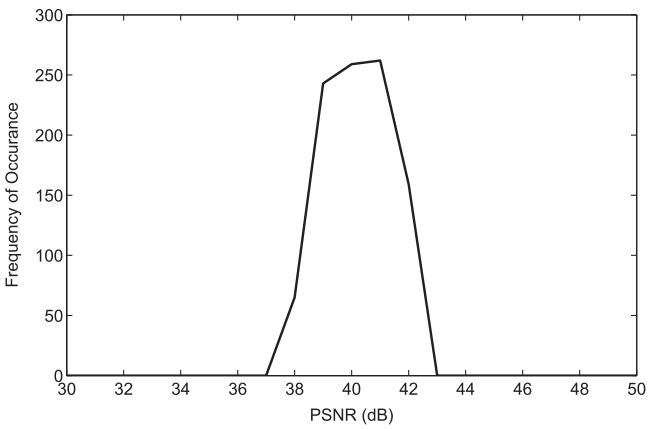

Fig. 7 Histogram of the PSNR values of watermarked images.

Fig. 8 Example of watermark embedding; (a) original image and (b) watermarked image (PSNR = 41 dB).

different attacks. We tested the robustness against cropping, blurring, noise, rotation, scaling, and JPEG compression. We also employed attacks that are not part of the StirMark benchmark, such as amplitude modulated (AM) halftoning with different halftoning frequencies (10 to 40 lines per centimeter). In addition, to test the method in a real world situation, we printed images on a laser printer (Xerox Phaser 6250 N) with a printing resolution of 600 dpi. The size of the printed images was 13×13 cm. After that, the prints were digitized on a flatbed scanner (Microtek Scanmaker 8700) with a scanning resolution of 150 dpi. The prints were also photographed with a digital camera on a cell phone (Sony Ericsson C702). Images acquired with the cell phone were JPEG compressed and had resolution of 1024×768 pixels. During the experiment, it was noticed that the sharpening of the digital image using a Laplacian-based unsharp filter before detection, significantly improved acquired detection value; this is also included in the results.

5.2 *Results*

For the evaluation of robustness, detection rate and receiver operating characteristic (ROC) curves were used.

The detection rate was determined after watermarked images were subjected to an attack. The value of the detection threshold was set to $t = 0.25$. This value was chosen because the highest detection value of the unwatermarked set of images was 0.23, thus avoiding false positive detection for the given dataset. The detection rates after different attacks are given in Table 2.

The detection rates after an attack show that our method is very robust to most of the attacks employed. It is especially robust to geometrical distortion, which was expected due to inherent properties of DFT. However, DFT is known to be very sensitive to cropping. Even here, the detection rate for 50% cropping was 92%. Very interesting is the resistance of the method to AM halftoning, with robustness to halftoning frequencies as low as 10 lin/cm. Our method was weakest to blurring, with the filter size greater than 5×5 pixels. Detection rate after the PS and PC process was 86.9 and 82.7%, respectively. A lower detection rate for photographed images was expected since the images in PC process were JPEG compressed. The experiment also showed that the detection rate after the PS and PC process is increased if a Laplacian-based unsharp filter was used before detection. With the unsharp filter, the effect of low-pass filtering of the PS and PC process is somewhat attenuated. It should be noted that the same effect on detection rate was obtained for the blur attack. For other

Table 2 Detection rate for $t = 0.25$ after different attacks.

	JPEG						PS		PC	
Attack	0	20	40	60	80	100		Unsh		Unsh
Detection rate [%]	9.10	22.5	58.2	82.2	97.6	100.0	86.9	95.0	82.7	87.4
	Crop (%)			Scale (%)			Rotation (°)			
Attack	50	70	90	50	75	200	−60	−30	30	60
Detection rate [%]	92.2	97.6	99.6	85.9	99.8	100.0	97.7	98.6	98.0	94.7
	AM Halftone (lin/cm)			Blur			Noise (%)			
Attack	13	15	40	3×3	5×5	7×7	3	5	7	9
Detection rate [%]	97.4	99.7	100.0	95.1	91.1	21.7	99.4	97.4	95.8	88.1

attacks, however, unsharp filtering did not give an increase in the detection rate.

To avoid the influence of the predefined threshold value, the ROC curves were used. The ROC curve is a graphical plot of the probability of true positive detection versus. the probability of false positive detection.[23] It provides a good tool for estimating the behavior of a detector for different types of degradations introduced to an image.

For the detection of a watermark in an image, correlation of extracted vector r with the generated vector v, has to exceed a value set as the threshold. This means that the

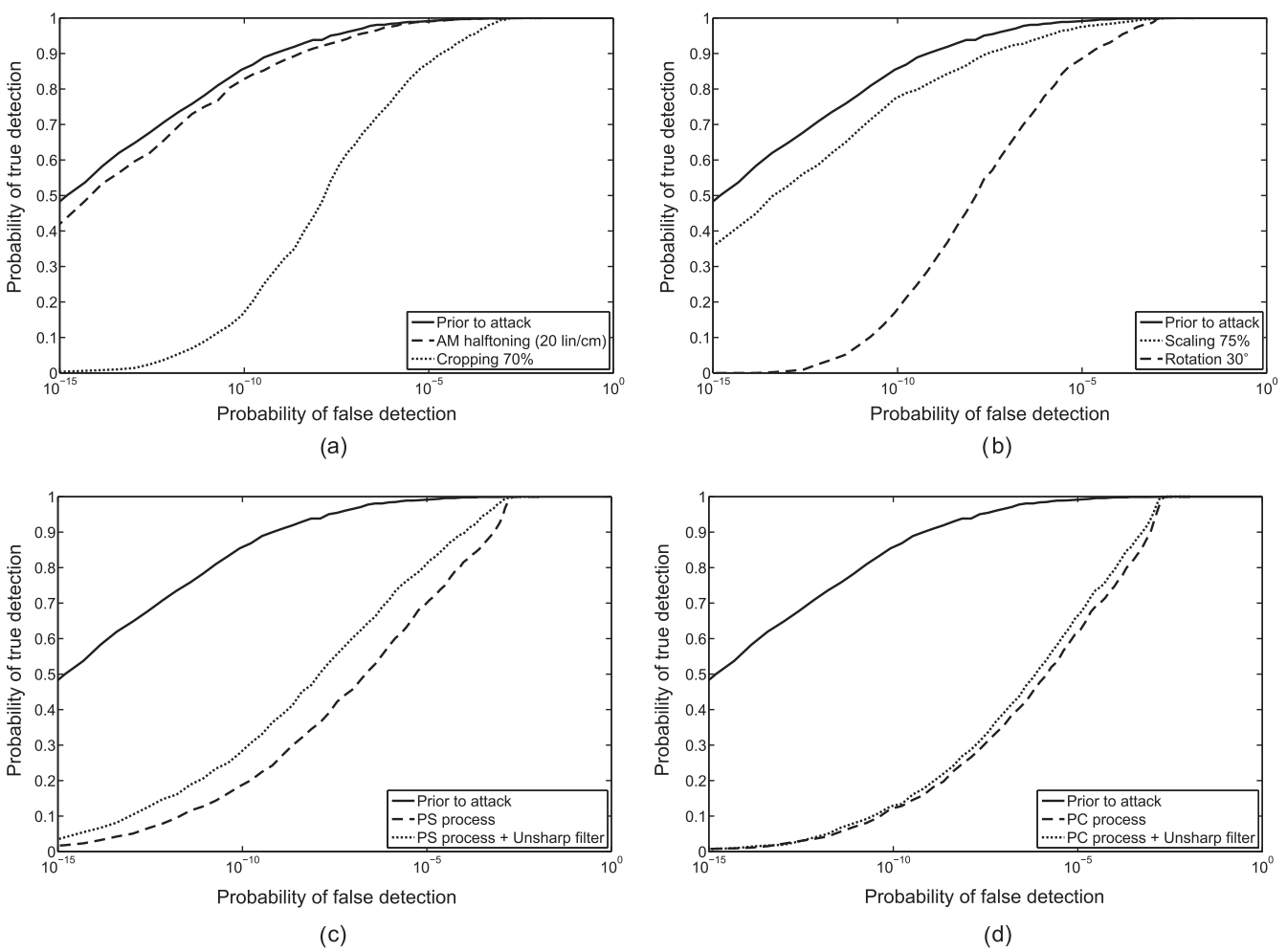

Fig. 9 ROC curves prior to and after attacks: (a) AM halftoning and cropping; (b) Scaling and rotation; (c) PS process; (d) PC process.

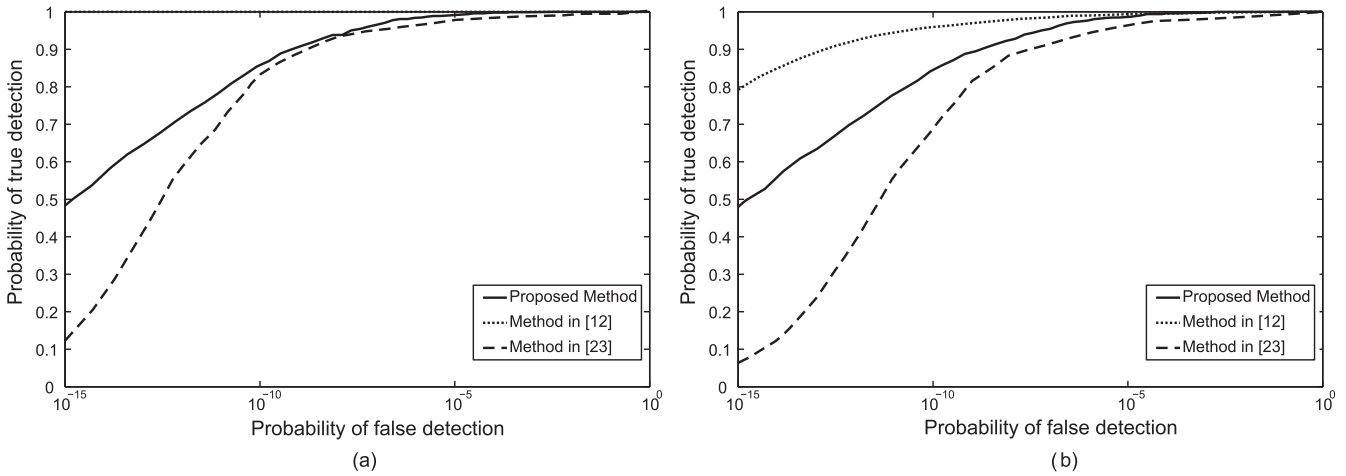

Fig. 10 Comparison of ROC curves (a) prior to attack and (b) after JPEG 70 compression.[12,23]

probability of true and false positive detection depends on the threshold value t chosen at the detector. The threshold has to be set low enough to enable the detector to detect a watermark in a watermarked image, even if the image goes through intentional or unintentional attacks which may occur. However, by decreasing the value of t, the probability of a false positive detection increases. The false positive detection occurs when the detector detects a watermark in an unwatermarked image. High false positive detection rate is, for most practical watermarking methods, unacceptable.

The probability of a false positive is the probability that the detection value for unwatermarked image will exceed the threshold value. It is hard to empirically determine, since the real watermarking systems usually generate low detection values for unwatermarked images (in our case the highest detection value for unwatermarked dataset was 0.23). Therefore, the probability of false positive is usually estimated using some theoretical model such as the one described in Refs. 24 and 25. Chang *et al*. states that if D is the correlation coefficient between a d-dimensional watermark vector and a random vector drawn from a radially-symmetric distribution the probablility of false positive detection can be modeled as Ref. 25:

$$P\{D > t\} = \frac{\int_0^{\cos^{-1}(t)} \sin^{d-2}(u)du}{\int_0^{\pi/2} \sin^{d-2}(u)du}, \tag{9}$$

where P is the probability of a false positive detection for threshold value t, and d is the dimension of a watermark vector. We used the same model for the estimation of the false positive probability.

ROC curves prior to and after attacks are shown in Fig. 9. For simplicity, we did not include the ROC curve after every attack. The ROC curve prior to attack serves as upper bound on robustness. For relatively high false positive probability (10^{-3}), the proposed method is very robust to most attacks. For lower false positive probability ($<10^{-5}$), the detection value decreases. ROC curves show that our watermarking method is especially resilient to AM halftoning with frequency higher than 20 lin/cm [Fig. 9(a)], scaling, and rotation [Fig. 9(b)]. In cropping, our method is less robust, but the detector is still able to detect the watermark in most of the pictures cropped to 70% for false positive probability around 10^{-4} [Fig. 9(a)].

For the PS and PC process, ROC curves are slightly worse [Figs. 9(c) and 9(d)]. It is shown that the result can be improved if unsharp filtering is used. Unsharp filtering is especially useful for improvement of detection values after scanning.

5.3 *Comparison with Other Methods*

The main advantage of the proposed method over other similar methods is computational simplicity, device independence, and adaptability, while maintaining the same robustness. The authors in Ref. 18 state that their method is only effective with laser printers, while our method is not restricted to one type of printer. The results of robustness against AM halftoning suggest that our method can be used with conventional imaging devices and printing presses. In Ref. 18, printed images should be scanned with at least 600 dpi in order to extract a watermark, while we used a resolution of 150 dpi. Since the proposed method is simple, the time needed for a watermark extraction is short, about 1 s in comparison with 29 s for the method in Ref. 25. Also, our method adapts the parameters of a watermark to generate a more robust watermark for the same PSNR value.

Further, we compare ROC characteristics of our method with those in Refs. 12 and 23. We note that our dataset differs from those in Refs. 12 and 23, but since the number of images was great, results are still comparable. PSNR values of obtained watermarked images for all three methods was around 40 dB. Methods[12,23] are based on log-polar mapping in Fourier domain, which makes their methods computationally more complex than our method. Figure 10 shows the comparison ROC curves of the three methods prior to attack and after JPEG 70 compression. While the method in Ref. 12 gives superior results in terms of robustness, our method considerably improves over the method in Ref. 23.

6 Conclusion

In this paper we proposed, a fast, simple, and robust watermarking method based on DFT. Evaluating the influence of watermark properties on the PSNR value of the watermark image, we conclude that deterioration depends heavily on

the statistical properties of the cover work, and that each watermark property affects the overall quality of an image differently. While the influence of the implementation factor can be presumed, the influence of the watermark length and the radius of the implementation cannot be estimated. The experiment showed that for some vector lengths and some radii, the deterioration of the quality is much smaller.

This is used to develop a watermarking method which minimizes the quality deterioration of the watermarked image by finding the optimal implementation radius. With a modified coder, our method is able to adapt to the properties of an image which leads to a more robust watermark while maintaining the same influence on overall quality of a watermarked image.

The proposed method showed excellent robustness to the attacks from the StirMark benchmark, AM halftoning, PS process, and PC process. We also conclude that the detection rate after blurring, PS, and PC process is increased if an unsharp filter is used. In comparison with most other watermarking methods, our method showed improvement in robustness against cropping, PS and PC process, and ROC performance.

References

1. G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on DWT-SVD," *Computer Standards & Interfaces* **31**(5), 1002–1013 (2009).
2. M.-S. Wang and W.-C. Chen, "A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography," *Computer Standards & Interfaces* **31**(4) 757–762 (2009).
3. S. H. Wang and Y. P. Lin, "Wavelet tree quantization for copyright protection watermarking," *IEEE Trans. Image Process.* **13**(2), 154–165 (2004).
4. A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," *Pattern Recogn. Lett.* **26**(7) 1019–1027 (2005).
5. M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Trans. Image Process.* **8**, 783–791 (2001).
6. A. Al-Haj, "Combined DWT-DCT digital image watermarking," *J. Comput. Sci.* **3**(9), 740–746 (2007).
7. C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Process.* **8**, 58–68 (1999).
8. G. C. Langelaar and R. L. Lagendijk, "Optimal differential energy watermarking of DCT encoded images and video," *IEEE Trans. Image Process.* **10**, 148–158 (2001).
9. W. C. Chu, "DCT-based image watermarking using subsampling," *IEEE Trans. Multimedia* **5**, 34–38 (2003).
10. A. M. Fard, M. Akbarzadeh-T, and F. Varasteh-A, "A new genetic algorithm approach for secure JPEG steganography," in *Proc. IEEE Int. Conf. on Engineering of Intelligent Systems*, Vol. 22–23, pp. 1–6, Islamabad, Pakistan (2006).
11. D. He and Q. Sun, "A practical print-scan resilient watermarking scheme," in *IEEE Proc. Int. Conf. on Image Processing (ICIP)*, pp. 257–260, Genova, Italy (2005).
12. X. Kang, J. Huang, and W. Zeng "Efficient general print-scanning resilient data hiding based on uniform log-polar mapping," *IEEE Transactions on Information Forensics Security* **5**(1), 1–12 (2010).
13. S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," in *IEEE Trans. Image Process.* **9**(6), 1123–1129 (2000).
14. J. S. Lee and W. Y. Kim, "A robust image watermarking scheme to geometrical attacks for embedment of multibit information," *Lect. Notes Comp. Sci.* **3333**, 348–355 (2005).
15. A. Pramila, A Keskinarkaus, and T. Seppänen, "Multiple domain watermarking for print-scan and JPEG resilient data hiding," *Lect. Notes Comp. Sci.* **5041**, 279–293 (2008).
16. K. B. Raja, C. R. Chowdary, K. R. Venugopal, and L. M. Patnaik, "A secure image steganography using LSB, DCT, and compression techniques on raw images," in *Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing*, pp. 170–176, Bangalore, India (2005)..
17. A. Cheddad, J. Condell, K. Curran, and M. Kevitt: "Digital image steganography: suvey and analysis of current methods," *Signal Process.* **90**, 727–752 (2010).
18. K. Solanki, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Estimating and undoing rotation for print-scan resilient data hiding," *IEEE Proc. Int. Conf. on Image Processing (ICIP)*, Singapore, Vol. 1, pp. 39–42 (2004).
19. B. Perry, B. MacIntosh, and D. Cushman, "Digimarc MediaBridge: the birth of a consumer product from concept to commercial application," *Proc. SPIE*, **4675**, 118 (2002).
20. F. A. P. Petitcolas, M. Steinebach, F. Raynal, J. Dittmann, C. Fontaine, and N. Fatès, "A public automated web-based evaluation service for watermarking schemes: StirMark Benchmark," in *Proceedings of Electronic Imaging, Security, and Watermarking of Multimedia Contents III*, Vol. 4314,. The Society for Imaging Science and Technology (I.S.&T.) and the International Society for Optical Engineering (SPIE) (2001).
21. F. A. P. Petitcolas, "Watermarking schemes evaluation," *IEEE Signal Process.* **17**(5), 58–64 (2000).
22. H. V. Poor, "An introduction to signal detection and estimation," Springer-Verlag, Berlin, Germany (1994).
23. C. Y. Lin, M. Wu, J. Bloom, I. Cox, M. Miller, and Y. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. Image Process.* **10**(5), 767–782 (2001).
24. M. L. Miller and J. A. Bloom, "Computing the probability of false watermark detection," *Information Hiding, LNCS*, Vol. 1768, pp. 146–158, Springer, Berlin/Heidelberg (2005).
25. X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "ADWT-DFT composite watermarking scheme robust to affine transform and JPEG compression," *IEEE Trans. Circuits Syst. Video Technol.* **13**(8), 776–786 (2003).

Ante Poljicak obtained his BSc degree from the Faculty of Graphic Arts at the University of Zagreb. After graduation, he worked in a publishing company in the prepress department. In 2008, he became a research fellow at the Faculty of Graphic Arts, University of Zagreb, where he worked on his doctoral thesis. He authored and co-authored a number of scientific papers. His research interests include color appearance models, image processing, and steganograpy.

Lidija Mandic obtained her BSc, MSc, and PhD degreesfrom the Faculty of Electrical Engineering and Computing, University of Zagreb. After graduation, she worked at the Technical School for Electronics in Zagreb as an lecturer and then as a chief technologist at the Research Department at Factory for Radio Industry in Zagreb. From 1995, she worked as an assistant at the Reproduction Photography Department at the Faculty of Graphic Arts, University of Zagreb. Today, she works as an assistant professor at the Faculty of Graphic Arts, University of Zagreb. She has published a number of scientific papers in Croatian and international scientific journals. She participated in many Croatian and foreign scientific meetings. Her research interests include the field of colorimetry, color management, image processing, and color appearance models.

Darko Agic obtained his BSc and MSc degrees from the Faculty of Technology at the University of Zagreb. After graduation, he joined the academic staff of the Reproduction Photography Department at the Faculty of Graphic Arts, University of Zagreb. He worked as an assistant and then as a lecturer at the same department. In 2001, he received his PhD from the Faculty of Organization and Informatics in Varazdin, University of Zagreb. He now works as a professor at the Faculty of Graphic Arts, University of Zagreb. His research activities are primarily concerned with the reproduction of picture information and color management in the area of printing science and graphic communication. He has published many original scientific and technical papers and took part in many scientific meetings in Croatia and in other foreign countries.