Enhancement of Fourier Image Watermarking Robustness

Rabia Riad [*,**] **Frédéric Ros** [*] **Rachid Harba** [*] **Hassan Douzi** [**] **Mohamed Elhajji** [**]

[*] *PRISME Laboratory, University of Orléans, BP 6744, 45067 Orléans cedex2, France. (e-mail: {rabia.riad, frederic.ros, rachid.harba}@univ-orleans.fr)*
[**] *IRF-SIC Laboratory, Ibn Zohr University, BP 8106 - City Dakhla, 80000 Agadir, Morocco. (e-mail: {h.douzi, m.elhajji}@uiz.ac.ma)*

Abstract: Fourier watermarking is often chosen to watermark images that have to be printed and scanned on a physical support, during which the so-called print-scan attack occurs. One popular method embeds the watermark in the FFT magnitudes of the image along a circle of optimal radius. This paper presents an enhancement of Fourier watermarking robustness by pre-processing data to be watermarked before insertion of the watermark. This pre-processing consists in reducing the variance of the FFT magnitudes of the image. Two schemes are proposed to reduce the variance: the first is based on a low pass filter applied on the data, while the second selects the FFT magnitudes that lower the variance in a region located between two predefined circles. Results show that the robustness to print-scan attack is increased compared to traditional Fourier watermarking. The whole scheme is efficient and has a low computational cost that makes it compatible with industrial constraints.

Keywords: Image, Watermarking, FFT, Pre-processing, Counter attacks.

1. INTRODUCTION

The development of Internet and the evolution from analog to digital media has created many new security issues, among which the need for embedding copyright information. Data hiding is a form of communication in which a watermark is conveyed by embedding it in a cover object, such as an image, video or audio to protect it from illegal copying or reproduction. Most of the watermarking methods proposed are designed to protect digital images. These methods embed a short message (a watermark) in the image, which does not affect usability, but can be detected using dedicated analysis software. The watermarks should be robust enough to survive various attacks. At the same time, the embedded watermark should not degrade the visual quality of the cover. The receiver should be convinced that the cover work has been created by an identifiable entity, and that it has not been tampered with. The essential requirements of digital watermarking are robustness, perceptual transparency and capacity. In addition, watermark embedding and retrievals should have low complexity and be real time in order to be acceptable for various industrial applications.

Most image watermarking methods are in the spatial or transform domain. Popular methods are spread spectrum (Valizadeh and Wang, 2012), discrete cosine transform (Pan et al., 2013), discrete Fourier transform (Poljicak et al., 2011), and wavelets transform (Musrrat et al., 2015). Some schemes take advantage of multiple domain methods (Musrrat et al., 2014). Others exploit the characteristics of the Human Visual System in the watermarking process (Li et al., 2013). A comprehensive description of watermarking techniques can be found in (Cox et al., 2007).

The print scan process on a physical support is commonly used for image reproduction and distribution. Document authentication of passports, ID cards, etc. is becoming more and more important today due to the security concerns. The print scanned image is subject to different degradations called the print-scan attack.

This attack can be considered as one of the strongest that watermarked images undergo (Yu et al., 2005; Amiri and Jamzad, 2014). The print-scan process is complex as it is a composite of various attacks, which cause various distortions divided into operational distortions (for example global RST: Rotation, Scale, Translation) and systematic distortions (local RST, noise, blur, etc) (Yu et al., 2005). These attacks are not only user and equipment dependent but also time-variant (Yu et al., 2005). Different features of the original signal are degraded at various levels. The print-scan attack is still a challenging issue in the image watermarking community. To deal with geometrical attacks produced during the print-scan process, several synchronization schemes have been successfully designed (Kang et al., 2010; Lin et al., 2001). A review is presented by (Kang et al., 2010). Different Fourier schemes have demonstrated their efficiency as they can deal with geometrical transformations such as translation and rotation that occur during the print-scan attack (Poljicak et al., 2011; Ros et al., 2006). In the most recent developments in (Poljicak et al., 2011; Riad et al., 2014) and then in (Riad et al., 2016), researchers have focused on how to

⋆ This work is supported by the GEMALTO COSEC ID EU project.

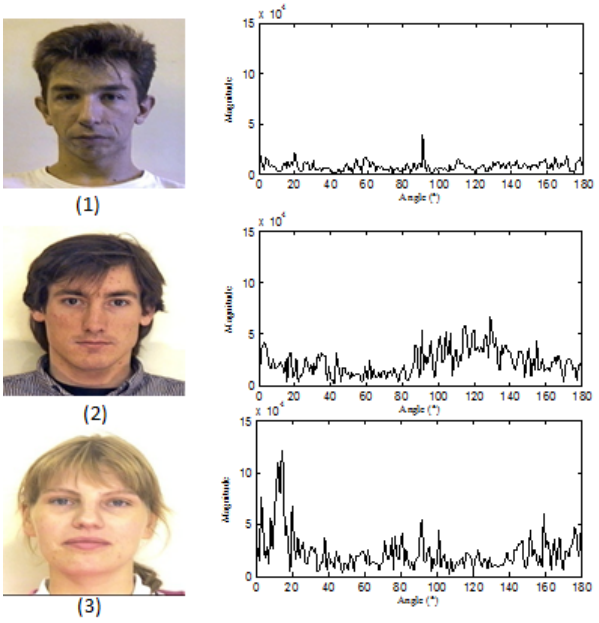

Fig. 1. Three selected images and the distribution of their corresponding Fourier coefficients.

pre-process the image before watermark detection in order to resist the print-scan attack (*e.g.* deblurring filter, color correction) and acting as a counter attack.

These methods are only partially successful. The complex nature of the combined attack makes it difficult to understand all aspects of changes imposed on printed and scanned images. The interest of the research community for this type of attack has never been greater and the challenge is to find better schemes. The search for more efficient counterattacks is essential, but their role is only curative.

Other fields, however, have to be more thoroughly explored, and among them, pre-processing the image before watermarking.

Some images, even those of the same nature (for example ID images) and usage scenario (insertion, synchronization and counterattacks), are naturally more appropriate for the embedding process. They obtain better detection rates than others and the difference can be high. As an example, the three images in Fig. 1 respectively give correlation scores of $R_{cor} = 0.88$, $R_{cor} = 0.61$ and $R_{cor} = 0.39$ applying the same Fourier watermarking scheme proposed in (Poljicak et al., 2011). This has motivated the development of a pre-processing scheme. Pre-processing can be considered as a preventive method aiming at improving the whole watermarking process.

To the best of our knowledge, few image watermarking schemes have exploited this idea during the embedding phase. Efficiency of the pre-processing is linked to the embedding scheme and many schemes are not suitable. One way to pre-process the images before watermarking was presented by (Cox and Miller, 2004). The aim of pre-processing is to modify the image in order to increase the detection rate. The authors embedded the watermark using an additive spatial domain spread spectrum technique, and the pre-processing was used prior to watermark embedding. In the case of a print-scan watermarking application, (Reed and Bradley, 2005) applied a tone correction to bring the pixel levels into the linear region of the print-scan response curve in order to deal with images that have significant saturation problems.

The present paper is based on the concept of pre-processing the host vector before watermarking. It is motivated by an industrial application where identity images are watermarked and printed on a smart card plastic support to increase security checking.

More precisely, the constraints are the following: the watermark is to be invisible, the error rate must be very low (less than 1%), and the method should be fast and simple for the user.

The method proposed by (Poljicak et al., 2011) consists in watermarking the FFT magnitude of the image along a single circle of optimal radius. This method is efficient when print-scan attacks occur and suitable for a pre-processing process. It will be chosen here. Reducing the variance of this vector increases the robustness of the watermarked image. Two schemes are proposed to reduce the variance: the first is based on a low pass filtering of the FFT magnitude, while the second one selects the FFT magnitude in a region located between two predefined circles. These two methods will be compared to the original one in (Poljicak et al., 2011) under StirMark attacks (various signal and geometrical attacks), and finally under print-scan attack. For the latter case, two counterattacks deblurring and color correction recently proposed by (Riad et al., 2016) will be associated to the proposed method.

The paper is organized as follows: Section 2 describes the original Fourier watermarking scheme suitable for the proposed technique. Section 3 presents the method by first focusing on the theoretical justification and presents the principle of the two pre-processing enhancements. Section 4 shows the results. The final Section concludes the study.

2. FOURIER WATERMARKING

2.1 Embedding phase

The scheme presented by (Poljicak et al., 2011) is particularly interesting. A watermark W is embedded in the FFT magnitude along a circle of optimal radius r_0 while the phase is not modified. W is a white random sequence of 1 and -1 which is zero mean and unit variance. For grey level images, the FFT magnitude is that of the image. For color images, only the luminance image is watermarked while the other two chrominance components are unmodified. The circular watermark is inserted additively as follows:

$$X_W = X_0 + \alpha W, \tag{1}$$

where X_W are the watermarked FFT magnitudes along the circle of radius r_0, X_0 are the original ones, and α is the watermark strength.

In the case of a grey level image, the watermarked image is the inverse FFT of the watermarked FFT coefficients. In the case of color images, the color watermarked image is reconstructed by applying the inverse FFT to obtain the luminance of the watermarked image, from which the color image is recovered using the two unmodified chrominance components.

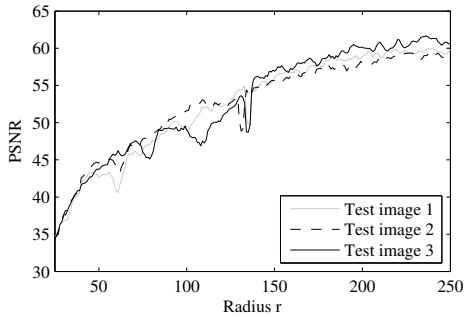

Fig. 2. Influence of the watermark radius r on the PSNR for three different images.

The embedding scheme depends on three parameters: The length of the watermark, the radius and the factor α that have an influence on the overall quality of the watermarked image. The quality of watermarked images is assessed using the Peak Signal to Noise Ratio (PSNR). Other quality metrics such as WPSNR in (Voloshynovskiy et al., 2000) or SSIM in (Wang et al., 2004) are often pointed out as more relevant as they take into account psychovisual concepts. In the proposed scheme, this consideration is not so useful. PSNR requires less complex computations, and is still considered to be a fair indicator to provide qualitative rank order scores in overall image.

Many experiments have shown that the radius and the factor α are essential. The length vector plays a secondary role. When the factor α and radius are fixed, the length vector produces a similar PSNR. The function $PSNR = f(l)$ can be assimilated to a constant with an added small Gaussian noise. The length vector is then not considered. It has been fixed to 180 elements, this is useful for the application and does not penalize the efficiency (Poljicak et al., 2011). The factor α and radius have a different influence on the overall quality of the watermarked image. The radius is extremely important as it is directly linked to the magnitude coefficient in the Fourier domain. A smaller radius leads to greater degradation of the image quality while a higher radius leads to a smaller degradation. Very high radii are not so interesting. It is well-known that the print scan attack in its simplest form can be considered as a low pass filtering in which the high frequency components of the cover image are attenuated. Then, appropriate radii are in a interval $[r_{min},\ r_{max}]$. The r_{min} value is easily estimated with the level of degradation, and the r_{max} one is estimated by analyzing the transfer function of the printer. Within this interval, there is a general rule to approximate the PSNR but for some radii the value is smaller, while for other radii it is bigger than expected as shown in Fig. 2.

Concerning the α factor, the PSNR decreases monotonously when α increases as shown in Fig. 3. For both parameters, the level of PSNR depends on the properties of the cover image. Then, the adopted strategy consists in finding r_0 to deduce α.

The optimal radius r_0 is estimated as follows: for a given watermarking strength α, the optimal radius corresponds to the maximum value of the PSNR. It is determined by calculating the PSNR for various radii in $[r_{min},\ r_{max}]$. The search for the optimal radius r_0 enables adaptation of the watermark for an individual image. Once r_0 has been estimated, α is chosen such that a given PSNR is reached. See Fig. 4 for a block diagram of the Fourier watermarking scheme.

2.2 Detection phase

Blind watermark detection is performed using the input image (that may be watermarked or not watermarked in the case of a malicious attack for example) and the watermark W. The principle of the detection process is as follows. The FFT is applied to the image grey level (or luminance). The FFT magnitude X_j of the image is extracted from a radius r_j in the interval $[r_{min},\ r_{max}]$. An estimation of the normalized cross-covariance at lag zero between X_j and W is computed:

$$\widehat{R}_{X_j,W}(0,j) = \frac{1}{N}\frac{\sum_{k=0}^{N-1}(X_j(k)-\widehat{\mu}_X)W(k)}{\sqrt{\widehat{\sigma}^2_{X_j}\widehat{\sigma}^2_W}}, \qquad (2)$$

N is the number of watermarked FFT magnitudes, $\widehat{\mu}$ is the estimator of the mean, and $\widehat{\sigma}^2$ is the unbiased variance estimator. Note that the image can suffer from a print-scan attack, *i.e.* rotation and translation may be present. In the Fourier domain, a translation does not modify the FFT magnitude. A rotation of the image results in a rotation of the FFT magnitude by the same angle. It is assumed here that the possible rotation angles fall between two angles $[\theta_{min},\ \theta_{max}]$. The cross-correlation between X_j and W is calculated for an angle θ_i in the interval $[\theta_{min},\ \theta_{max}]$ and for r_j in the interval $[r_{min},\ r_{max}]$:

$$\widehat{R}_{X_j,W}(i,j) = \frac{1}{N-i}\frac{\sum_{k=0}^{N-i-1}(X_j(k+i)-\widehat{\mu}_X)W(k)}{\sqrt{\widehat{\sigma}^2_{X_j}\widehat{\sigma}^2_W}}, \qquad (3)$$

R_{max}, the maximum of $\widehat{R}_{X_j,W}$ as a function of i and j is searched. If the image is watermarked, R_{max} is close to 1. Otherwise, R_{max} is close to zero. If R_{max} is greater than a predefined threshold T, the image is considered to be watermarked. Else, it is considered that the image is not watermarked. The predefined threshold T can be chosen to be the highest R_{max} of a non-watermarked set of images (Poljicak et al., 2011) or can be defined by using some theoretical model of the false positive behavior of the system as presented by (Lin et al., 2001) or by (Miller and Bloom, 2000).

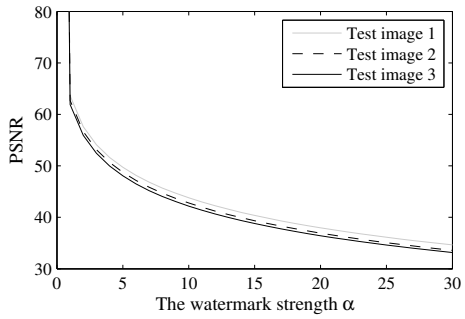

Fig. 3. Influence of the watermark strength α on the PSNR for three different images.

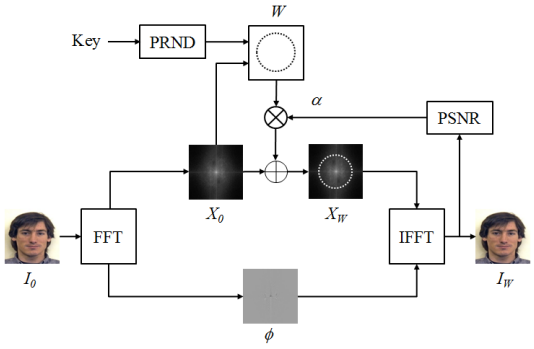

Fig. 4. Block diagram of the embedding process.

3. METHOD

3.1 Presentation

This paper is based on the concept of pre-processing the host vector (here the FFT magnitude of the image along a circle) before watermarking. The idea is to reduce the variance of the host vector to enhance the watermarking robustness. To illustrate this idea, Fig. 5 depicts the relationship between R_{max} and the host vector variance. This relationship was assessed from a set of 300 color identity (ID) images of 512 pixels selected randomly from (PICS, 2012) that were watermarked.

Fig. 5 shows that there is a large disparity in R_{max} as a function of the host vector variance. From this analysis, the idea of artificially reducing the variance of the host vector to enhance the performance of Fourier watermarking suggests itself. In that case, the total error rate will be reduced as explained in the following section.

3.2 Theoretical analysis

To estimate the evolution of the error rate when the variance of the host watermark vector X_j is modified, the probability density function (pdf) of R_{max} is of interest. Its derivation can be obtained from that of $\widehat{R}_{X_j,W}(i,j)$ using results in ordered statistics theory. Two cases have to be considered:

- No watermark in X_j (case 1),
- X_j is watermarked with W (case 2).

Case 1 corresponds to images that are not watermarked. It happens for example when a malicious person uses a false document containing a non watermarked picture. In this case, the pdf of R_{max} cannot evolve by an artificial

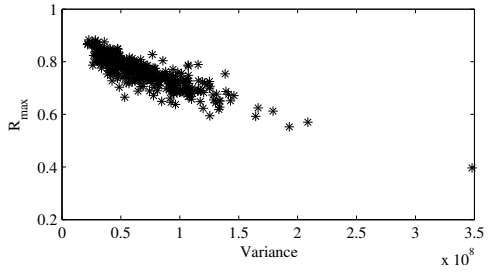

Fig. 5. R_{max} as a function of the variance of the host vector.

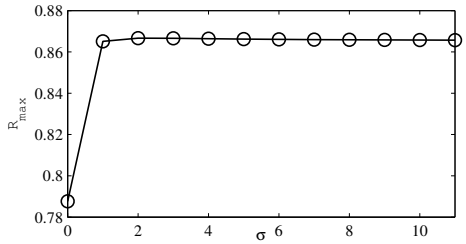

Fig. 6. The values of R_{max} for each σ of the Gaussian filter.

reduction of the host vector since the malicious person is not aware of the watermarking process. As a result, the pdf is a given curve that only depends on the image data set of interest (here identity images). For case 2, when the image is watermarked, the exact derivation of the pdf of R_{max} is a difficult issue since the pdf of X_j is unknown. Only an indirect result can be assessed. It is possible to estimate the expectation of $\widehat{R}_{X_j,W}(i,j)$. From Eq.3 one gets:

$$\mathbb{E}(\widehat{R}_{X_j,W}(i,j)) = \frac{Cov(X_j,W)}{\sqrt{\sigma^2_{X_j}\sigma^2_W}}, \tag{4}$$

where Cov is the covariance operator. Consider an image watermarked by W. The extracted vector can be written as $X_j = X_0 + \alpha W$, where X_0 is the host vector before watermarking. Recalling that $\mathbb{E}(W) = 0$ and $Var(W) = 1$, one obtains:

$$\mathbb{E}(\widehat{R}_{X_j,W}(i,j)) = \frac{\alpha}{\sqrt{\sigma^2_{X_0} + \alpha^2}}. \tag{5}$$

Equation 5, shows that decreasing the variance of the host vector when α is constant increases the mean of $\widehat{R}_{X_j,W}$ As a result the mean of R_{max} will also increase. The pdf of R_{max} for watermarked images will be subject to translations to the right as the variance of the host vector decreases (see section 4.1 for an illustration of this result).

The reason why the errors decrease when the variance of the FFT magnitude decreases is elucidated. Two such methods are proposed in the following.

3.3 Method 1

The first scheme to lower the variance of the host data is to apply a low pass filter. A centered Gaussian filter of standard deviation σ is chosen. During the embedding phase, it is necessary to determine the different parameters (α, r_0, σ) so that a given PSNR is reached. The algorithm comprises three steps as follows:

- Step 1: the optimal radius r_0 which maximizes the PSNR for a given α is determined by the process presented in paragraph 2.1.
- Step 2: the Gaussian filter is applied to the FFT magnitude along the circle of radius r_0. The σ parameter is increased and R_{max} quickly reaches a plateau value as shown in Fig. 6. The smallest value of σ on this plateau is chosen (one or two in practice).
- Step 3: the coefficient α is determined to obtain the desired PSNR.

The new embedding scheme is shown in Fig. 7. The detection of the mark is identical to that of the original method presented by (Poljicak et al., 2011).

3.4 Method 2

This scheme consists in selecting the FFT magnitudes between two circles of radii in the interval r_{min} and r_{max} located in the middle frequencies so that the total variance is as low as possible. The proposed algorithm is divided into 3 steps:

- Step 1: the mean of the FFT magnitudes that are located between two circles of radii r_{min} and r_{max} is calculated.
- Step 2: for each radial direction θ_i, the coefficient having the value closest to the mean value previously calculated is selected.
- Step 3: the coefficient α is determined to obtain the desired PSNR.

Fig. 8 shows the selected coefficients of the FFT magnitude of an image.

The watermark is inserted in the selected coefficients in an additive way. Fig. 9 shows the block diagram of the watermark embedding using the process via selection.

The detection of the watermark is more complex than the original method presented by (Poljicak et al., 2011). In addition to the watermark W, the input image, and the positions of the selected points must be known for each image.

Both methods share the same concept. The selection scheme is smarter but requires additional input to perform the detection. Then, the selection depends on the application context.

4. RESULTS

1000 ID images selected from (PICS, 2012) were scaled to 512 × 512 and watermarked using a constant PSNR of 40dB. This value corresponds to an invisible watermark (Poljicak et al., 2011). The watermark length is 180 elements. In the experiments three schemes were evaluated : the original Fourier watermarking presented by (Poljicak et al., 2011), the process via the Gaussian filtering, and finally the selection strategy. For the last scheme, the FFT magnitudes were located between radii in the interval [60, 120]. Note that all the methods are compared via the same referential. The watermarking strength has been

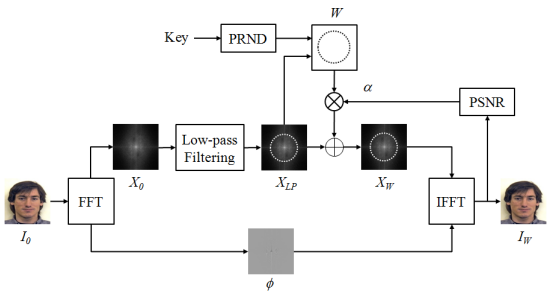

Fig. 7. Modified block diagram of the embedding process using the first method via filtering.

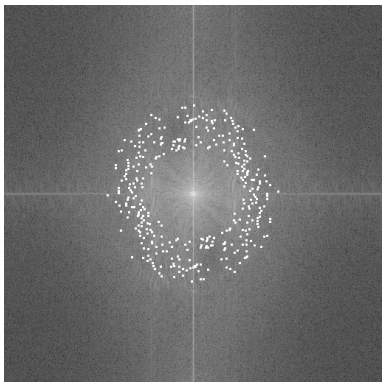

Fig. 8. Selected FFT magnitudes for embedding the watermark..

adapted so that obtaining a final constant PSNR of 40dB for all images and methods.

In a first step, preliminary results will be shown. They concern the two proposed methods compared to the original one in terms of pdf of R_{max}. Then, the three methods will be tested under StirMark attacks. Finally, they will be compared during a print-scan attack for an industrial application for smart plastic card supports.

4.1 Preliminary results

The pdf of R_{max} is plotted in Fig. 10 for case 1 (no watermark) and case 2 (watermark) using the three methods (original one presented by (Poljicak et al., 2011), process via filtering, and process via selection).

This method has been selected for all comparisons as it appears to be the most relevant competitor for our proposal. It is recent and popular but chiefly conceptually close to our approach as only a small set of selected bits in the DFT space are concerned by the watermarking process.

Results show that the pdf of R_{max} is subject to translations to the right while the variance of the host vector is reduced. As a result, errors will be lower when the variance of the host vector is reduced.

A comparison of the experimental results in terms of the true positive detection for various thresholds is presented in Fig. 11.

When the threshold values are low, the three methods give similar results. For higher threshold values, the schemes via filtering and process via selection proposed in this work

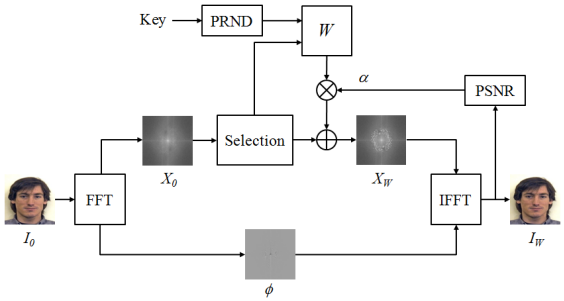

Fig. 9. Block diagram of the embedding process using the second scheme via selection.

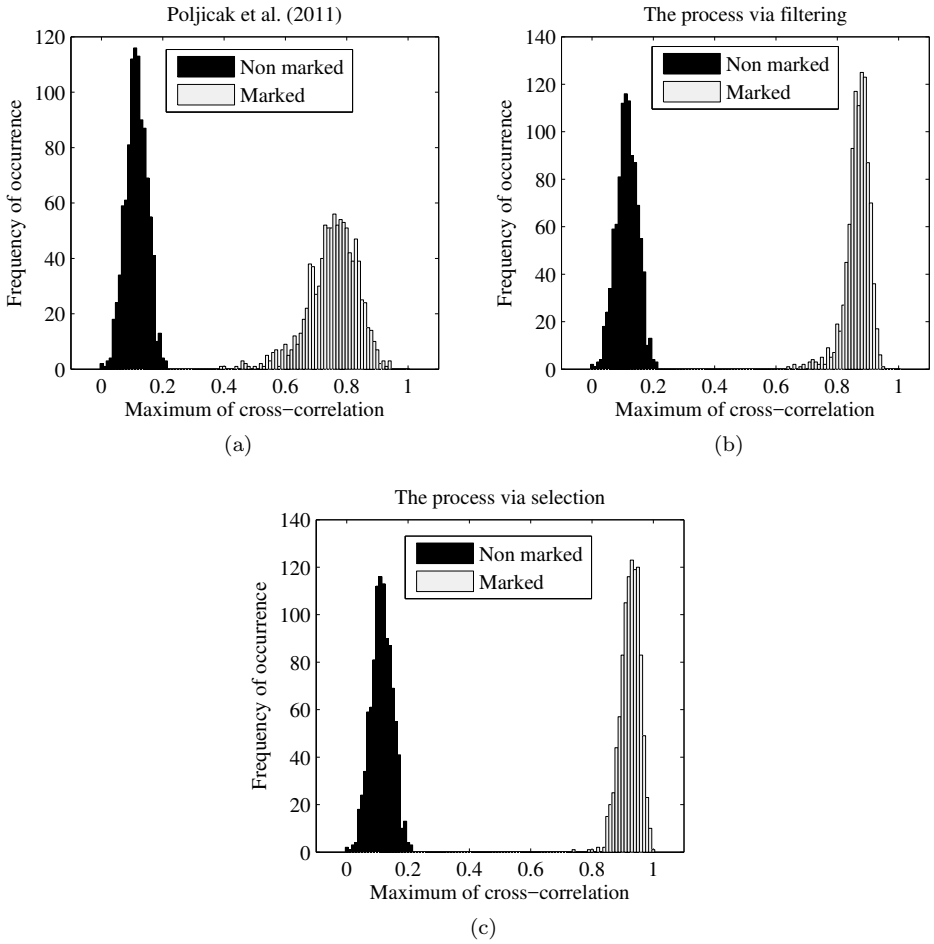

Fig. 10. Pdf of the R_{max} before attacks using three methods: (a) The method in (Poljicak et al., 2011), (b) the process via filtering, (c) the process via selection.

outperform the original method in (Poljicak et al., 2011). The best results are achieved by the scheme via selection.

4.2 Signal and geometrical attacks

Some StirMark attacks at different levels were applied. These attacks include JPEG-lossy compression, additive white Gaussian noise, median filtering and geometrical attacks. The performance of the method was measured and is plotted as ROC curves in Fig. 12 and Fig. 13.

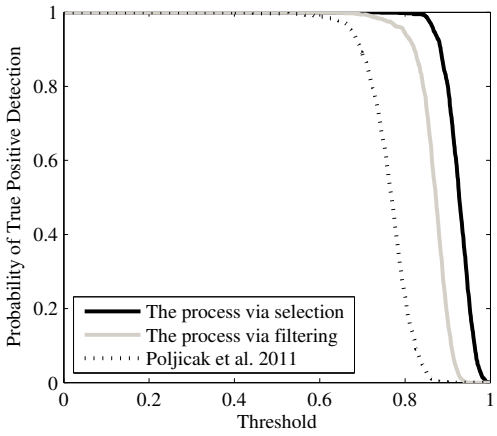

Fig. 11. True positive detection without attacks for various thresholds.

Fig. 12-a shows results for ID images under JPEG compression. As can be seen, the two proposed methods outperform the original one, the process via selection being the most efficient.

The robustness when applying a median filter and additive white Gaussian noise was assessed. Results are reported in Fig. 12-b for ID images under median filtering and in Fig. 12-c for noise addition. The same conclusions can be drawn.

Geometric attacks include the combination of the rotations and cropping. Results are reported in Fig. 13. The same conclusion is reached: the pre-processing scheme improves the efficiency of the original approach.

4.3 Comparison with other similar methods

In this test, the watermarked images are tested with selected attacks such as geometric attacks (rotation and cropping) and signal processing attacks (JPEG compression, Noise and median filter). To prove the effectiveness of the proposed methods, the robustness is compared with (Poljicak et al., 2011) and also with the method presented in (Solachidis and Pitas, 2001). This method is a reference in the watermarking field. The watermark is embedded in

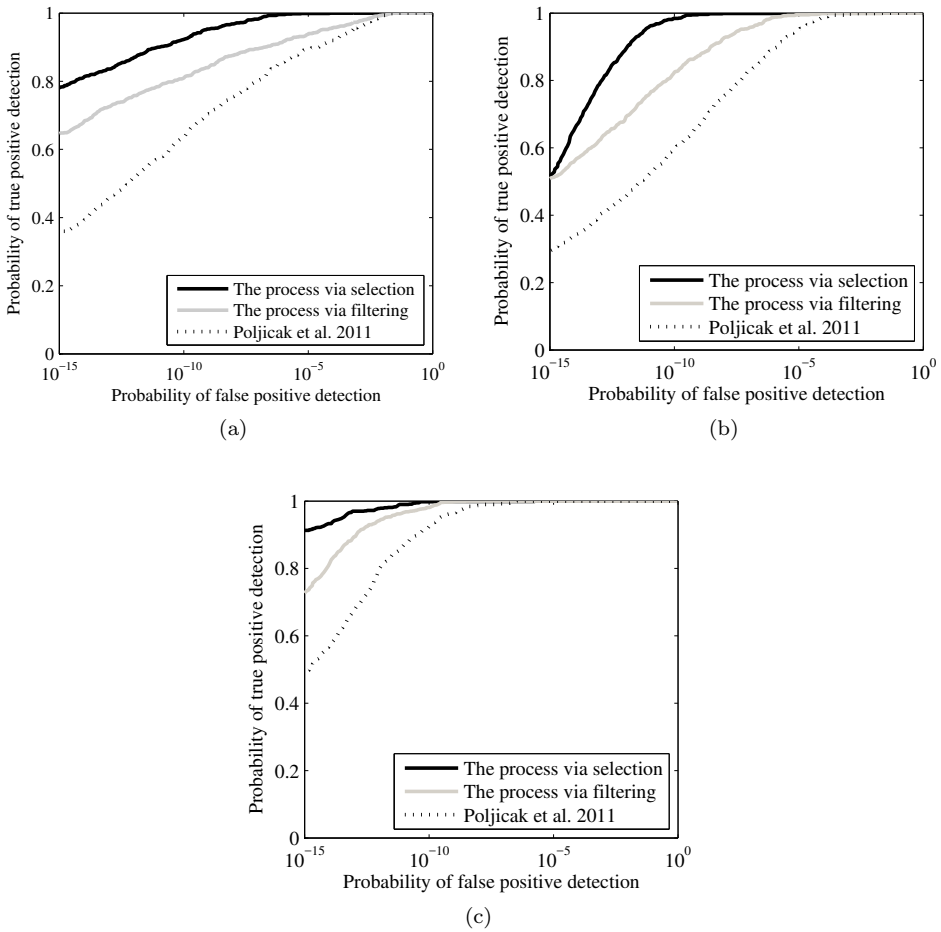

Fig. 12. ROC curves after attacks: (a) JPEG-lossy compression QF = 20%; (b) 7×7 Median filtering; (c) 10% Noise.

the DFT domain and consists of a 2-D circularly symmetric sequence. The comparison results are reported in terms of percentage of images for which correlation is higher than the predefined thresholds (detection rate). The threshold was fixed to $T = 0.323$, this threshold T was estimated using a theoretical model as described in (Lin et al., 2001) Results can be found in Table 1. Experimental results clearly show that our proposals are much better than all the others.

4.4 Security attacks

In addition, a security test was performed. This test shows the ability of the detector to discriminate between the correct key and wrong keys. 1000 keys including the one used for the embedding process (key = 300) were applied in the detection process. Results using random keys on a constant image are displayed in Fig. 14. The pre-processing scheme does not affect the level of security of the watermarking scheme. It even contributes to amplifying the discrimination between the correct and wrong keys.

4.5 Print-scan attack

An industrial application concerning smart card plastic supports is of interest. For this application, the process via selection was not chosen due to its complexity. Only the process via filtering will be compared to the original Fourier watermarking.

The same 1000 ID images as presented in section 4.1 were printed on a smart card plastic support with a surface of 86×54 mm^2. The industrial print and scan prototype was composed of a card printer Fargo Persona C25 with a printing resolution of 300 *dpi*. The size of the printed image on the plastic card was 20×20 mm^2. The scanner was an HP ScanJet with a scanning resolution of 300 *dpi*. Scanned images were resized to 512×512 pixels.

Fig. 15 presents the results of the original method in (Poljicak et al., 2011) and the proposed method using filtering. Note that a strong improvement in the detection rate is achieved in the case of the print-scan attack with the proposed method.

Finally, two counter-attacks were applied before detection of the watermark as presented by (Riad et al., 2016). They were composed of a dedicated Wiener filter to remove the blur of the print-scan process and a color correction. Results show that the combination of the proposed method and the counter-attacks provides substantial improvements.

Table 2 presents the detection rate for a fixed threshold $T = 0.323$. The detection rate was 70% for the original Fourier, and increased by more than 22% using the

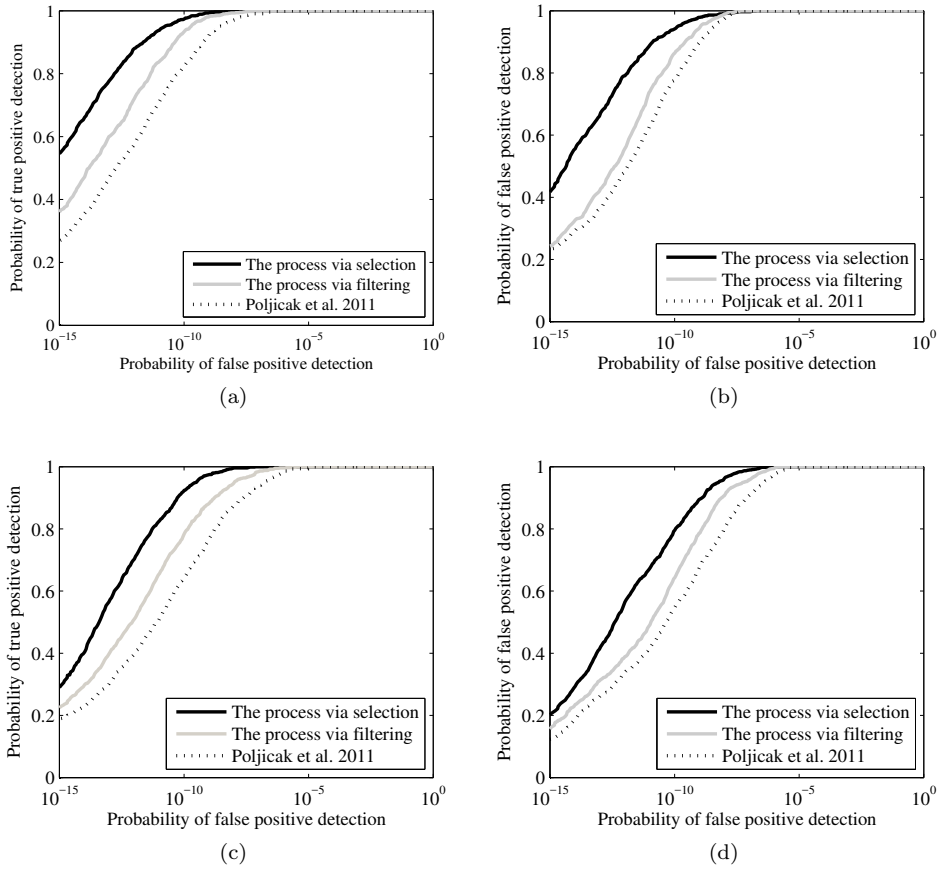

Fig. 13. ROC curves after the combination of rotation and cropping attacks: (a) Rotation 3°; (b) Rotation 5°; (c) Rotation 30°; (d) Rotation 45°.

Table 1. Detection rate (%) of the proposed method under processing and geometric attacks

	(Poljicak et al., 2011)	(Solachidis and Pitas, 2001)	Method via filtering	Method via selection
JPEG Compression	89.5	96	94	99.9
Median filter	95.1	93.9	99.5	100
Noise	91.2	92	98.4	99
Rotation & Cropping	95.7	93.1	97.8	99.9

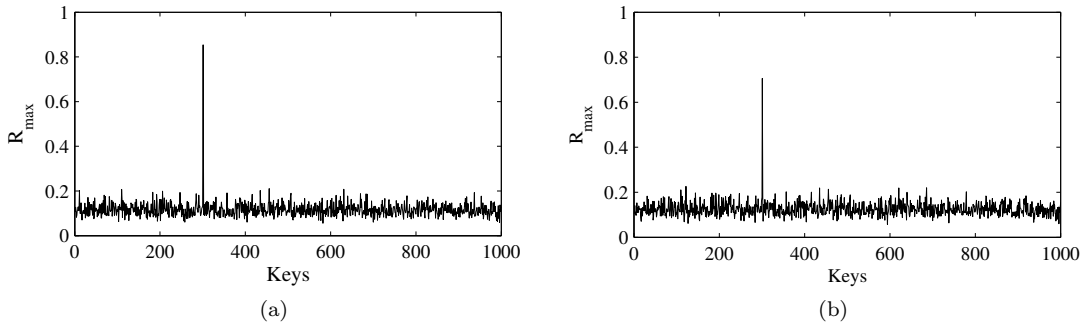

Fig. 14. The image was watermarked using the key associated with location 300 on the x-axis, where the R_{max} value is very high.(a) the image was watermarked using the pre-processing scheme, (b) the image was watermarked using (Poljicak et al., 2011)

proposed method via filtering. It rose to nearly 100% when counterattacks were used. Finally, the watermark detection took less than one second on an ordinary laptop computer.

5. CONCLUSION

This paper proposes an enhancement of Fourier image watermarking robustness. The idea consists in pre-processing the image before watermark embedding by decreasing the

Table 2. Detetion rate (%) of the proposed method under print-scan attack

	(Poljicak et al., 2011)	The proposed method	Proposed method + counterattacks in (Riad et al., 2016)
Detection Rate	70	92.83	99.89

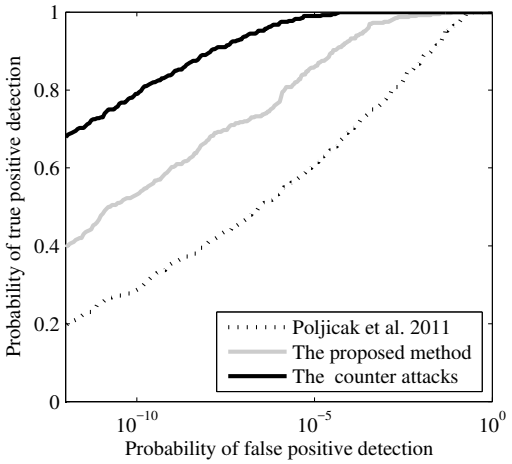

Fig. 15. ROC curves after print-scan attacks.

variance of the FFT magnitudes of the image. Results show that the proposed approach significantly enhances the original method. It leads to an average improvement of 22% in the detection rate within a print-scan attack. The detection rate rose to almost 100% when counterattacks were combined to the proposed method. The whole scheme is efficient and has a low computational cost making it compatible with industrial constraints.

REFERENCES

Amiri, S.H. and Jamzad, M. (2014). Robust watermarking against print and scan attack through efficient modeling algorithm. *Sig. Process.: Image Communication*, 29(10), 1181 – 1196. doi:10.1016/j.image.2014.07.004.

Cox, I., Miller, M., Bloom, J., Fridrich, J., and Kalker, T. (2007). *Digital watermarking and steganography*. Morgan Kaufmann.

Cox, I.J. and Miller, M.L. (2004). Facilitating watermark insertion by preprocessing media. *EURASIP J. Appl. Sig. Process.*, 2004, 2081–2092. doi: 10.1155/S1110865704403072.

Kang, X., Huang, J., and Zeng, W. (2010). Efficient general print-scanning resilient data hiding based on uniform log-polar mapping. *IEEE Trans. on Info. Forensics and Security*, 5(1), 1–12. doi: 10.1109/TIFS.2009.2039604.

Li, W., Zhang, Y., and Yang, C. (2013). A survey of jnd models in digital image watermarking. In *Inter. Conf. on Information Technology and Software Engineering*, volume 212, 765–774. doi:10.1007/978-3-642-34531-$9_8$1.

Lin, C.Y., Wu, M., Bloom, J., Cox, I.J., Miller, M., and Lui, Y.M. (2001). Rotation, scale, and translation resilient watermarking for images. *IEEE Tran. on Image Process.*, 10(5), 767–782. doi:10.1109/83.918569.

Miller, M.L. and Bloom, J.A. (2000). Computing the probability of false watermark detection. In *Information Hiding*, volume 1768, 146–158. doi:10.1007/$10719724_1$1.

Musrrat, A., Ahn, C.W., and Pant, M. (2014). A robust image watermarking technique using {SVD} and differential evolution in {DCT} domain. *Optik - Inter. J. for Light and Electron Optics*, 125(1), 428 – 434. doi: 10.1016/j.ijleo.2013.06.082.

Musrrat, A., Ahn, C.W., Pant, M., and Siarry, P. (2015). An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. *Information Sciences*, 301, 44 – 60. doi:10.1016/j.ins.2014.12.042.

Pan, I.H., Huang, P., and Chang, T.J. (2013). Dct-based watermarking for color images via two-dimensional linear discriminant analysis. In *Information Technology Convergence*, volume 253, 57–65. doi:10.1007/978-94-007-6996-0_7.

PICS (2012). Psychological image collection at stirling aberdeen. URL `pics.psych.stir.ac.uk`.

Poljicak, A., Mandic, L., and Agic, D. (2011). Discrete fourier transform based watermarking method with an optimal implementation radius. *J. of Electronic Imaging*, 20(3), 033008–033008–8. doi:10.1117/1.3609010.

Reed, A. and Bradley, B. (2005). Automatic pre-processing after image robustness analysis. In *IEEE Inter. Conf. on Image Processing, ICIP*, volume 1, I–957–60. doi: 10.1109/ICIP.2005.1529911.

Riad, R., Harba, R., Douzi, H., El-hajji, M., and Ros, F. (2014). Print-and-scan counterattacks for plastic card supports fourier watermarking. In *IEEE Inter. Symp. on Industrial Electronics, ISIE*, 1036–1041. doi: 10.1109/ISIE.2014.6864755.

Riad, R., Harba, R., Douzi, H., Ros, F., and Elhajji, M. (2016). Robust fourier watermarking for id images on smart card plastic supports. *Advances In Electrical and Computer Engineering*, 16(4), 23–30. doi: 10.4316/AECE.2016.04004.

Ros, F., Borla, J., Leclerc, F., Harba, R., and Launay, N. (2006). An industrial watermarking process for plastic card supports. In *IEEE Inter. Conf. on Industrial Technology, ICIT*, 2809–2814. doi:10.1109/ICIT.2006.372635.

Solachidis, V. and Pitas, L. (2001). Circularly symmetric watermark embedding in 2-d dft domain. *IEEE Tran. on Image Processing*, 10(11), 1741–1753. doi:10.1109/83.967401.

Valizadeh, A. and Wang, Z. (2012). An improved multiplicative spread spectrum embedding scheme for data hiding. *IEEE Tran. on Info. Forensics and Security*, 7(4), 1127–1143. doi:10.1109/TIFS.2012.2199312.

Voloshynovskiy, S.V., Pereira, S., Herrigel, A., Baumgartner, N., and Pun, T. (2000). Generalized watermarking attack based on watermark estimation and perceptual remodulation. volume 3971, 358–370. doi:10.1117/12.384990.

Wang, Z., Bovik, A., Sheikh, H., and Simoncelli, E. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE Tran. on Image Processing*, 13(4), 600–612. doi:10.1109/TIP.2003.819861.

Yu, L., Niu, X., and Sun, S. (2005). Print-and-scan model and the watermarking countermeasure. *Image and Vision Computing*, 23(9), 807 – 814. doi: 10.1016/j.imavis.2005.05.014.