A Print-Scan Resilient Watermarking based on Fourier Transform and Image Restoration

R. Riad
IRF-SIC, Ibn Zohr University, Agadir, Morocco

H. Douzi
IRF-SIC, Ibn Zohr University, Agadir, Morocco

M. El Hajji
IRF-SIC, Ibn Zohr University, Agadir, Morocco

R. Harba
PRISME, University of Orleans, Orléans, France

F. Ros
PRISME, University of Orleans, Orléans, France

ABSTRACT
The print-scan operation is still challenging in the watermarking community, some watermarking techniques were proposed in the literature to deal with this operation. These watermarking techniques are still very sensitive to degradations produced by the print-scan process. This paper investigates a watermarking technique in the Fourier domain that is robust to degradation produced when an image is printed in physical support then rescanned. The watermark is embedded in a middle frequency band of the discrete Fourier transform of an image using the improved spread spectrum technique. Some image restoration techniques were implemented. They were tested on images which were watermarked, printed and then rescanned before the watermark extraction. Experimental results clearly show the advantage of using the proposed approach.

Keywords
Watermarking, Fourier transformation, spread spectrum, print-scan, image restoration.

1. INTRODUCTION
Image watermarking may be used to verify the authenticity of identity documents where pictures are present. In [1], a watermarking process for plastic card supports was proposed. The image is first watermarked, and then printed on the plastic support. To check if the watermark is present in the image, the document must be scanned (see figure 1 for more details).The so-called print-san operation can strongly reduce the efficiency of the watermark extraction. The watermarks should be robust enough to survive to various attacks produced in the print-scan process. At the same time, the embedded watermark should not degrade the visual quality of the image. 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. Adapted strategies must be developed in that context.

The print-scan operation leads to a complex combination of different attacks, which produces various distortions. In [2], Lin and Chang separated these distortions into two main categories: geometric distortions and pixel value distortions. In the first case, those distortions consist in rotation, scaling and translation. In the second case, distortions are caused by luminance and color variations, contrast modifications, gamma correction, and blurring.

Several approaches that counterattack the general geometric distortions have been developed in the literature; such as invariant transform [3], template insertion [1], feature-based algorithms [4], autocorrelation based method [5], and circularly symmetric watermark embedding in the DFT domain [6]. For the pixel value distortions, experimental models of the print-scan channel were proposed in [7]. For simplicity, the print-scan attack can be modeled as a low pass filter plus an additive noise independent of the image. A natural idea to reduce pixel value distortions could be to use a deconvolution method before the watermark extraction or some enhancement filters [8].

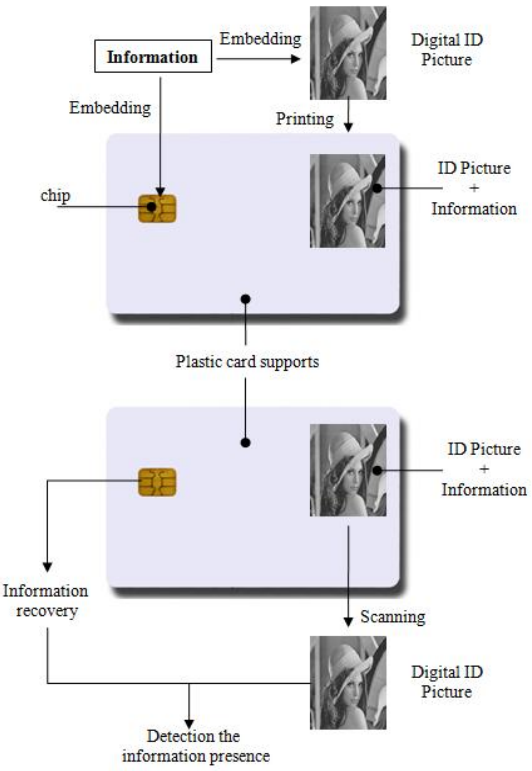

Fig 1: A possible scheme for securing smart card, insertion (top) and detection (below) of information in a smart card.

In this paper, the watermark is embedded in the Fourier domain using spread spectrum technique. Before the watermark extraction a preprocessing step based on image enhancement techniques were applied the print/rescanned images. This preprocessing has as goal to reduce image blurring that occurs during the print-scan process.

The paper is organized as follows: section 2 describes the chosen watermarking method. Section 3 presents the pretreatment method based on image deconvolution. Section 4 shows the experimental results. The conclusion and future works are described in the final section.

2. WATERMARKING METHOD

When print-scan operation is present, rotation and translation problems are one of the most severe attacks. The Fourier transform is used to embed the watermark because of its invariance to geometrical transformations. The magnitude of the Fourier transform is invariant to translation in the spatial domain, rotation in the spatial domain provide rotation in the Fourier domain by the same angle [9]. In this work, two watermark are inserted in the image, the first is the information to be inserted and the second is a synchronization template serve to calculate the rotation angle.

Several studies have focused on watermarking based on the Fourier transformation [1], [6], [10]. Solanki et al. [10] have investigated the effect of the print-scan operation on the coefficients of the Fourier transform magnitude; they concluded that the middle and low frequency coefficients are better preserved than the high frequency ones. If the watermark is inserted in the low frequency coefficients, there occurs a significant distortion of the image. For this reason, the watermark is generally inserted in the middle band of the Fourier transform [1], [6].

2.1 Embedding stage

First, the original image is transformed by the discrete Fourier transform (DFT) using FFT algorithm. Before the embedding process, the zero frequency point is shifted to the center of the DFT of the image. Then the watermark is inserted in a middle frequency band in the magnitude the DFT between two circles with radii R_1 and R_2. The watermark is embedded using an improved spread spectrum technique [11]. The proposed method consist to define J segments T in the middle frequencies as shown in figure 2. The j^{th} bit of the message is inserted redundantly in T_j.

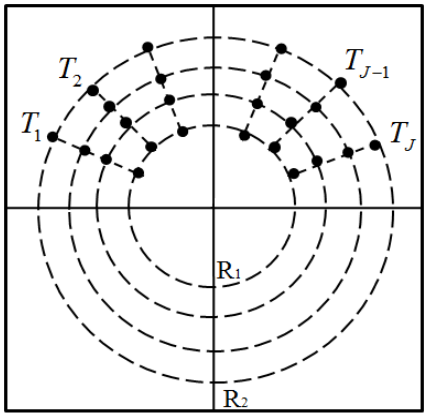

Fig 2: Embeddable positions in the DFT magnitude.

A secret key k is generated using a pseudo random number generator to produce a chip sequence u with zero mean and unit variance. The sequence u is added to, or subtracted from, the original segment T according to variable m_j, where m_j is +1 or -1, according to the bit (or bits) to be transmitted. The watermark embedding is performed using the improved spread spectrum as described in [12] by the following equation:

$$T_W = T + (\alpha m - \lambda \hat{T})u \qquad (1)$$

where $\hat{T} = < T, T >$ and T_W is the watermarked segment, α and λ control the robustness and imperceptibility of the watermark.

Then the synchronization template is embedded. This template contains no information but it serves to compute the rotation angel, the template consisted of a random sequence of peaks in the DFT magnitude embedded in circular way after the watermark embedding as shown in figure 3. Finally, the watermarked image is reconstructed by applying the inverse DFT to obtain the watermarked image.

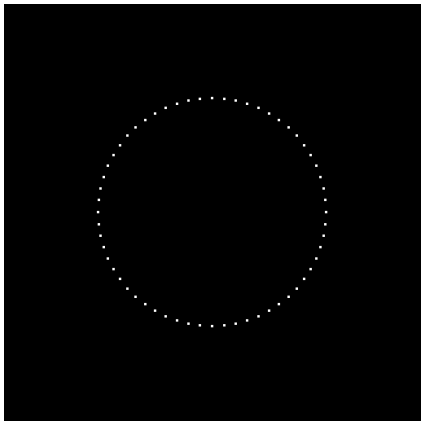

Fig 3: The synchronization template in the DFT magnitude.

2.2 Extraction stage

Blind watermark extraction is performed only using the watermarked image and the key k. The following steps describe the algorithm of the extraction process:

1. Apply the FFT algorithm to the watermarked image then shift the zero frequency point to the center of the DFT.
2. Estimate the angle of rotation using the cross-correlation between the inserted template coefficient and the random sequence of peaks, then apply the invers transformation to the magnitude of the DFT.
3. The secret key is used to generate the chip sequences u.
4. The message is extracted by computing the correlation factor of watermarked segments with the chip sequences u as following:

$$c = \frac{< T, u >}{< u, u >}, \qquad (2)$$

where < , > represents the scalar product. According to [11] the message is decoded by:

$$m^* = sign(c). \qquad (3)$$

3. IMAGE RESTORATION THECHNIQUES

This paper consider that the watermarked images are submitted only to print-scan attacks. These attacks can be separated into two categories of distortions [2]; geometric distortions and pixel value distortions. The important attack in the pixel value distortions is noise and blurring. According to [7] and [8], the print-scan attacks can be modeled in simpler form by a low-pass filter plus an additive noise independent of image pixels. The image g after print-scan process can be written in the spatial domain as:

$$g = f * h + b, \qquad (4)$$

where f is the original image, h is the low-pass filter representing the degradation produced during the print-scan process, b is the additive noise, and the symbol $*$ represents the convolution product.From the eq.4, the print-scan operation affect high frequency. To illustrate these phenomena, the spectrum of an image contains a uniform white noise before and after the print-scan operation are compared (see Figure 4); the DC frequency is shifted to the center position. This frequency analysis provides valuable information for setting the watermarking algorithm. It is possible to know the limit above which frequencies are attenuated. In addition, to achieve the best compromise between the watermark robustness and invisibility to the naked eye.

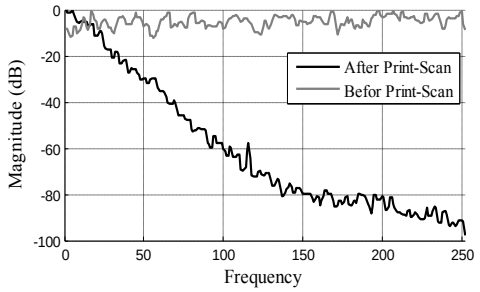

Fig 4: Frequency analysis of the print-scan process.

To counterattack the degradations produced during the print- and scan operation, a preprocessing step is applied before the watermark extraction. This technique allows applying an inverse procedure to recover an approximation $\hat{f}$ of the image f before the print-scan attack as shown in figure 5.

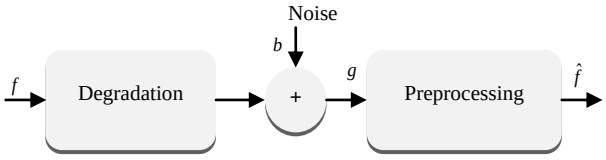

Fig 5: The model of the image degradation and preprocessing process.

Therefore, in order to reduce the degradation of a watermarked mage during the print-scan operation, some image restoration techniques should be used such as blind deconvolution and Unsharp filter [8]. Among different classical techniques used for image restoration, three filters were used in this paper: inverse filter, Wiener filter and Tikhonov-miller filter. The selected filters operate in the frequency domain, and are computationally less expensive than filters operating in the spatial domain. A blind deconvolution method will also be tested.

3.1 Inverse filter

In the frequency domain, the inverse filter is expressed as:

$$\hat{F} = \frac{G}{H} \tag{5}$$

where $\hat{F}$, G, and H are the Fourier transforms of the functions $\hat{f}$, g, h respectively.

3.2 Wiener filter

Image deconvolution by Wiener filter is expressed in the frequency domain by the following formula:

$$\hat{F} = G\frac{H^*}{|H|^2 + \frac{1}{SNR}} \tag{6}$$

where H^* is the complex conjugate of H and SNR is the known signal to noise ratio.

3.3 Tikhonov-Miller filter

The Tikhonov-Miller filter is formulated in the Fourier domain in this form:

$$\hat{F} = G\frac{H^*}{|H|^2 + \gamma|C|^2} \tag{7}$$

where γ is a parameter which must be carefully chosen, C is a high pass filter in the spectral domain. For the high pass filter the Laplacian operator id used.

3.4 Blind deconvolution

The performances of previous methods are based on a good knowledge of the estimation of the point spread function (PSF). In some cases, one cannot know these parameters with accuracy, and therefore using a blind deconvolution is of interest. This technique restores the image and the PSF simultaneously, using an iterative process based on the maximum likelihood algorithm.

4. RESULTS

The method was tested on four images (Peppers, Lena, Airplane and Mandrill) of 512×512 pixel by embedding a message of size 160 bits between two circles of radii R_1 = 64 and R_2 = 128. The quality of watermarked images was assessed using the peak signal-to-noise ratio (PSNR). It is define as:

$$PSNR = 10\log\left(\frac{255^2}{\frac{1}{M \cdot N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left\|I_W(i,j) - I(i,j)\right\|^2}\right) \tag{7}$$

where M and N are the dimensions of an image, i and j are the image coordinates, I_W is the watermarked image, and I is the original image.

Figure 6 shows a zoom of Lena image before and after watermarking; the quality of the watermarked image is about 40dB. Generally, if PSNR of watermarked image is about 40dB, the watermark is considered invisible [13].

(a) (b)

Fig 6: Zoom of Lena image (a), Zoom of watermarked Lena (b).

The Bit Error Rate (BER) between the extracted watermark and the original one was used to measure the robustness of watermarking algorithm; the bit error rates (BER) is the percentage of bits that have errors relative to the total number of bits detected.

Watermarked images were printed and scanned. The print-scan device is an HP LaserJet Pro 400 printer and an HP Scanjet 5550c scanner. Images were scanned with 300 dpi. Chosen deconvolution methods presented above were applied. Each filter is to be parameterized to be optimal. For the inverse filter, division by zeros, which greatly limits its effectiveness were avoided. The choice of the signal to noise ratio value for Wiener filter was done after several attempts to take the best value. This is also the case for the parameter lambda of Tikhonov-Miller filter. Results on the Lena image are presented in figure 7.

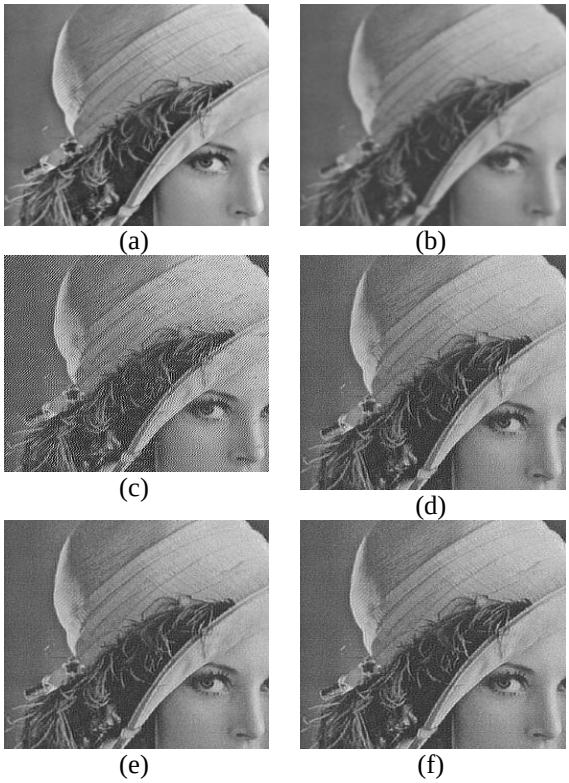

Fig 7: Zoom of Lena image (a) and after print-and-scan operation (b). Restored image by inverse filter (c), Wiener filter (d), Tikhonov-Miller Filter (e), Blind deconvolution (f).

Figure 7.a and present the Lena image, which was watermarked, then print-scanned in figure 7.b. Results of the deconvolution images are presented in figure 7.c for the invers filter, figure 6.d for the Wiener filter, figure 7.e for Tikhonov-Miller filter and figure 7.f for blind deconvolution.To assess the efficiency of the proposed methods, the BER of images after print-scan attack are presented in Table 1 and in Figure 8.

Table 1. BER after print-scan attack

Deconvolution techniques	Peppers	Lena	Airplane	Mandrill
Without deconvolution	0,06875	0,0375	0,0875	0,1
Inverse filter	0,075	0,0625	0,1125	0,1125
Wiener filter	0,04375	0,0125	0,05	0,0375
Tikhonov-Miller filter	0,0375	0,0125	0,0625	0,05
Blind deconvolution	0,06875	0,03125	0,08125	0,0875

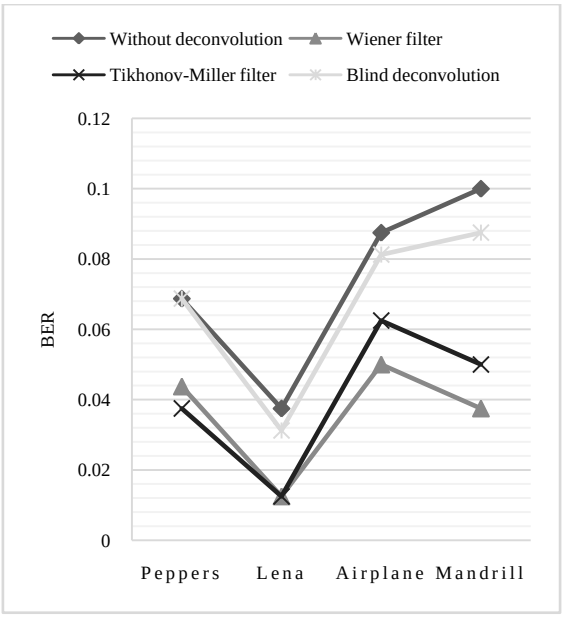

Fig 8: BER values for four test images after the print-scan attack.

Results show that, except for inverse filter, the BER significantly improved using the deconvolution techniques. The best correlation coefficient values are obtained with the Wiener filter and Tikhonov-Miller filter.

5. CONCLUSION

In the context of securing images such ID pictures printed on smart cards, an improved watermarking robust to print-scan attacks was presented. It is based on a pre-processing step before the extraction of the watermark. A watermarking technique based on Fourier transform was implemented. This transformation is characterized by its invariance by translation and rotation. The watermark is generated using the improved spread spectrum to ensure its robustness against noise. Classical deconvolutions were tested: Inverse filter, Wiener filter, Tikhonov-Miller filter and finally blind deconvolution. The results presented in this paper show that image deconvolution can significantly improve watermarking against print-scan attack. In this preliminary work, only the blur caused by the print-scan was corrected. In the future work techniques to correct the local geometric attacks is to be implemented.

6. REFERENCES

[1] F. Ros, J. Borla, F. Leclerc, R. Harba, and N. Launay, An industrial watermarking process for plastic card supports, in IEEE International Conference on Industrial Technology, ICIT, 2006, pp. 2809–2814.

[2] C. Y. Lin, and S. F. Chang, Distortion modeling and invariant extraction for digital image print-and-scan process. In Proceedings of International Symposium on Multimedia, 1999, December.

[3] J. Ouyang, G. Coatrieux, B. Chen, and H. Shu, Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping, Computers & Electrical Engineering, Available online 25 March 2015.

[4] J. S. Tsai, W. B. Huang, Y. H. Kuo, and M. F. Horng. Joint robustness and security enhancement for feature-based image watermarking using invariant feature

regions. Signal Processing, vol. 92, no.6, 2012, pp.1431-1445.

[5] M. J. Lee, K. S. Kim, T. W. Oh, H. Y. Lee, and, H. K. Lee. Improved watermark synchronization based on local autocorrelation function. Journal of Electronic Imaging, vol. 18, no.2, 2009, pp. 023008-023008.

[6] A. Poljicak, L. Mandic, and D. Agic, Discrete fourier transform based watermarking method with an optimal implementation radius, Journal of Electronic Imaging, vol. 20, no. 3, 2011, pp. 033008–033008–8.

[7] S. H. Amiri and M. Jamzad, Robust watermarking against print and scan attack through efficient modeling algorithm, Signal Processing: Image Communication, vol. 29, no. 10, 2014, pp. 1181-1196.

[8] A. Poljicak, L. Mandic, M. Strgar Kurecic, Improvement of the watermark detector performance using image enhancement filters, International Conference on Systems, Signals and Image Processing (IWSSIP), 11-13 April 2012, pp. 68-71.

[9] S. Pereira and T. Pun, Robust template matching for affine resistant image watermarks, IEEE Transactions on Image Processing, vol. 9, 2000, pp. 1123–1129.

[10] K. Solanki, U. Madhow, BS Manjunath, S. Chandrasekaran, and I. El-Khalil, Print and scan resilient data hiding in images, IEEE Trans. on Information Forensics and Security, vol. 1, no. 4, pp. 464–478, December 2006.

[11] H.S. Malvar and D. A. F. Florncio, Improved spread spectrum: A new modulation technique for robust watermarking, IEEE Trans. on Signal Processing, vol. 51, no. 4, pp. 898–905, April 2003.

[12] M. El Hajji, H. Douzi, R. Harba, and F. Ros, Improved Spread Spectrum Watermarking Based on Wavelet Dominant Coefficients, International Journal of Engineering and Industries, vol. 2, no. 3, 2011, pp.131-140.

[13] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing, vol. 90, no. 3, 2010, p.727-752.