Robust Fourier Watermarking for ID Images on Smart Card Plastic Supports

Rabia RIAD[1,2], Rachid HARBA[2], Hassan DOUZI[1], Frédéric ROS[2], Mohamed ELHAJJI[1]
[1]*IRF-SIC Laboratory, Ibn Zohr University, Agadir, Morocco*
[2]*PRISME Laboratory, University of Orléans, Orléans, France*
rabia.riad@etu.univ-orleans.fr

***Abstract*—Security checking can be improved by watermarking identity (ID) images printed on smart cards plastic supports. The major challenge is resistance to attacks: printing the images on the plastic cards, durability and other attacks then scanning the image from the plastic card. In this work, a robust watermarking technique is presented in this context. It is composed of three main mechanisms. The first is a watermarking algorithm based on the Fourier transform to cope with global geometric distortions. The second comprises a filter that reduces image blurring. The third attenuates color degradations. Experiments on 400 ID images show that the Wiener filter strongly improves the detection rate and outperforms competitive algorithms (blind deconvolution and unsharp filter). Color corrections also enhance the watermarking score. The whole scheme has a high efficiency and a low computational cost. It makes it compatible with the desired industrial constraints, i.e. the watermark is to be invisible, the error rate must be lower than 1%, and the detection of the mark should be fast and simple for the user.**

***Index Terms*—Fourier transform, printing, scanning, smart cards, watermarking.**

I. INTRODUCTION

Watermarking is considered as a rather young discipline that complements steganography and cryptography [1]. Watermarking can secure a medium such as a sound, an image, or a video. Concerning images, watermarking is achieved by inserting a permanent watermark in the image without any visible alteration. The key elements of image watermarking schemes are imperceptibility (humans cannot distinguish the difference between a watermarked and a non-watermarked image), robustness to attacks (ability to remain detectable when attacked), and finally capacity (amount of information that can be stored).

The choice of a watermarking scheme depends on its usage scenario. There is no ideal solution able to match all requirements with 100% efficiency while being fast, secure, imperceptible and robust. Several watermarking schemes have been proposed in the literature such as spatial methods [2], discrete cosine transform [3], discrete Fourier transform [4], discrete wavelets transform [5], and the content based method [6]. Spread spectrum is probably the oldest and most popular technique to embed the watermark [7]. Others exploit the characteristics of the human visual system in the watermarking process [8]. Watermarking technologies have evolved very quickly in recent years, as the demand through secure transmission channels is high. Applications of image watermarking are rapidly developing and among them security applications for smart cards. The major methodological advances were done in the 2000s [9].

A smart card often comprises a picture of the holder embedded on a plastic support, a text, a chip, and an interface to communicate with the outside world. Smart cards can be secured with a number of techniques. Some involve adding a physical security device to the object body such as holograms or bare codes. However, among all the innovative solutions available, watermarking appears to be one of the most attractive solutions due to its invisibility. The watermark may contain information regarding the validity of the document, the permissions attached to the document, or an indication of the document owner's identity. As a result, anyone unlawfully claiming to be its owner can be exposed.

This work is motivated by an industrial application of security checking for smart cards documents using watermarking. The ID image is watermarked, printed on the document and scanned in a second step by security services to assess the validity of the document. The so called print-and-scan attack occurs when the image is printed on the card and is scanned. Additional attacks like durability and other attacks are also present. Increasing the robustness to print-and-scan attack has concentrated most of research efforts because this attack is often the strongest one and is always present [10]. The print-and-scan attack includes global and local distortions such as geometrical attacks (rotation, translation, and cropping), and pixel value distortions (blur, noise and color distortions). After geometrical attacks, the synchronization between the extracted watermark and the embedded watermark is lost. Several synchronization schemes have been designed. The main ones are an exhaustive random search over the space containing the set of acceptable attack parameters [11], and embedding a template to estimate the affine geometric attacks in the image [12]. Even if these techniques are efficient, the Fourier based watermarking is often chosen due to its translation invariance and rotation property [4, 13]. It is easy to implement and does not need any additional embedded synchronization. The original Fourier watermarking consists in embedding the watermark in a circular way between two radii in the FFT magnitude [4] or along a single circle of optimal radius [13].

Concerning pixel value distortions, the print-and-scan process can be modeled by a linear filter plus an additive white Gaussian noise independent of the image. The filter attenuates the high-frequency components of the data. Enhancement filters such as unsharp filter and blind deconvolution were proposed in [14, 15]. The main difficulty is to design filters that are efficient. In our application scenario, the print-and-scan channel is known. A Wiener filter is an interesting alternative [16] as the impulse

Digital Object Identifier 10.4316/AECE.2016.04004

response and the signal to noise ratio of the print-and-scan channel can be assessed. Another possible improvement when the channel is known would be to correct color distortions that occur during the print-and-scan process.

This paper concerns the development of a robust Fourier watermarking method for ID images printed and scanned on a smart card plastic support. For the targeted industrial application, the print-and-scan channel is known because the card is produced by authorities with a given printer and digitized with a known scanner. The industrial constraint are as follows: the watermark is to be invisible, the error rate must be lower than 1%, and the watermark detection should be fast and simple for the user. The Fourier watermarking will be chosen because it is naturally adapted in the case of global geometric attacks occurring during the print-and-scan process [4, 13]. The Fourier domain has been proved for a long time to be the best space for the smart card application [10]. In recent years, different improvements have been proposed in the watermarking field [17-21]. Very little concerns our application problematic [10, 13]. Recent studies [3, 9] are multi-bits watermarking then not compliant with the application constraints. The involved techniques are also reputed to suffer from implementation issues [20] and additional computational costs [18-19], then not in line with our industrial constraints.

Two improvements will be developed to face the industrial challenge. The first concerns the reduction of image blurring. A Wiener filter will be proposed by taking into account the impulse response of the system and the noise variance that will be assessed on the print-and-scan channel. Wiener filter will be compared to unsharp filtering and blind deconvolution. The second counterattack consists in correcting color distortions using the estimated color transfer function. The efficiency of the method will be compared in the case of print-and-scan attacks occurring in the targeted industrial application. Finally, a series of degradations will be simulated to test the effects of durability and additional attacks of the proposed method.

The organization of the paper is the following: section II presents the method. Results are shown and discussed in section III. Finally the paper is concluded in section IV.

II. METHOD

In this work, the watermarking process of a colored ID image on a plastic support document is the following. The watermark is first embedded in the ID digital image and the image is printed on the plastic card document. When a given document is to be checked, (it could be a true or a false document), the ID image printed on the card is scanned and a decision is taken. Knowing the scanned image and the watermark, the binary decision is watermark present or watermark not present [10].

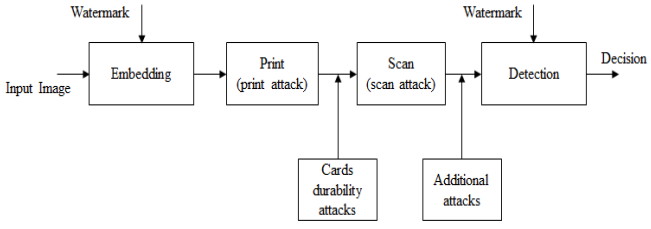


Figure 1. ID image watermarking process in the context of smart cards

As shown in Figure 1, the watermarked image is subject to print-and-scan attacks, to card durability attacks (attacks of the card during its lifetime). Additional attacks after scanning the image such noise related to the transmission channel or intentional attacks can also be present. All these attacks can lead to wrong decisions.

The print-and-scan attack includes pixel value distortions as well as global geometric attack (rotation and translation). Fourier watermarking was chosen, as it is naturally adapted to global geometric attack. In this section, Fourier watermarking will be first presented. Various attacks will be described, and finally the two counterattacks will be proposed.

A. Fourier watermarking

1) Watermark embedding

Fourier watermarking consists in embedding a watermark in the FFT magnitude of the image while the phase is not modified. Translation does not affect the FFT magnitude. Rotation in the spatial domain causes rotation of the Fourier domain by the same angle [12]. To be resistant to rotation, a circular watermark W (a pseudo-random sequence of L binary elements) is inserted between two radii in a redundant way [4]. Another solution consists in embedding the mark along one circle of optimal radius [13]. The one circle strategy is chosen here because of its simplicity and efficiency.

The watermark W is inserted along a unique circle of radius r in an additive way by using the following equation:

$$M_W(x,y) = M_0(x,y) + \alpha \times W(x,y), \quad (1)$$

where M_W is the watermarked FFT magnitude, M_0 is the original one, α is the strength parameter, and x and y are image coordinates in the frequency domain. For colored images, only the luminance is watermarked (chrominance components are not modified). Finally, the watermarked image is reconstructed by applying the inverse FFT to the watermarked magnitude and to the unmodified phase to obtain the luminance of the watermarked image, from which the colored image is recovered using the unmodified chrominance components.

The parameters that influence the quality of the watermarked image are the radius r, and the watermarking strength α. The choice of these parameters should be based on a quality indicator [13].

In many watermarking applications, the peak signal-to-noise ratio (PSNR) is used to evaluate the quality of the method [13] and is defined as:

$$PSNR_{[dB]} = log_{10}\left(\frac{255^2}{MSE}\right), \quad (2)$$

where MSE is the mean squared error between the original and the watermarked image.

PSNR values above 40dB indicate invisible degradation. Values below 30dB indicate high degradation [22]. For these reasons, a PSNR of 40dB was chosen here to watermark ID images, as it is mandatory that the watermark be invisible. It should be noted that other quality metrics [23] are often pointed out as more relevant than PSNR, the weighted peak signal-to-noise ratio (WPSNR) and the Structural Similarity Index Measure (SSIM) being the most popular ones. They often require too complex computations

for applications [24], and some limitations of these metrics for watermarking applications were also recently pointed out [25]. Moreover, in the proposed scheme, the watermark is spread over all the pixels of the image without taking into account psycho visual aspects, all of these justifying the PSNR indicator.

In the embedding process, an optimal radius r_0 was defined as in [13] and is estimated as follows: for a given α, the optimal radius corresponds to the maximal value of the PSNR resulting from an iterative search in a medium frequency interval. After this step, the implementation radius r being fixed to the previously found value r_0, the strength factor α is varied such that the targeted PSNR is reached. The optimal radius r_0 and the α are defined and the desired PSNR is reached. A simpler strategy is preferred here to deal with the required industrial constraints. The optimal radius for each image of a large set of ID images is first calculated. r_0, the mean of these optimal radiuses is estimated. The radius r_0 is taken to watermark any other image. r_0 being chosen, α was determined such that the final PSNR of 40dB is reached. The general scheme is shown in Figure 2.

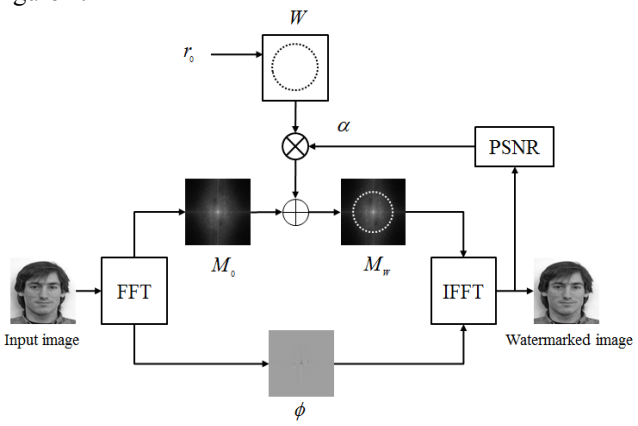


Figure 2. Block diagram of the embedding process using the Fourier transform

2) Watermark detection

Blind watermark detection is performed using the scanned image, the watermark W and the radius r_0. The FFT is first applied to the luminance image.

The FFT magnitude coefficients denoted M are extracted along the circle of radius r_0. The normalized cross-correlation is computed between the watermark W and M. During the print-and-scan process, rotation can occur. The maximum of the normalized cross-correlation $C_{\max}$ with respect to the rotation angle j is to be found:

$$C_{max} = \max_{-K \le j \le K} \left[\frac{\sum_{i=0}^{L-1} (W(i) - \bar{W})(M(i+j) - \bar{M})}{\sum_{i=0}^{L-1} (W(i) - \bar{W})^2 \sum_{i=0}^{L-1} (M(i) - \bar{M})^2} \right], \quad (3)$$

where L is the size of W and M, [-K, K] is the angular region where the maximum of the normalized cross-correlation is searched, $\bar{W}$ and $\bar{M}$ are the mean of the watermark and the mean of extracted coefficients, respectively. The watermark is present if the maximum value of the normalized cross-correlation exceeds a predefined threshold t, otherwise the watermark is not present, providing a binary decision. Figure 3 shows the principle of the detection process.

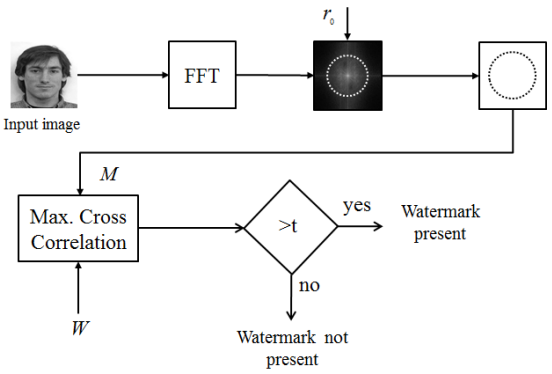


Figure 3. Block diagram of the detection process using the Fourier transform

The threshold t results from the following analysis. It requires the use of a theoretical model of the false positive behavior of the watermarking system. Assuming that the vector extracted from non-watermarked images is drawn from a radially symmetric distribution, the probability of false positive is as follows [26]:

$$Pf\{C > t\} = \frac{\int_0^{\cos^{-1}(t)} \sin^{L-1}(u)du}{2\int_0^{\pi/2} \sin^{L-1}(u)du}, \quad (4)$$

where Pf is the probability of false positive detection for a given threshold t, C is the correlation coefficient value and L is the watermark vector dimension.

When the detection measure is the maximum of the cross-correlation value, this formula has been adapted in [27], as:

$$Pf\{C_{max} > t\} = min(1, 2 \times K \times Pf\{C > t\}), \quad (5)$$

where C_{max} is the maximum of the normalized cross-correlation obtained from the decoder on non-watermarked images, K represent the half length of the angular region where the maximum of the cross-correlation is searched.

B. Card attacks

These attacks are the print-and-scan attack, the card durability attacks, and finally additional attacks.

1) Print-and-scan attacks

These attacks appear during both the printing and the scanning operations. In [28], Lin *et al.* separated the distortions of the print-and-scan process into two categories: pixel value distortions and geometric distortions due to the card placement in the scanner, for example. Geometric distortions are avoided by the chosen watermarking technique.

For pixel value distortions, several models were proposed in the literature [5, 29]. The print-and-scan model can be divided into two blocks: a low pass linear filter plus an additive noise on one hand, and color distortions, on the other hand.

For the first block, let I_0 be the original image. The output image (printed and scanned) I is given by:

$$I = h * I_0 + n, \quad (6)$$

where h is the impulse response of both the printer and scanner, the symbol * stands for the convolution product, and n is a zero-mean white Gaussian noise of unknown variance and independent of the image.

Color distortions can be modeled as a nonlinear function between the input and output color level in a given color space.

2) Card durability attacks

Most ID card personalization features such as photos, text, logos, or bar code are regularly exposed to a variety of potentially destructive elements that can degrade printed images. Essentially, secure documents must not be altered through the ID document lifetime, which can be up to 10 years. ID documents also promote the image of the issuing authority and it is important that the document does not need to be reissued before its expected expiry date. There are many kinds of durability attacks such as color fading, dust, and scratches. All these attacks appear during the authentication of the ID card and may prevent detection of the watermark.

In [30], a series of attacks was established to simulate these aggressions and attest to the robustness of the card. The author divided the card durability attack in two categories: mechanical and photometrical.

The first mechanical degradation of card durability is the number of times the card is inserted into a reader. This can result in persistent bending or flexing of the card, leading to the characteristic "barrel" shape. The barrel distortion model is described by the following equation:

$$a_d = a_u(1 + k \times a_u^2), \tag{7}$$

where a_d and a_u are radial distances in the distorted and in the undistorted image respectively, and k is the distortion parameter.

The card and ID image will also suffer from dust, scratches, or shocks due to the non-protected use of the card. This kind of attack can be simulated by:

- Adding an impulse noise to simulate dust;
- Adding lines randomly in the image to simulate scratches. It is not possible to simulate all the dimensions, sizes, and orientations of image scratches. That is why various vertical/horizontal lines will be drawn randomly on the image in order to simulate this kind of deterioration;
- Removing random parts from the images to simulate shocks. A square of $N \times N$ pixels will be removed in the image. This will be performed with different sizes and at different geometrical positions.

Color fading occurs when the card is exposed to sunlight for a long time. This degradation consists in a loss of color density, which introduces a decrease in saturation of ID images. This degradation can be delayed by different means (e.g. film UV protection on the image), but there will always be a color change. The simulation of color fading consists in converting the image from RGB (Red Green Blue) to Hue Saturation Intensity color space, then decreasing the saturation value, and converting the image back to the RGB color space.

3) Additional attacks

Images can be subject to additional attacks that take place between the scan and the decision (see Figure 1). These attacks can be unintentional attacks such as JPEG compression, or additive Gaussian noise. They occur for example if the image has to be transmitted through a channel before decision. Some can be malicious attacks such as the overmarking. The latter consists in embedding another watermark in the scanned images. Other attacks also exist but only the above-mentioned ones will be evaluated in this work.

C. Counterattacks

The best defense regarding these attacks is to correct their effects before the detection stage. These preventive defenses are called counterattacks. The print-and-scan attack is often the most aggressive one and is always present. Other attacks are difficult to correct preventively since they are not always present. In this work, a print-and-scan counterattack is proposed, which involves reducing the blur effects and correcting color variations.

In [15] an unsharp filter was used before the watermark detection to correct the blur that occurs during the print-and-scan attack. In [14], degraded images were enhanced using unsharp, Laplacian and blind deconvolution filters. Here, the Wiener filter can also be tested. The Wiener filter is expressed in the frequency domain by:

$$\hat{F} = F \frac{H^*}{H^* H + \frac{1}{SNR}}, \tag{8}$$

H represents the Fourier transform of h, the impulse response of the system. H^* is the complex conjugate of H, F and $\hat{F}$ are the Fourier transforms of the degraded and corrected images, respectively. The SNR (signal to noise ratio) is equal to P/P_n, with P_n and P the power of the noise n and the power of the image, respectively.

The second step of the counterattack consists in a color correction. The color correction process chosen here is presented in Figure 4, where RGB are original color values, $R'G'B'$ are color values after print-and-scan and $R^*G^*B^*$ are the color values of the corrected image. The 1D look up tables (LUT) in Figure 4 are the inverse of the color responses of the system for R, G and B, respectively.

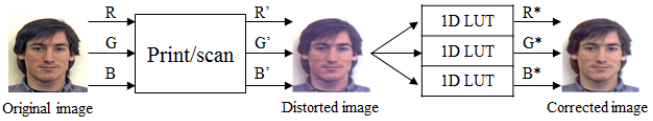


Figure 4. Color distortions produced during the print-and scan process and the proposed color correction

For the industrial application studied in this paper, the print-and-scan channel is known. Indeed, secure ID documents are printed and scanned only by authorized secure system. As results, parameters used in the Wiener filter, h and the noise variance can be measured. The look up tables used for color correction also can be assessed.

III. Results

Experiments were carried out on colored ID images extracted from the Psychological Image Collection at Stirling. Images were scaled to 512×512 pixels, and printed on a plastic card support with a surface of 86×54mm^2 and a thickness of 0.76 mm. The industrial print-and-scan prototype was composed of a card printer Fargo Persona C25 with a printing resolution of 300dpi. The size of the printed image on the plastic card was 20×20 mm^2. The scanner was an HP ScanJet with 300dpi. Scanned images were resized to 512×512 pixels. Figure 5, shows a picture extracted from the database before and after the print-and-scan operation.

(a) (b)

Figure 5. Sample from the database before (a) and after (b) the print-and-scan process

Degradations due to the print-and-scan are clearly visible and must be corrected to enhance the watermarking performances.

The first part of this section concerns preliminary results. The parameters of the Fourier watermarking will be chosen. Then, the PSF (Point Spread Function, or impulse response), the noise variance and the color transfer function of the print-and-scan channel will be estimated from the experimental bench described above.

The second part of the Results section concerns the comparison of the various deblurring methods facing the print-and-scan attacks, the best method will be chosen. The effects of the color correction will be analyzed later. Finally, additional results concerning the card durability and additional attacks will be shown.

A. Preliminary results

1) Design of the Fourier watermarking method

A set of 100 ID images was extracted from the Psychological Image Collection at Stirling database. The optimal radius, i.e. which maximizes the PSNR, was searched in the interval [60; 80] for each image. The mean of these radii was calculated and was found to be 64. This value is therefore the constant radius r_0 that will be chosen for every other image. The watermark size is fixed at 180 elements and the strength factor α is chosen for each image such that the PSNR is 40dB (see Figure 2). It was experimentally observed that the angle of rotation that occurs during the print-scan attack are between ±10 degrees. It corresponds to $K = 10$ (see Equation (3) and (5)).

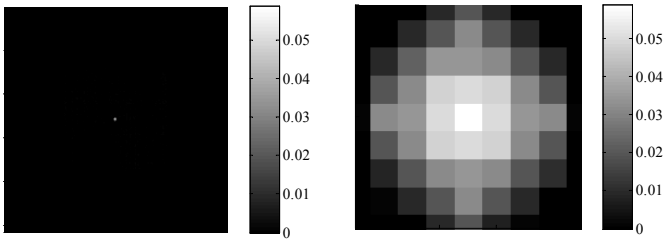
2) Estimation of the PSF

The PSF takes into account diffractions and aberrations of the optical system in measurement conditions. The PSF was assessed by estimating the cross correlation of a white noise input image with that of the same image printed and scanned. Cross correlation is one of the most commonly used methods to estimate the impulse response of systems such as a wireless communication channel for example [31].

Let N_{in} be the $M \times M$ array of the original noise and N_{out} be array obtained after the print-scan process. The estimated PSF is the cross correlation between the output N_{in} and the input N_{out}:

$$\hat{h}(i,j) = \frac{1}{(M-i)(M-j)} \sum_{m=0}^{M-i-1} \sum_{n=0}^{M-j-1} N_{in}(m,n) N_{out}(m+i,n+j). \quad (9)$$

The final estimation of the PSF is the average over 10 such experiments. Results are shown in Figure 6.



(a) (b)

Figure 6. Estimated PSF (a) and zoom (b)

3) Estimation of the noise variance

As described in [32], two sources of noise are usually considered in image acquisition. The first one corresponds to the stochastic nature of the photon-counting process in the detector. The second corresponds to the intrinsic thermal and electronic fluctuations of the acquisition device. The second source of noise, which is independent for each pixel and independent of the signal intensity, is stronger than the first one. This motivates the usual additive white Gaussian noise (AWGN) assumption.

To determine the noise in the print-and-scan channel, it is assumed to be an AWGN independent from the image. Several methods are proposed in the literature to estimate the noise variance [33]. In this work, 256 images with uniform gray levels varying from zero to 255 were printed and scanned. Image variance was computed for each gray level image. The noise variance of the print-and-scan channel is the mean of all gray levels variance of the 256 uniform images and is equal to 2.13.

4) Inverse color transfer function estimation

This color transfer function is converting the color levels of an original pixel to the color levels of the printed and scanned pixel. This transfer function includes gamma correction, contrast variation and color distortions. To compute the color transfer function, 256 colors were chosen to be representative of the colors in ID images, especially skin and hair colors. A total of 256 rectangular regions with the 256 chosen color levels were printed and scanned as shown in Figure 7.

(a) (b)

Figure 7. Color template before (a) and after (b) print-and-scan

After scanning, the mean of each region of color components in the RGB color space was computed. Finally, the inverse transfer function of the RGB components was estimated using a 4-order polynomial curve and is shown in Figure 8. It is also the 1D LUT presented in Figure 4.

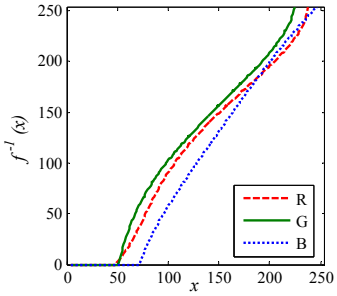


Figure 8. Inverse transfer functions for each color component

B. Results: print-and-scan attack

A set of 400 ID images was extracted from the Psychological Image Collection at Stirling database. The same set of 400 images was watermarked. This set of 800 ID images were printed and scanned using the experimental bench. The maximum of the normalized cross-correlations of the 800 ID images are computed. The histograms are shown in Figure 9 before and after the print-and-scan attack for watermarked and non-watermarked images.

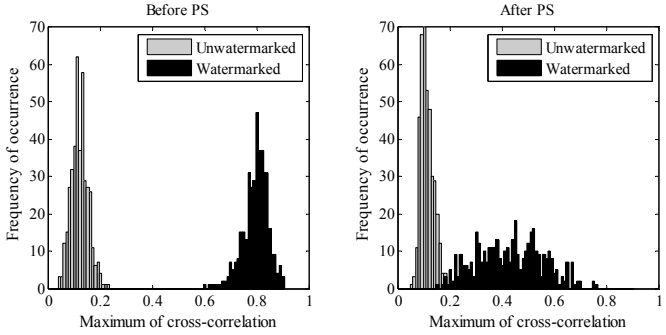


Figure 9. Normalized cross-correlation before (a) and after (b) the print-and-scan process (PS)

It appears that the print-and-scan operation has little influence on the histogram of the maximum of the cross-correlation of non-watermarked images. At the opposite, it has a significant impact on that of the maximum of cross-correlation for watermarked images, which moves left side and spread. As a result, the histograms of watermarked and non watermarked printed and scanned images now overlap. Therefore, wrong decisions will occur. It is expected that the proposed counterattacks will reduce the occurrence of the errors.

Wiener filter, unsharp filter and blind deconvolution were applied to the printed and scanned images, and the same test was run. The estimated PSF is used as initialization of the blind deconvolution. Results are shown in Figure 10. The comparison of Figure 9 and Figure 10 clearly show that the three deblurring methods improves the watermark detection as the overlap between the histogram of watermarked and non watermarked images is reduced. To better analyze the results, ROC curves are presented in Figure 11. ROC curves show that the Wiener filter is the most efficient one when compared to unsharp filter [15] or blind deconvolution [14]. The Wiener filter is therefore chosen.

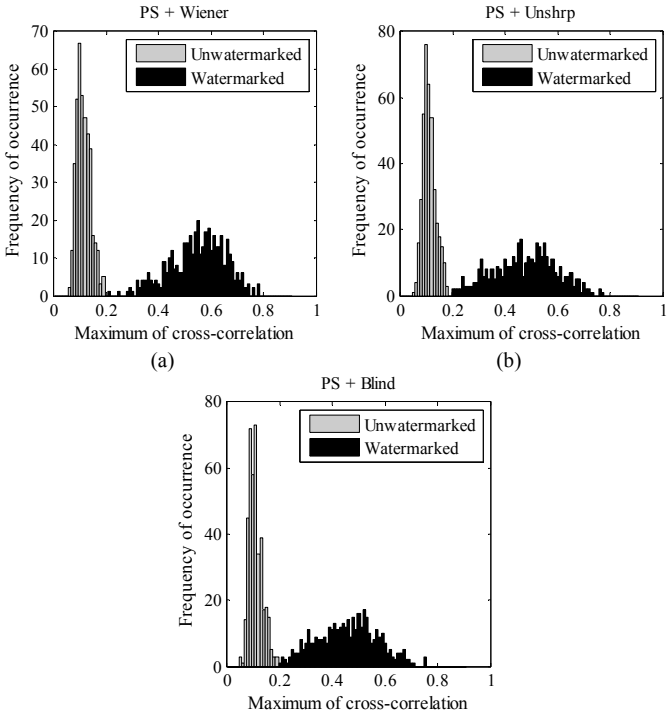


Figure 10. Normalized cross-correlation for the three deblurring methods (Wiener (a), Blind (b) and Unsharp (c))

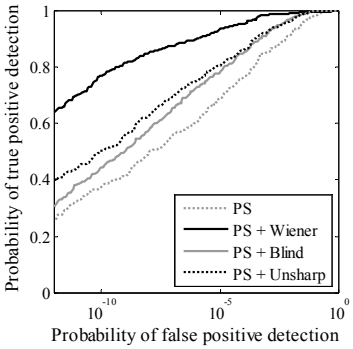


Figure 11. Comparison of ROC curves before and after blur corrections

The second step of the proposed counterattack consists in a color correction. A color corrected image is shown in Figure 12. Results are of high quality especially in the hair and skin regions. Figure 13 presents the ROC curves where the color correction was included.

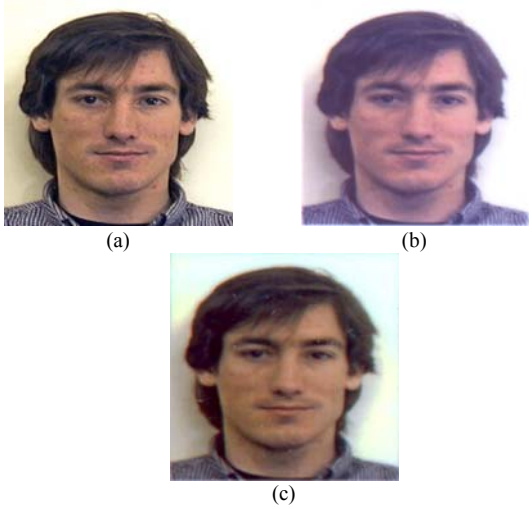


Figure 12. Results of color correction, original image (a), printed/scanned image (b) and Color-corrected (c)

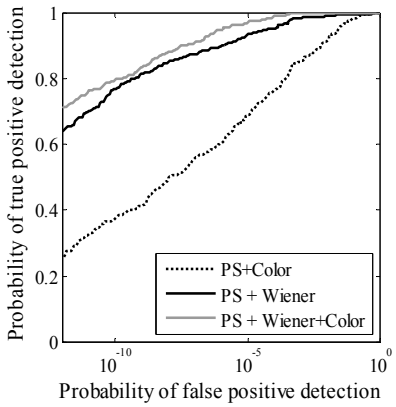


Figure 13. Comparison of ROC curves before and after the counterattack

It is seen that the blur correction alone has more effects than the color correction alone. When they are combined, results are of high quality. The total errors are to be estimated. For the application considered here, the total error rate must be lower than 1%. For that reason, a false positive error of 10^{-4} was chosen. It corresponds to a detection threshold $t = 0.323$ (see Equation (5)). The false negative error is of 0.75% when the Wiener filter and color correction are combined. The total error is of 0.76%. It is lower than the 1% that was required. These results lead to the final structure of the robust watermarking. The one-circle Fourier watermarking is chosen with $r_0 = 64$, the PSNR is 40dB, and the counterattacks are composed of a Wiener filter associated to a color correction as described above. Figure 14 shows the defined method for which the watermark is invisible and the error rate is lower than 1% for ID images printed on a smart card plastic supports.

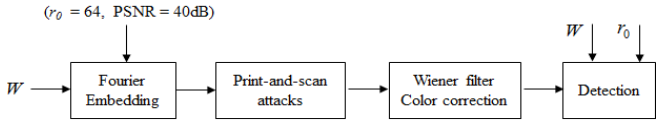


Figure 14. Robust watermarking process in the context of ID images on plastic cards supports

C. *Additional results: card durability attacks*

The robustness of the proposed method to card durability attacks was assessed. Some of the durability attacks employed in the present study were very strong, as shown in Figure 15. Adding 16 random lines to the images, (Fig.15-c) corresponds to a deterioration, which is not acceptable for the ID document. In this case, the ID document must be reissued. The aim of these tests was to reach the limit of the proposed method against extreme card usage conditions.

The results are listed in Table I. First, no counterattack is present, and in a second step, the counterattacks (Wiener filter + color corrections) are used. Results are given in term of the detection rate.

It can be seen that, in general, card durability attacks have severe effects. Counterattacks increase the detection rate. The proposed method is very sensitive to noise.

Figure 15. Example of card durability attacks applied after print-and scan process, image before attacks (a), impulse noise (b), 16 lines added (c), 5% removed from the image (d)

TABLE I. DETECTION RATE AFTER CARD DURABILITY ATTACKS

Bending	**k = 0.01**	**k = 0.03**		**k = 0.05**
No counterattack	87.25%	86.12%		81.5%
With counterattacks	98.25%	96.87%		91.87%
Impulse noise	**1%**		**2%**	
No counterattack	79.25% (80.87%)		76.37% (80.62%)	
With counterattacks	74.87% (97.75%)		72.12% (96.12%)	
Lines added	**2**	**4**	**8**	**16**
No counterattack	88.25%	87.87%	84.37%	81.25%
With counterattacks	98.5%	96.87%	89.87%	87.62%
Part removed from image	**1%**	**3%**		**5%**
No counterattack	87.5%	86.87%		82.5%
With counterattacks	98.87%	98.25%		97.62%
Color fading	**20%**	**50%**	**80%**	**100%**
No counterattack	88.5%	87.12%	85.25%	83%
With counterattacks	99.15%	98.75%	95.25%	90.37%

This can be explained by the fact that image deconvolution increases the high frequencies corresponding to noise. A median filter applied before the watermark detection improves the detection rates as shown in the results between brackets in Table I.

Additional attacks (JPEG compression, noise and the overmarking) were also studied and results are reported in Table II. The same conclusions as previously can be drawn.

TABLE II. DETECTION RATE AFTER ADDITIONAL ATTACKS

JEPG compression	**80**	**60**	**40**
No counterattack	85.37%	84.37%	75.62%
With counterattacks	98.62%	97.37%	90.12%
AGWN	**σ = 3**	**σ = 5**	**σ = 7**
No counterattack	87%	84.62%	82.12%
With counterattacks	98.25%	90%	81.12%
Overmarking	**40dB**	**35dB**	**30dB**
No counterattack	86.5%	84%	82.75%
With counterattacks	97.75%	90.37%	82.12%

An indication of the calculation time can be given. The whole Fourier based detection scheme including corrections takes less than one second using an ordinary laptop computer. The computational cost of the proposed method is acceptable for the use in the given industrial context.

IV. Conclusion

This paper has proposed a robust Fourier watermarking for ID images on smart plastic card supports. It consists of combining Fourier watermarking with a Wiener filter followed by a color correction. These counterattacks are applied to images before watermark detection. Results on 400 ID images show that the proposed method is robust, simple and fast. It reaches the targeted industrial objectives, i.e. an invisible mark, an error rate lower than 1% and fast. Further work will concern the use of a psycho-visual mask that could improve the quality of the detection. In addition, in the near future, the print-cam attack will be considered.

Acknowledgment

This work is supported by the Franco-Moroccan Volubilis 2697WA project and by the GEMALTO COSEC ID EU project.

References

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography: Morgan Kaufmann, 2007.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM systems journal, vol. 35, pp. 313-336, 1996. doi:10.1147/sj.353.0313.

[3] A. Poljicak, G. Botella, C. Garcia, L. Kedmenec, and M. Prieto-Matias, "Portable real-time DCT-based steganography using OpenCL," Journal of Real-Time Image Processing, pp. 1-13, 2016. doi:10.1007/s11554-016-0616-9.

[4] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," IEEE Transactions on Image Processing, vol. 10, pp. 1741-1753, 2001. doi:10.1109/83.967401.

[5] S. H. Amiri and M. Jamzad, "Robust watermarking against print and scan attack through efficient modeling algorithm," Signal Processing: Image Communication, vol. 29, pp. 1181-1196, 2014. doi:10.1016/j.image.2014.07.004.

[6] P. Bas, J.-M. Chassery, and B. Macq, "Image watermarking: an evolution to content based approaches," Pattern recognition, vol. 35, pp. 545-561, 2002. doi:10.1016/S0031-3203(01)00059-0.

[7] H. S. Malvar and D. A. Florêncio, "Improved spread spectrum: a new modulation technique for robust watermarking," IEEE Transactions on Signal Processing, vol. 51, pp. 898-905, 2003. doi:10.1109/TSP.2003.809385.

[8] W. Wan, J. Liu, J. Sun, C. Ge and X. Nie, "Logarithmic STDM watermarking using visual saliency-based JND model," in Electronics Letters, vol. 51, no. 10, pp. 758-760, 5 14 2015. doi:10.1049/el.2014.4329.

[9] T. Bianchi and A. Piva, "Secure Watermarking for Multimedia Content Protection: A Review of its Benefits and Open Issues," in IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 87-96, 2013. doi: 10.1109/MSP.2012.2228342.

[10] F. Ros, J. Borla, F. Leclerc, R. Harba, and N. Launay, "An industrial watermarking process for plastic card supports," ICIT 2006. IEEE International Conference on Industrial Technology, 2006, pp. 2809-2814. doi:10.1109/ICIT.2006.372635.

[11] J. F. Lichtenauer, I. Setyawan, T. Kalker, and R. L. Lagendijk, "Exhaustive geometrical search and the false positive watermark detection probability," Proc. SPIE 5020, Security and Watermarking of Multimedia Contents V, p. 203, 2003. doi:10.1117/12.503186

[12] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," IEEE Transactions on Image Processing, vol. 9, pp. 1123-1129, 2000. doi:10.1109/83.846253.

[13] A. Poljicak, L. Mandic, and D. Agic, "Discrete Fourier transform–based watermarking method with an optimal implementation radius," Journal of Electronic Imaging, vol. 20, pp. 033008-033008-8, 2011. doi:10.1117/1.3609010.

[14] A. Poljičak, L. Mandić, and M. S. Kurečić, "Improvement of the watermark detector performance using image enhancement filters," in Systems, Signals and Image Processing (IWSSIP), 2012 19th International Conference on, 2012, pp. 68-71.

[15] L. Yu, X. Niu, and S. Sun, "Print-and-scan model and the watermarking countermeasure," Image and Vision Computing, vol. 23, pp. 807-814, 2005. doi:10.1016/j.imavis.2005.05.014.

[16] R. Riad, R. Harba, H. Douzi, M. El-hajji, and F. Ros, "Print-and-scan counterattacks for plastic card supports Fourier watermarking," in IEEE 23rd International Symposium on Industrial Electronics (ISIE), pp. 1036-1041, 2014. doi:10.1109/ISIE.2014.6864755.

[17] A. Keskinarkaus, A. Pramila, T. Seppänen, "Image watermarking with feature point based synchronization robust to print–scan attack," Journal of Visual Communication and Image Representation, vol. 23, no. 3, pp. 507-515, 2012. dx.doi.org/10.1016/j.jvcir.2012.01.010

[18] X.-y. Wang, Y.-n. Liu, S. Li, H.-y. Yang and P.-p. Niu, "Robust image watermarking approach using polar harmonic transforms based geometric correction," Neurocomputing, vol. 174, Part B, pp. 627-642, 2016. dx.doi.org/10.1016/j.neucom.2015.09.082

[19] H.-Y. Yang, X.-Y. Wang, P.-P. Niu, and A.-L. Wang, "Robust Color Image Watermarking Using Geometric Invariant Quaternion Polar Harmonic Transform," ACM Trans. Multimedia Comput. Commun. Appl., vol. 11, pp. 1-26, 2015. doi:10.1145/2700299.

[20] Z. Shao, Y. Shang, Y. Zhang, X. Liu, and G. Guo, "Robust watermarking using orthogonal Fourier–Mellin moments and chaotic map for double images," Signal Processing, vol. 120, pp. 522-531, 2016. dx.doi.org/10.1016/j.sigpro.2015.10.005.

[21] M. Ali and C. W. Ahn, "An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain," Signal Processing, vol. 94, pp. 545-556, 2014. dx.doi.org/10.1016/j.sigpro.2013.07.024.

[22] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal processing, vol. 90, pp. 727-752, 2010. doi:10.1016/j.sigpro.2009.08.010.

[23] C. Strauss, F. Pasteau, F. Autrusseau, M. Babel, L. Bédat, and O. Déforges, "Subjective and objective quality evaluation of lar coded art images," IEEE International Conference on in Multimedia and Expo ICME 2009, pp. 674-677, 2009. doi:10.1109/ICME.2009.5202586.

[24] M. Carnec, P. Le Callet, and D. Barba, "Objective quality assessment of color images based on a generic perceptual reduced reference," Signal Processing: Image Communication, vol. 23, pp. 239-256, 2008. doi:10.1016/j.image.2008.02.003.

[25] P. Le Callet, F. Autrusseau, and P. Campisi, "Visibility control and quality assessment of watermarking and data hiding algorithms," Multimedia Forensics and security, pp. 163-192, 2008. doi:10.4018/978-1-59904-869-7.

[26] M. L. Miller and J. A. Bloom, "Computing the probability of false watermark detection," in Information Hiding, pp. 146-158, 1999. doi:10.1007/10719724_11.

[27] C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," IEEE Transactions on Image Processing, vol. 10, pp. 767-782, 2001. doi:10.1109/83.918569.

[28] 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.

[29] A. Malvido, F. Pérez-González, and A. Cousiño, "A novel model for the print-and-capture channel in 2D bar codes," in Multimedia Content Representation, Classification and Security, ed: Springer, 2006, pp. 627-634. doi:10.1007/11848035_83.

[30] R. Riad, M. El Hajji, H. Douzi, R. Harba, and F. Ros, "Evaluation of a Fourier Watermarking Method Robustness to Cards Durability Attacks," in Image and Signal Processing, ed: Springer, 2014, pp. 280-288. doi:10.1007/978-3-319-07998-1_32.

[31] Z. Sharif and A. Z. Sha'Ameri, "The application of cross correlation technique for estimating impulse response and frequency response of wireless communication channel,", SCOReD 2007. in 5th Student Conference on Research and Development, 2007, pp. 1-5. doi:10.1109/SCORED.2007.4451386.

[32] F. Luisier, T. Blu, and M. Unser, "Image denoising in mixed Poisson–Gaussian noise," IEEE Transactions on Image Processing, vol. 20, pp. 696-708, 2011. doi:10.1109/TIP.2010.2073477.

[33] C. Liu, R. Szeliski, S. B. Kang, C. L. Zitnick, and W. T. Freeman, "Automatic estimation and removal of noise from a single image," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 30, pp. 299-314, 2008. doi:10.1109/TPAMI.2007.1176.