Watermarking in E-commerce

Peyman Rahmati, and Andy Adler
Department of Systems and Computer Engineering
Carleton University
Ottawa, Canada

Thomas Tran
School of Information Technology and Engineering
University of Ottawa
Ottawa, Canada

***Abstract*—A major challenge for E-commerce and content-based businesses is the possibility of altering identity documents or other digital data. This paper shows a watermark-based approach to protect digital identity documents against a Print-Scan (PS) attack. We propose a secure ID card authentication system based on watermarking. For authentication purposes, a user/customer is asked to upload a scanned picture of a passport or ID card through the internet to fulfill a transaction online. To provide security in online ID card submission, we need to robustly encode personal information of ID card's holder into the card itself, and then extract the hidden information correctly in a decoder after the PS operation. The PS operation imposes several distortions, such as geometric, rotation, and histogram distortion, on the watermark location, which may cause the loss of information in the watermark. An online secure authentication system needs to first eliminate the distortion of the PS operation before decoding the hidden data. This study proposes five preprocessing blocks to remove the distortions of the PS operation: filtering, localization, binarization, undoing rotation, and cropping. Experimental results with 100 ID cards showed that the proposed online ID card authentication system has an average accuracy of 99% in detecting hidden information inside ID cards after the PS process. The innovations of this study are the implementation of an online watermark-based authentication system which uses a scanned ID card picture without any added frames around the watermark location, unlike previous systems.**

Keywords*—Data hiding; geometric distortion; watermarking; print-and-scan; and E-commerce Introduction

I. INTRODUCTION

In E-commerce, one clear concern of content owners is unauthorized reproduction of digital products. Copyright owners seek methods to control and detect such reproduction, and therefore research on digital product copyright protection has significant practical significance for E-commerce. Most electronic commerce systems use cryptography to secure the electronic transaction process [1]. Encryption provides "data confidentiality, authentication, data integrity, and in some cases authentication of the parties involved" [1, 2]. Copyright protection involves the authentication of the ownership and can be used to identify illegal copies. To detect reproduction of a digital product, a digital watermark created from information about the relationship between the product and its owner can be used. This information may be perceptible or imperceptible to the human senses. In 2009, Hirakawa and Iigima evaluated the effectiveness of using digital watermark technology for E-commerce website protection; and they reported a 60% reduction in the quantity of unauthorized content on E-commerce websites when protected by Digital watermarking technology [3]. In 2008, Sherekar et al. recommended that the watermarks for images in e-governance and e-commerce applications should be invisible for human eyes and robust for possible attacks, such as geometric attack, and compression attack (JPEG or other image compression formats) [4].

A number of watermarking algorithms have been proposed over twenty years [5, 6]. Friedman proposed a trusted digital camera, which embeds a digital signature for each captured image [7]. With the digital signature, one can verify that the image is not changed as well as identify a specific camera that pictured the image [7]. Yeung and Mintzer proposed an authentication watermark that uses a pseudo random sequence and a modified error diffusion method to protect the integrity of images [8]. Lin and Chang proposed a scheme to insert authentication data in JPEG cqoefficients so that the authentication watermark has resilience against JPEG compression [9]. Wong and Memon proposed a secret and public key image watermarking schemes for grayscale image authentication [10]. Digimarc Corporation developed a search engine, MarcSpider, to search web sites for images that contain Digimarc watermarked images. When watermarked images are found, the information is reported back to the registered owners of the images [11]. In [12, 13], it has been shown how documents can be marked so that they can be traced in the photocopy process.

One of the most common attacks for watermarked multimedia products is Print-Scan (PS) process as the watermark can be degraded by the PS operation used once or several times [14]. The robustness of watermarking algorithm against PS attack for the online authentication system is a new, important challenge in multimedia communication security as well as E-commerce [15]. The progress in Print-Scan resilient watermarking will ease promoting watermark-based E-commerce and provide the ground for copyright tracking to prevent any illegally copying after selling a digital watermark product. This study proposes a watermark-based E-commerce model designed for online, secure ID card submission. The proposed model in comparison with preceding models has five new preprocessing blocks in the decoder with the role of providing robustness for watermarking algorithm against PS distortions (figure 1 and figure 3).

The applications of the proposed online ID card based authentication system are where 1) a seller needs to check the identity of a buyer before successfully completing the trade through the internet and 2) an applicant needs to electronically submit his/her Passport/ ID card to a high security organization. For example, a company for authentication purposes may ask customers to upload a scanned picture of

their watermarked Passport or watermarked ID card to continue a trade with them through the internet. The watermark extracted from the uploaded ID card image, which is already scanned from the hardcopy of the ID card, determines the genuineness of the hardcopy.

This paper is organized as follows: In the next section, we review related work and discuss their drawbacks; Section III is to explain the proposed ID card authentication method and also to detail the design of the five proposed preprocessing blocks in the decoder; Section IV discusses the achieved experimental results; and finally conclusion and suggestion for the further research are offered in section V.

II. Related Works

In the print-scan resilient data hiding area, distortion parameters quantification due to print-scan operation is challenging. There are several papers that model Print-Scan distortions [16, 17]. Generally, we can divide these distortions into three parts [18]: 1) "Randomness": The printed and scanned image is highly different than the original digital image. 2) "Man-dependency": the setting of the printer and the scanner may change; and also the paper orientation in printer's paper input tray and on flatbed of scanner may change during the PS process. 3) "Indistinguishability": the distortion of PS process is an accumulation from both printer and scanner. The regained watermark from the inspected data is applied for authentication in different ways, such as localizing the occurred distortions [19-20] or recognizing the type of attacks performed [21].

The main challenge in online authentication system is to overcome the print-scan distortions, which is considered as a combination of different attacks [22-24]. Longjiang Yu [18] proposes a print-and-scan model so that his work is realized in the presence of an added rectangular frame around the watermark location. This rectangular frame around watermark location makes it easier to find the geometric distortion along the print-scan process, and to localize the watermark location. The main drawback of using a frame around the watermark location is that in various types of authentication applications either the presence of this frame is not allowed or not favorable.

For example, it might not be allowed in important documents, such as passport, driving license, and ID cards. Solanki et al. proposed a print-scan resilient data hiding algorithm analyzing halftone effect (intensity shift) occurred after print-and-scan operation for the sake of presenting a model of print-and-scan process [17].

The main drawback of their method is that halftone analyzing in PS operation is severely dependent to the hardware features of Printer and Scanner, which are variable from one commercial brand to another.

This paper proposes a new online ID card authentication model which is different, compared with the preceding models [17, 18], in this way that it does not offer any added rectangular frame around the watermark location, and also there is no need to model halftone effect occurred after PS process.

III. Method

In this work, we used ID cards as the required document needed to be submitted through the internet for online authentication purposes. The proposed model establishes a linkage between the ID card holder's photo and his/her personal identification number, considered as the watermark. Also, we used a simple block-based watermarking algorithm in spatial domain, and proposed five preprocessing blocks in the decoder to remove the PS distortions (figure 1). The proposed online ID card based authentication system for E-commerce has the same security design similar to [25]; however, improves its robustness against PS attack/ distortion. In [25], Ingemar et al. proposed a new Security Architecture of a watermark-based E-commerce model which involves watermarking as an extra security for the online authentication system along with cryptography (figure 2) . In Figure 2, the original data (payload) is first encrypted and watermarked in encoder (transmitter) and then sent to a decoder (receiver) through the internet to be decrypted and extracted. In this architecture, watermarking has been used as a security layer to add extra personal information about the user (customer) to the original data (payload) to increase the security of online authentication system in E-commerce. In the following, we will see the design of the proposed ID card based authentication system.

Fig.1. Overall schematic of the proposed ID card based authentication system.

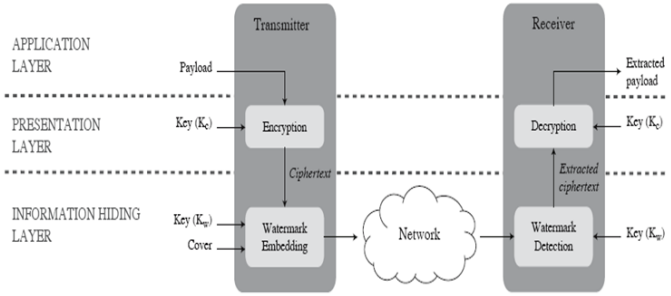

Fig.2. Representing the security architecture of a watermark based authentication system, reproduced from [25].

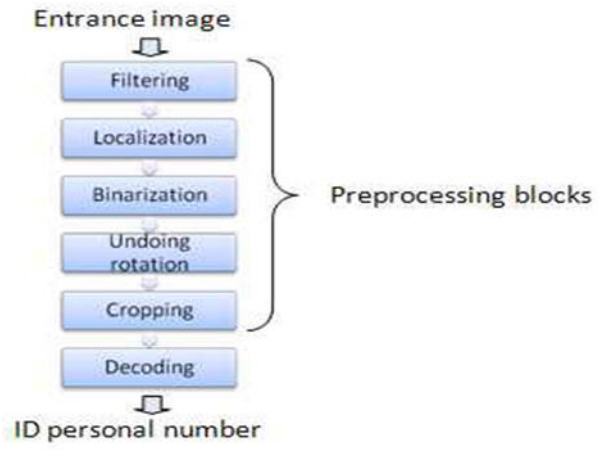

Fig.3. Representing the name and the sequence of applying the five proposed preprocessing blocks in the decoder to remove PS distortions.

A. Encoder

In the first step of authentication system, we need to hide the personal information of user/customer into the original digital ID card image. We use block-based embedding due to its simplicity in implementation, providing low computing time for real time application [26]. Several approaches have been suggested to achieve digital data hiding: Some in the spatial domain [27, 28], some in the frequency domain [29, 30], some on the basis of quantization [31, 32], and some based on spread spectrum methods [33, 34]. In this work, a simple block-based watermarking method using Hadamard patterns in spatial domain is introduced. The personal information, which is ID card personal number, is embedded into the ID card's holder photo place in the encoder. Two Hadamard patterns (f0 and f1) with small changes in their intensities, lower frequency than the frequency of the intensity changes in the original image, are applied to embed the data stream (ID card personal number) into the original image. First, the original image is divided into blocks with dimension of N×N and each bit of the data stream is assigned to each block. Then embedding procedure follows up this rule: if the bit of data stream assigned to a block is 0, f0 will add up to that block; if it is 1, f1 will add up to the block, see figure 4. The correlation between patterns (f0 and f1) and the blocks (B) is zero. Suppose that I is an original image with the dimensions N1×N2 which is divided into blocks, with the dimensions N×N. Since a bit of all desired data bits is embedded into each block, so, (N1.N2)/N2 bits can be hidden into the original image. Note that f0(k,l), f1(k,l) ; $0 \leqslant k, l \leqslant$ N-1 are indicators of the Hadamard patterns, which has property of f0 = -f1, and B(k,l) indicates the blocks. We can write the binary bit (W(i, j)) to be hidden as follows:

$$W(i,j) \in \{0,1\};\ 0 \le i \le (N1/N)-1,\ 0 \le J \le (N2/N)-1 \qquad (1)$$

The embedding algorithm will start by converting the designed patterns to an image matrix. Therefore, the watermarked image is:

$$I_w(m,n) = I(m,n) + \lambda . f_w\left(\left[\frac{m}{N}\right],\left[\frac{n}{N}\right]\right)(m\ Mod\ N, n\ Mod\ N), \qquad (2)$$

where $0 \leqslant m \leqslant$ N1-1 ,$0 \leqslant n \leqslant$ N2-1, IW (m, n) is the watermarked image, λ is Inductance Coefficient, [x] is the largest integer that is smaller or equal to x, and Mod is residue of an integer division. The above equation when f0 = -f1 can be shortened as:

$$I_W(m,n) = I(m,n) + \lambda.\left(2\,W\left(\left[\frac{m}{N}\right],\left[\frac{n}{N}\right]\right)-1\right).f\,(m\ Mod\ N, n\ Mod\ N) \qquad (3)$$

Inductance Coefficient (λ) compromise between visual quality of the watermarked image and resistance of the used method against attacks. The bigger the Inductance Coefficient, the lower the quality of the watermarked image will be. In (3), if the bit in the binary watermark placed at the position (i, j) of the original image is zero, the block related to (i, j) from the original image will induce with the pattern f0, and reversely, if the bit at the position (i , j) is one, the block related to (i , j) from the original image will induce with the pattern f1. Finally, the security of the algorithm can obtain by a watermark key is fed to the encoder and decoder blocks.

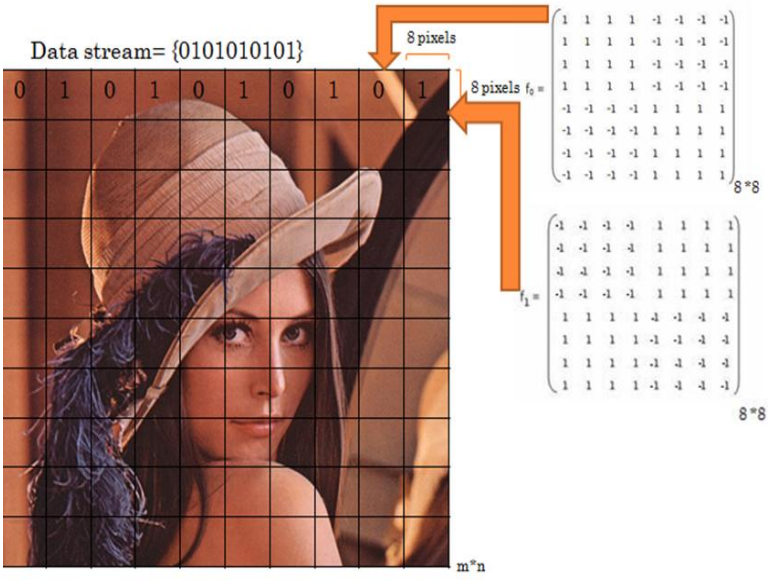

Fig.4. Representing an example of embedding the data stream with 10 bits into Lena image using two Hadamard patterns (f0 and f1), which are low frequency and f0=-f1.

B. The Watermark localization in the decoder

The next step after embedding information in the encoder is decoding the information after attacking the authentication system by the PS operation. To provide robustness for PS distortions, five preprocessing blocks are proposed in the decoder. Figure 3 shows the name and the sequence of applying these preprocessing blocks in the decoder. As shown in the figure 3, the first block is named filtering block to remove the possible noise on the entrance image. Gaussian filter is used as a low pass filter to denoise the entrance image. Then, a localization block is proposed with the duty of estimating the location of watermark region (ID card's holder photo place). In this block an approximate watermark region is achieved and the remaining area out of this region is omitted.

Whereas, we embed the information into a rectangular frame, belonging to the ID card holder's photo place, in the encoder, therefore, we should look for a rectangular frame (watermark region) in the decoder. To localize the rectangular watermark region, we put a rectangular mesh over the entrance image to the decoder, see figure 6. The dimension of the rectangular elements inside the mesh can be calculated by having the maximum occurred rotation angle after PS operation. This maximum rotation angle (MRA) can be written by two parameters as:

$$MRA = \theta_{max} = \theta_i + \theta_u \quad (4)$$

Where θ_i is maximum rotation angle created by the printer, and θ_u is maximum probable rotation angle that may occurs by user in the scanner. Now, the maximum dimension of the rectangular frame can be evaluated as:

$$Height \approx L.cos(\theta_{max}) + W.sin(\theta_{max}) + H0$$
$$Width \approx W.\cos(\theta_{max}) + L.\sin(\theta_{max}) + W0 \quad (5)$$

Where L is the approximate height of the ID card's holder photo place (watermark region), and W is the approximate width of watermark location. Both of these parameters are known by having "dots per inch" (dpi), which is adjustable in printer and scanner setting. H0, W0 are the additional parameters to qualify our approximation, selected by user. Figure 5 represents equation (5). After applying the mesh over the entrance image, the rectangular watermark region is achieved by the rule: The rectangular element inside the mesh with the biggest width in its histogram specification is the one has the watermark region inside. This rule comes from this fact that the watermark is embedded in the photo place of ID card's holder which has biggest width in its histogram compared with other regions of ID card. Note that, the output of the localization block is an estimate of the watermark region and we still need to have next blocks to get the exact watermark location.

C. Binarization algorithm in the decoder

In the previous block an estimate of the watermark region, including regions without watermark, achieved. The binarization block, located after localization block in figure 3, is proposed with the duty of discriminating the exact watermark location from the other region without any watermark inside.

The proposed binarization method is based on the thresholding and tries to find the exact watermark location using histogram specification of the estimated watermark region, achieved from the localization block. Figure 7 shows the histogram specification of the estimated watermark region in localization block. The circular sign in this figure corresponds to the region without any watermark, which should be removed in this block. To remove the region without watermark, we need to use a threshold value to make a binary image from the entrance image.

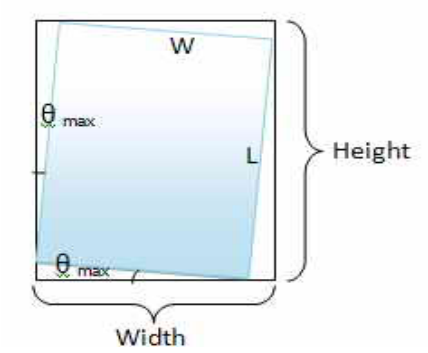

Fig.5. A schematic to get a frame with the maximum dimension based on the maximum probable rotation angle θ_{max}.

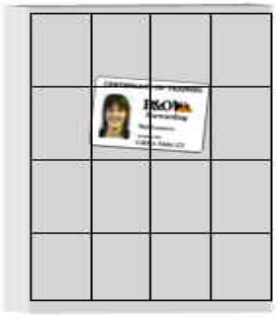

Fig.6. Outline of how a rectangular grid is applied on the entrance image to localize the watermark location.

The first local minimum (star sign in figure 7) around the circular point can be the initial guess of threshold value to make a binary image. As it is shown in Figure 8, if we consider the star point as the threshold value, the earned binary image will not show our desired watermark region, a rectangular frame. However, we consider this point as our initial threshold value. Looking at the histograms depicted in Figure 7 which belongs to the image in Figure 10(a) after print-scan operation, we can find out the existence of the gray levels shifting (halftone effect), appeared as several small peaks around the circular sign in figure 7. This is because of histogram distortion occurred after the print-scan operation.

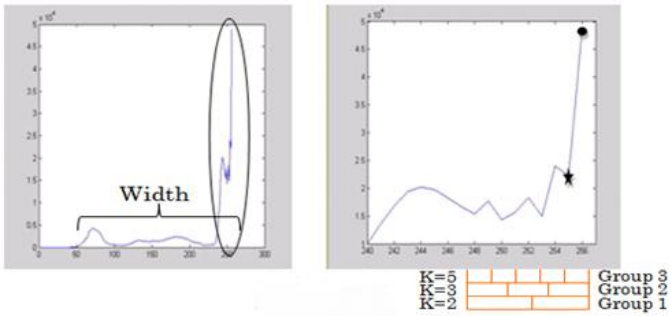

Fig.7. Histogram specification of the output image of localization block, which is an estimated image of watermark location.

In the left panel, histogram of the estimated watermark location which has the biggest width. In the right panel, a closer view of the black oval to show the occurred histogram distortion (halftone effect) after print-scan operation. The star sign on the right curve indicates the initial threshold value in binarization block, and K shows the number of the subdivisions.

A hierarchical algorithm to get the best threshold value which discriminates exactly the watermark location from other regions is proposed in this stage. Defining parameter P over the histogram as start points for searching the threshold value, and also parameter D that expresses the distance of the search, P-D is the last search point. We divide the distance D into K equal subdivision, and it is supposed that the bin with the least local minimum in each subdivision is our desired threshold value (figure 7).

The local minima are achievable by differentiating from the histogram curve. The number of the binary images is equal to the number of our subdivision. By considering several K for a fixed D, we will establish several groups with different number of subdivisions, see Figure 8. The more number of groups, the more precision and the more computing time to select the optimum threshold value will be. In each group a truth criterion (dmin) for the binary images, earned based on the number of K used in each group, is considered as:

$$D_k = \sum_{m=1}^{M}[(V_{k,m} - V_{I,m})^2] \;;\; d_{min} = \min[D_k] \qquad (6)$$

where D_k is vector distance, k=1,2,…,K, and K is the number of subdivisions used in each group, and V_I is our ideal feature vector that includes M specified features and may be expressed as: $V_I = [V_{I,1}, V_{I,2}, \ldots, V_{I,M}]^T$. As an example, the ideal feature vector can be chosen to include:

The number of pixels in the watermark location, the perimeter of the watermark location, the aspect ratio of the watermark location, and the ratio of the number of pixels in the watermark location (black rectangle in figure 10(d)) to the number of pixels out of watermark location (white region in figure 10(d)). Figure 9 shows the flowchart of the iterative binarization algorithm for a single group in figure 8. The binary image with the least distance criterion, dmin, in each group is considered as the output binary image in that group. The hierarchical process (figure 8) will be terminated in a group if the condition dmin<THD in that group is met, where THD is an arbitrary number selected by user. In the end, the output binary image of the group with the least dmin is selected as the final binary image.

Figure 10 shows the experimental results of applying the proposed binarization block for different values of K. As it is shown in Figure 10, the higher the number of the subdivisions (K), the more the accuracy in estimating the watermark location (black region in figure 10 (d)) will be.

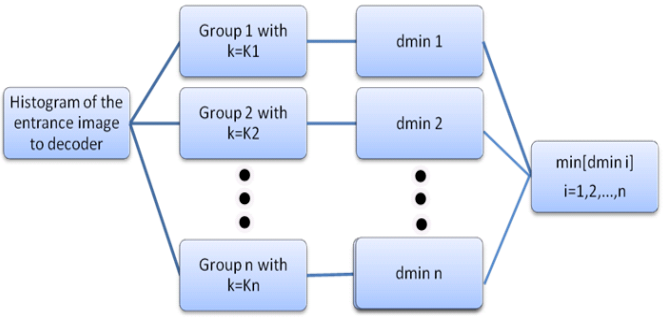

Fig.8. Hierarchical representation of finding the best threshold value from histogram specification of entrance image to the binarization block.

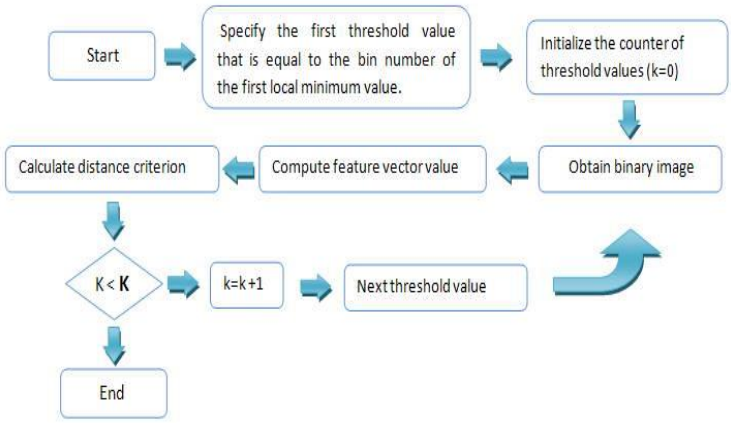

Fig.9. Iterative binarization algorithm for a single group in the hierarchical representation shown in figure 8.

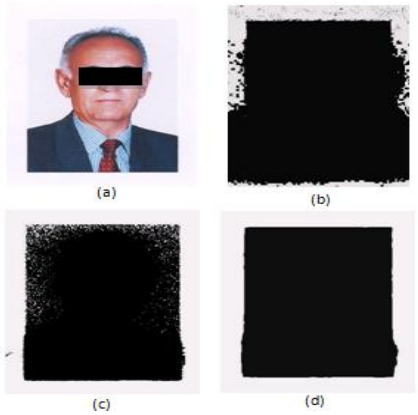

Fig.10. Example of three binary images earned from three different threshold values in an ID card with a white background. (a) The entrance image to the binarization block after print-scan operation, with a histogram specification drawn in Figure 7. (b) The obtained binary image after applying the first local minimum (star point in figure 7) as initial threshold value (Note that, the binary image does not show the watermark location accurately). (c) Obtained binary image by choosing a Threshold value achieved in group 3 with 3 subdivisions (Note that, the number of tested binary images is equal to *K=3*, and also the search distance was *D=10*). (d) Obtained binary image in group 5 with 5 subdivisions, which is the best achieved binary image.

D. Undoing the rotation

In this stage, we need to eliminate the occurred rotation angle on the obtained watermark location (black region in figure 10(d)) after print-scan operation. Several approaches have been proposed to undo the rotation [17, 18]. In [18], a template is produced by transforming the original image to a rotation space without the interpolation operation. By template matching, pixels of the original coordinate in the rotated image are defined and interpolation points are eliminated. After this process, pixels of the original coordinate are rotated back during the rotation restoration process; and non-integer coordinate is rounded into integer on some points. The benefit of this method is its capability in eliminating interpolation operation, that which preceding methods needed it for undoing rotation. The main drawback of [18] is its complexity in implementation which prohibited me to apply this method for undoing rotation. In this work, the method used for undoing rotation was Radon transform. The Radon transform is the projection of the image intensity on a radial line directed at a specific angle. We can estimate the rotation angle of the rectangular frame (watermark location) in the output image of binarization block using the following rule: the angle with the biggest projection value in its radon transform corresponds to the rotation angle of the rectangle frame. Applying the Radon transform, we can simply undo the rotation of the rectangle frame (watermark location), shown in black in figure 10 (d).

E. Cropping criteria

This phase of proposed authentication system is one of the most important units. This is because we need to crop the derotated image from the previous section at its optimum edges to achieve an accurate rectangular watermark location, where the personal information is hidden. Any mistake in estimating the optimum edges will result in the loss of hidden information inside the watermark location. The proposed algorithm to find the optimum edges uses two criterions: Average and Similarity criterion. We define two different regions: ***Non-transition region*** which *is* rows and columns with no intensity variation when we go from one row/column to its immediate adjacent row/column, and ***Transition region*** which is rows and columns with intensity variation when we go from one row/column to its immediate adjacent row/column, see figure 11. To reach to the optimum edges to crop the image, we need to first remove the non-transition region and then find the optimum edges within transition region. To remove the non-transition region, we define the average criterion (AVC) as follows:

$$\begin{aligned} AVC &= |AV(i) - N_i| ; \quad For\ rows \\ AVC &= |AV(j) - N_i| ; \quad For\ columns \end{aligned} \tag{7}$$

where N_i is average of the gray levels of the most outer pixels of the rectangular watermark location, and *AV(i)* and *AV(j) ; i=1,2,...,P ; j=1,2,...,Q* are, respectively, the average of the pixels in each row and column in non-transition region. Also, *P and Q* are the number of rows and columns of the watermark location respectively. The rows and columns having *AVC* lower than *T*, a threshold value selected by user, have to be removed. By doing so, we would remove the rows and columns without any transition. This criterion is done in a small distance from the most outer edges of the rectangular watermark location, see figure 11(b). Note that, the existence of the region without any transition in Fig. 11(b) depends on the application and the value of rotation angle created by PS process. In cases with small applied rotation angle, we do not have any non-transition region. In the following, we need to choose the optimum edges within the transition region to crop the rectangular frame. To do so, we consider the homogeneity criterion for each one of rows or columns within the transition region. The homogeneity criterion (HMC) for rows and columns within the transition region is evaluated as:

$$HMC = \frac{VAR}{AVG} , \tag{8}$$

where *VAR* is the variance of gray levels of pixels in each row or column, and *AVG* is the average of the gray levels of the pixels in the same row or the column. It is supposed that the optimum edges within the transition region are located between two columns/rows with the highest similarity in intensity. Now, the similarity between the sequential rows/ columns can be evaluated by taking the difference between the homogeneity values of those rows/ columns. Therefore, the similarity criterion (SCR) can be written as:

$$\begin{aligned} SCR &= |Hmc(i \pm 1) - Hmc(i)| ; \quad For\ rows \\ SCC &= |Hmc(j \pm 1) - Hmc(j)| ; \quad For\ columns \end{aligned} \tag{9}$$

Note that, the movement direction to compute the above equation is always from outer edges toward inner edges (see the direction of arrows in Figure 11). This difference (the similarity criterion) is the least amount at the optimum edges within the transition region. Therefore, we will consider a row or column as an optimum edge to crop the image if the *SCR* in that row or column is lower than a critical value *CV*, selected by user. We can write the cropping criterion (CRC) as follows:

$$CRC|_{i,j} = SCR|_{i,j} < CV \tag{10}$$

Finally, we deliver the cropped rectangular frame to the next decoding block to extract the hidden data inside it.

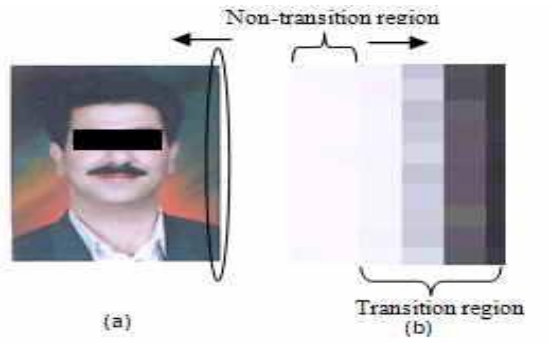

Fig.11. Example of the transition and non-transition regions in a test image after print-scan operation. (a) Representing a derotated rectangular watermark location. (b) A close view of the black oval in figure 11(a) to represent the transition region, and non-transition region. (Note the direction of drawn arrows in figure 11(a) and figure 11(b)).

F. Decoder

The final stage for the proposed authentication system is the decoding block. The decoding process is according to this

property that the original image has a minimum similarity to the Hadamard patterns (f_0 *and* f_1*)*, which are already used in the encoder. This means that correlation between the blocks (*B*) and Hadamard patterns is always zero, i.e. $Corr(B, f_x)=0$ where *B* is the blocks inside the original image in figure 4 and f_x can be either f_0 or f_1. A decision function for extracting a bit of the hidden data at the position (i, j) can be written as:

$$d(i,j) = Corr\left(B_{i,j}^{W}(k,l), f_1(k,l)\right) - Corr\left(B_{i,j}^{W}(k,l), f_0(k,l)\right), \quad (11)$$

where $B^{w}_{i,j}(k, l)$ is the block in the watermarked image. Since $B^{w}_{i,j}(k, l) = B_{i,j}(k, l) + \lambda . f_x(k, l)$, and also $Corr(B, f_x)=0$; therefore, we can write:

$$d(i,j) = \lambda . Corr(f_1, f_x) - \lambda . Corr(f_0, f_x) = \begin{cases} +\lambda, & if\ x = 1 \\ -\lambda, & if\ x = 0 \end{cases} \quad (12)$$

where x is the unknown hidden bit in the block $B^{w}_{i,j}(k, l)$, and *Corr(X,W)* is define as:

$$Corr(X,W) = \frac{\sum\sum(X-\overline{X}).(W-\overline{W})}{\sqrt{\left(\sqrt{(X-\overline{X})^2}.\sqrt{(W-\overline{W})^2}\right)}} \quad (13)$$

In the end, the decision function can be written as:

$$\widehat{W}(i,j) = sgn(d(i,j)) = \begin{cases} +1 & if\ x = 1 \\ -1 & if\ x = 0 \end{cases} \quad (14)$$

Where $\hat{W}(i, j)$ is a bit of the binary hidden data at the position (i, j).

IV. Experimental results

The proposed ID card based authentication algorithm was tested on a Pentium IV (PC), Intel 3.0 GHz, with Windows XP Professional, 3.0 GB RAM, in MATLAB 8.0 (Mathworks, Natwick, USA). After several testes on the Hadamard patterns a low frequency template with the dimension 8 × 8 was selected.

In our experiments, we used typical printer and scanner with commercial brands: HP Photosmart 8450 and Canon L9950F, respectively. A database of 100 different ID cards with a wide range of possible colors, as background colors of the ID cards, was used. The original digital ID card image was printed with the resolution of 300 dpi, and then scanned with the resolution of 600 dpi. We embedded the ID card personal number, including 12 characters, inside the ID card's holder photo place in the encoder. The proposed ID card based authentication algorithm was applied to the whole of the database, including 100 ID cards, and an average accuracy criterion (ACC) was defines as:

$$ACC = 1 - \left(\frac{EB}{HB}\right) \quad (15)$$

Where *EB* is the number of detected bits with error, and *HB* is the number of all hidden bits. The average accuracy criterion has been depicted as a diagram in Figure 12 for different parameters introduced in the proposed ID card based authentication system. As it is obvious from the drawn diagram, the more the number of subdivisions (*K*) in the binarization block, the higher the average accuracy of detecting the hidden data will be. In Figure 12, the average accuracy is increased from 80% to 86% when increasing the number of the used groups in binarization block from *K*=1 to *K*=2. In Figure 12, the ideal feature vector, *VI*, was applied to get the accuracy results with two features were: the number of pixels inside the watermark location, and the aspect ratio of the watermark location. Also in the case of applying four features to achieve the average accuracy in figure 12, the used features were the same ones mentioned in the binarization section. The threshold value (*THD)* was set to 0.05 and the number of the groups in binarization block was different between 3 and 5 over our database.

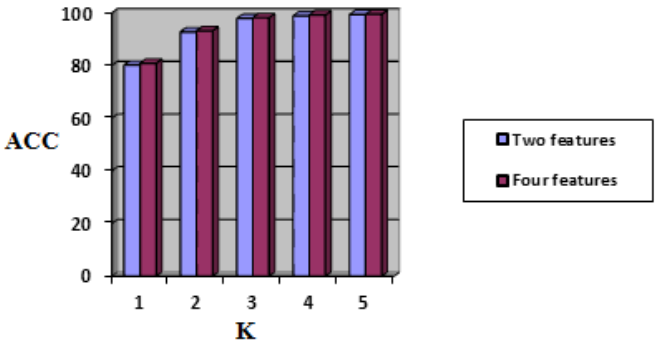

Fig.12. Representing a diagram to compare the average accuracy criterion for different values of subdivision number (*K*), and also different number of used features. (Note that, the selected value for distance of search, *D*, was equal to 10).

Figure 13 shows several case studies selected from our database before watermarking (figure 13(a)) and after watermarking and PS operation (figure 13(b)). Figure 13(c) depicts the Personal information, including 12 characters, embedded into the ID card's holder photo place.

Fig.13. Experimental results of applying the proposed authentication system over five case studies selected form our database, including 100 ID cards. (a) The original image of ID card's holder before watermarking. (b) The Image of ID card's holder after watermarking and PS operation, including ID card's holder personal information. The background of the study cases in this figure are different from one case to the other, ranged from light, plain background to the background with busy texture.

Figure 14 represents the effect of changing the Inductance Coefficient (λ) over the Signal to Noise Ratio (SNR) of the watermarked images in our database. The higher the inductance coefficient, the lower the SNR will be. This means that to preserve the visual quality of an image after watermarking, we need to select an appropriate value for λ.

TABLE I. Results of watermarked image quality (PSNR).

Methods	Images					
	Image (a)	Image (b)	Image (c)	Image (d)	Image (e)	Image (f)
Proposed method	44.3324	43.1223	40.5634	39.8912	45.6554	42.1342
Tsai's method	37.4323	38.2123	38.5654	38.2134	42.6723	39.3251

In all our experiments, the Inductance Coefficient after several times of examination was set to a fixed value of 8. With this value for λ, the watermarked image will be fairly imperceptible for human eyes, see figure 13(b).

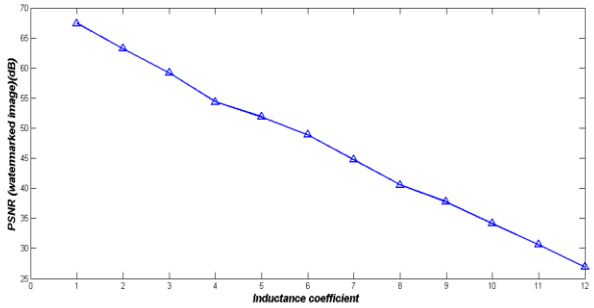

Fig.14. The effect of changing Inductance Coefficient (λ) over the visual quality of the watermarked images, calculated by using Signal to Noise Ratio (SNR) in decibel (*dB*), in our database. (Note that as the λ increases the SNR decreases, which means the watermark inside the image is more perceptible for human eyes).

Figure 15 is to assess the average accuracy of the proposed authentication model in detecting the hidden information into the watermark location when we do several Print-Scan operations in sequence. As the number of PS operations increases, the average accuracy of the authentication system decreases so that it reaches to 81% with $\lambda=8$ after doing PS operations for 6 times in sequence, which is still an acceptable accuracy (see figure 15).

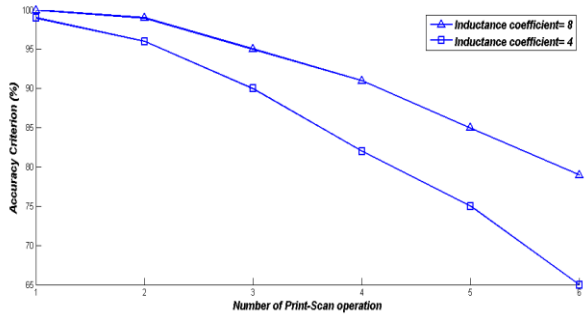

Fig.15. The average accuracy of the proposed authentication system for different values of λ when doing PS operations for several times in sequence.

In order to verify the effectiveness of the proposed watermark scheme, the method proposed by Tsai et al. [35] was also simulated for performance comparison. We used peak signal-to-noise ratio (PSNR) to evaluate the quality of the watermarked images using the two watermark methods. The PSNR is defined as:

$$MSE = \left(\frac{1}{m \times n}\right) \sum_{i=1}^{m} \sum_{j=1}^{n} (I(i,j) - I_w(i,j))^2$$
$$PSNR = 10 \log_{10} \frac{255 \times 255}{MSE} \; dB \qquad (16)$$

where I is the original image, I_w is the watermarked image, and $m \times n$ is the number of pixels in I. The PSNR values of each test image using the proposed method, and Tsai's method are summarized in Table 1. According to our experiments, if the PSNR value is greater than 36 dB, the watermark is almost invisible to the human eyes. To test the robustness of the proposed watermarking method, geometric distortions and common attacks including additive Gaussian noise, rotation, scaling, and cropping was performed to attack the watermarked images. Table 2 shows the experimental results of the average error ratio of the extracted watermarks of different attacks. The error ratio is defined as the number of extracted bits with error divided by the number of all hidden bits. In all cases, the results of our approach are better than the comparison method.

TABLE II. Results of average error ratio (%) of the extracted watermark at different attacks using the proposed method, and Tsai's method [35].

Attacks	Methods	
	Proposed method	**Tsai's method**
Additive uniform noise	**11.14**	**12.67**
Removed 1 row and 3 columns	**6.19**	**6.34**
Removed 3 row and 8 columns	**17.98**	**19.47**
Cropping ratio 90%	**18.58**	**18.76**
Cropping ratio 75%	**31.24**	**32.36**
Linear geometric transform (1.020,0.015,0.010,1.021)	**6.75**	**8.91**
Rotation 5°	**1.12**	**3.45**
Rotation 20°	**6.13**	**7.23**
Rotation 5° + cropping ratio 75%	**30.93**	**34.75**
Rotation 20°+ cropping ratio 90%	**24.12**	**25.32**

V. Discussion And Conclusion

This paper proposed a watermark-based E-commerce model to provide an online secure ID card authentication system which uses scanned picture of customer's ID card as identity. With the popularization of the internet and E-commerce and the expansion of E-government services, a variety of recorded data and documents that are relevant to such transactions and services are constantly created and exchanged electronically. In such situations, it is important to preserve the reliability of electronic data and documents by ensuring that the content cannot be altered. A watermark-based E-commerce model can provide us with an online secure ID card authentication system so that it is possible to learn whether the content of digital documents/data has been altered or not. Digital watermark technology embeds the user /customer's personal information into the digital content and makes it hard for criminals to abuse a content-based electronic business. In this work, the user/ customer takes the scan of hardcopy of his/her ID card and then uploads the scanned picture of ID card through the internet for authentication purposes to fulfill an online trade/transaction. The proposed authentication system extracts the watermark inside the ID card's holder photo place in the decoder and then checks it out with the ID card personal number. If the extracted watermark and the ID card personal number are the same, the identity of the user/ customer will be verified; otherwise, the identity will be denied. The main attack for the proposed authentication system is PS operation which imposes several distortions on the watermark location. To remove the PS distortions, five preprocessing blocks in the decoder are proposed. According to the experimental results, the proposed ID card authentication system has an average accuracy of 99% in finding correctly the hidden information into the 100 ID cards after PS operation. Unlike a preceding ID card authentication system [17], the proposed authentication method does not need to add a rectangular frame around the watermark location, which makes it applicable for online passport based authentication system. Moreover, the proposed authentication method outperforms the preceding proposed authentication system [18] in this way that it does not need to model the PS distortion (halftone effect), which is *variable* for printers and scanners from one brand to another, to remove the PS distortion on the watermark location. As the future work, we can use scanned picture of Passport as identity for the proposed authentication system. Also, this work is extendable where a frequency based watermarking algorithm is applied in the encoder and the decoder, in anticipation of achieving high quality watermarked images and higher average accuracy in finding correctly hidden information into the watermark location after PS operation.

References

[1] Schneier, B., Applied Cryptography, Second ed. John Wiley & Sons, New York, 1996.

[2] Ford, W., Baum, M., Secure Electronic Commerce. Prentice Hall, Upper Saddle River, NJ, 1997.

[3] Hirakawa, M., and Iijima, J. "Validating The Effectiveness of Using Digital Watermarking Technology for E-commerce Website Protection" The 9th Asian eBusiness Workshop, pp. 127-132, Japan, 2009.

[4] Role of Digital Watermark in E-governance and E-commerce" IJCSNS International Journal of Computer Science and Network Security, Vol. 8, No. 1, 2008.

[5] Podilchuk C.I., Delp E.J.: Digital watermarking: algorithms and applications, IEEE Signal Processing Magazine, Vol. 18 (2001) 33-46.

[6] Lee S.J., Jung S.H.: A survey of watermarking techniques applied to multimedia, Proc. of IEEE International Symposium on Industrial Electronics (ISIE), vol. 1 (2001) 272-277.

[7] Friedman G.L.: The trustworthy digital camera: Restoring credibility to the photographic image, IEEE Trans. Consumer Electron., vol. 39 (1993) 905-910.

[8] Yeung M.M., Mintzer F.: An invisible watermarking technique for image verification, Proc. ICIP (1997) 680-683.

[9] Lin C.Y., Chang S.F.: A robust image authentication method surviving JPEG lossy compression, Proc. SPIE, vol. 3312 (1998) 296-307.

[10] Wong P.W., Memon N.: Secret and public key image watermarking schemes for image authentication and ownership verification, IEEE Trans. Image Processing, vol. 10 (2001) 1593-1601.

[11] Digimarc Corporation, PictureMarcTM, MarcSpiderTM, http://www.digimarc.com

[12] Brassil, J., Low, S., Maxemchuk, N., O'Gorman, L., Electronic Marking and Identification Techniques to Discourage Document Copying. In Infocom94, 1994.

[13] Brassil, J., O'Gorman, L., Maxemchuk, N., Low, S., Document Marking and Identification using both Line and Word Shifting. In Infocom95, Boston, MA, April 1995, 853-860.

[14] K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran and I. El-Khalil, "'Print and scan' resilient data hiding in images," *IEEE Trans.* Information Forensics and Security. , vol. 1, no. 4, pp, 464– 478, Dec. 2006.

[15] Hyejoung Yoo, Kwangsoo Lee, Sangjin Lee, and Jongin Lim, "Off-Line Authentication Using Watermarks" Springer-Verlag Berlin Heidelberg, ICICS 2001, LNCS 2288, pp. 200–213, 2002.

[16] C. Y. Lin and S. F. Chang, "Distortion modeling and invariant extraction for digital image print-and-scan process," presented at the Int. Symp. Multimedia Information Processing Dec. 1999.

[17] K. Solanki, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Estimating and undoing rotation for print-scan resilient data hiding," presented at the ICIP, Singapore, Oct. 2004.

[18] L.Yu, X. Niu and S. Sun, "Print-and-scan model and the watermarking countermeasure," in Image and Vision Computing., May 2005, vol 23, pp. 807- 817.

[19] R. B. Wolfgang and E.J. Delp, "Fragile watermarking using the VW2d watermark", Proceeding of the SPIE/IS&T International Conference on Security and Watermarking of Multimedia Contents, vol. 3657,pp. 204-213,fan. 1999.

[20] J.Hu, j. Hunang, D.Hunang and Y. Q. Shi, "Image fragile watermarking based on fusion of multi-resolution tamper detection," IEE Electronic Letters, vol. 38, no. 24, pp 1512-1513, Nov. 2002.

[21] D. Kundur and D.Hatzinakos, "Digital watermarking for telltale temper-proofing and authentication," proceedings of the IEEE Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1167-1180, July 1999.

[22] A. T. S. Ho, J. Shen, H. P. Tan, and J. Woon, "Security-printing authentication using digital watermarking," Electronic Imaging, vol. 13, no.1, Jan. 2003.

[23] J. Mercer, Authentication News, 5 (9/10), 2001.

[24] C.-Y. Lin and S,-F. Chang, "Distortion modeling and invariant extraction for digital image print-and-scan process," Intl. Symp. on Multimedia Information Processing, Taipei, Taiwan, Dec. 1999.

[25] Ingemar J. Cox1, Gwena¨el Do¨err, and Teddy Furon, "Watermarking Is Not Cryptography" 2006.

[26] M. Swanson, B. Zhu, and A. Tewfik, "Data hiding for video in video," presented at the IEEE Int. Conf. Image Processing, 1997.

[27] M. Utku-Celik, G. Sharma, E. Saber, and A. Murat-Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Processing*, vol. 11, pp. 585–595, Jun. 2002.

[28] M. Ramkumar,"Data Hiding in Multimedia-Theory and Applications," Ph.D., New Jersey Inst. Technol., Newark, 2000.

[29] C.-Y. Lin and S.-F. Chang, "Watermarking capacity of digital images based on domain-specific masking effects zero-error information hiding capacity for digital image," in *Proc. IEEE Int. Conf. Information Technology: Coding and Computing*, Las Vegas, NV, Apr. 2001.

[30] C.-T. Hsu and J.-L. Wu, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, pp. 776–786, Aug. 2003.

[31] F. Perez-Gonzalez, F. Balado, and J. Martin, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Trans. Signal Processing*, vol. 51, pp. 960–980, Apr. 2003.

[32] N. Liu and K. P. Subbalakshmi, "Vector quantization based scheme for data hiding for images," in *Proc. SPIE Int. Conf. Electronic Images'04*, San Jose, CA, Jan. 2004.

[33] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, pp. 1673–1687, Dec. 1997.

[34] D. F. H. Malvar, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Processing*, vol. 51, pp. 898–905, Apr. 2003.

[35] P. Tsai, Y.C. Hu, C.C. Chang, A color image watermarking scheme based on color quantization, Signal Process. (2004) 95–105.