Robust Object-Based Watermarking Using SURF Feature Matching and DFT Domain

Manuel CEDILLO-HERNANDEZ [1], Francisco GARCIA-UGALDE[1], Mariko NAKANO-MIYATAKE[2], Hector PEREZ-MEANA[2]

[1]Electric Engineering Division, Engineering Faculty, National Autonomous University of Mexico, Circuito Exterior, Ciudad Universitaria, Coyoacan 04510, Mexico City, Mexico
[2] Postgraduate Section, Mechanical Electrical Engineering School, National Polytechnic Institute of Mexico, 1000 Santa Ana Avenue, San Francisco Culhuacan, Coyoacan 04430, Mexico City, Mexico

mcedillohdz@hotmail.com , fgugalde@gmail.com , mariko@infinitum.com.mx , hmpm@prodigy.net.mx

Abstract. *In this paper we propose a robust object-based watermarking method, in which the watermark is embedded into the middle frequencies band of the Discrete Fourier Transform (DFT) magnitude of the selected object region, altogether with the Speeded Up Robust Feature (SURF) algorithm to allow the correct watermark detection, even if the watermarked image has been distorted. To recognize the selected object region after geometric distortions, during the embedding process the SURF features are estimated and stored in advance to be used during the detection process. In the detection stage, the SURF features of the distorted image are estimated and matched with the stored ones. From the matching result, SURF features are used to compute the Affine-transformation parameters and the object region is recovered. The quality of the watermarked image is measured using the Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM) and the Visual Information Fidelity (VIF). The experimental results show the proposed method provides robustness against several geometric distortions, signal processing operations and combined distortions. The receiver operating characteristics (ROC) curves also show the desirable detection performance of the proposed method. The comparison with a previously reported methods based on different techniques is also provided.*

Keywords

Digital image watermarking, authentication, object matching, geometric attack, speeded up robust features.

1. Introduction

During the last decades, digital image, video and audio technologies, widely used in multimedia content within home computers, mobile devices and open networks, have grown dramatically. Allowing that, digital media may be easily copied, manipulated or format converted without any control. This fact suggests the necessity to develop some efficient methods to solve these problems. Digital watermarking is considered as a suitable solution for copyright protection and authentication of digital materials [1], [2], [3], [4]. In digital watermarking, a short message called "watermark signal" is embedded into an image, audio or video without affecting the quality such that it can be detected using a detection algorithm. Advances in image editing software, does possible the copy of a certain object region extracted from an image and paste this into other image. Moreover, the illicit object region may be distorted additionally by signal processing such as JPEG compression, image filtering, or aggressive geometric attacks such as cropping, rotation, scaling and affine transformation, which are the principal factors of watermark detection error due to the synchronization loss between the embedding and detection stages. Hence, in this paper we propose a robust object-based watermarking method that embeds and detects a watermark pattern into a digital image for authentication against the above mentioned scenarios. In the literature, several approaches are related to conventional object-based watermarking [5], [6], [7], in which the embedding and detection stages require a pre-definition between the object region and the background layers, so that the object region layer can be isolated and then the correspondent watermarking scheme is carried out on this layer. However, the process of isolate the object region layer from the background layer is very complicated and even some time impossible [8]. Our proposed method is not oriented to a pre-definition of object-background layers with object segmentation purposes to perform a watermarking algorithm. The scope is oriented in the same way that the related work presented in [8], in which, using object matching in conjunction with a frequency domain, a robust object-based watermarking method is developed, nevertheless, our proposed algorithm presents significant differences respect to [8] as follows: a) The replacement of the Scale Invariant Feature Transform (SIFT) algorithm [9] by the faster matching method SURF [10]. b) The design of a robust watermarking scheme based on the DFT domain; preserving the robustness against JPEG compression

provided by the Discrete Cosine Transform (DCT) domain used by [8] and at the same time improves the robustness against aggressive attacks such as translation and cropping image. c) The improvement of the watermark imperceptibility in terms of PSNR, SSIM and VIF metrics. Therefore, in this paper we propose a robust object-based watermarking method, in which the watermark is embedded into the middle frequencies band of the DFT magnitude of the selected object region, which maybe corresponds to the whole image or a special region of their content, altogether with the SURF algorithm to allow the correct watermark detection, even if the watermarked image has been distorted. The watermark consists a 1D binary pseudo random pattern composed by binary {0, 1} values generated by a secret key. To recognize the selected object region after geometric distortions, during the embedding process the SURF features are estimated and stored in advance to be used during the detection process. In the detection stage, the SURF features of the distorted image are estimated and matched with the stored ones. From the matching result, SURF features are used to compute the affine-transformation parameters and then the object region is recovered. Finally the watermark is detected using the Bit Correct Rate (BCR) criterion. The quality of the watermarked image is measured using the PSNR, SSIM and the VIF quality measures. The experimental results show that the proposed method provides robustness against several geometric distortions, signal processing operations and combined distortions. The ROC curves also show the desirable detection performance of the proposed method. A comparison with the previously reported methods based on different techniques is also provided. The general idea of the watermarking proposed detection method in this paper is shown in Fig. 1.

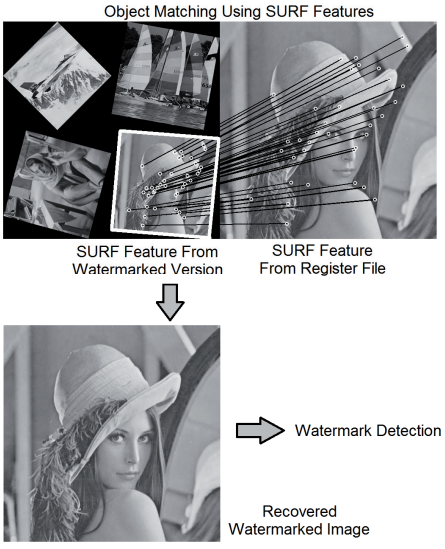

Fig. 1. General idea of the watermarking proposed detection method using object matching by SURF feature points.

The watermarked object "Lena" in Fig. 1 is distorted by being mixed with other images into a collage and additionally is geometrically transformed. To detect the watermark pattern in this object "Lena", we firstly detect the object region by using an object matching procedure. Two objects are matched by searching the nearest feature point pairs extracted from the two objects: the distorted one and the reference. The nearest feature point is defined as the feature point with the minimum Euclidean distance for the invariant descriptor vector. Once that the object matching operation is carried out, the affine parameters are estimated and the object is restored geometrically in order to detect correctly the watermark pattern.

The rest of this paper is organized as follows. Section 2 shows several methods related to geometrically invariant watermarking. Section 3 describes the SURF algorithm in general terms and the performance comparison with respect to the SIFT algorithm is shown. Section 4 describes the embedding and detection process of the proposed algorithm and the experimental results including comparison with the previously reported watermarking algorithms are presented in Section 5. Finally Section 6 concludes this work.

2. Related Works

There are several methods reported in the literature related to geometrically invariant watermarking. We categorize them in two groups.

2.1 Watermarking Algorithms Based on Feature Point Positions

The approaches in this category are feature-based methods in which salient image features are used for resynchronization, without embedding any additional signal into the image [11], [12], [13], [14], [15], [16]. The methods of this category are called of the second generation. The concept of second generation watermarking was firstly reported in [14]. The key idea is that the watermark information is associated with image features, which are invariant under some geometric attacks. Bas et al. [11] use the Harris detector to extract features and Delaunay Tessellation to define watermark embedding regions. Tang and Hang in [12] use the Mexican hat wavelet to extract feature points, and several copies of the watermark are embedded in the disks centered at the feature points. Lei-da et al. [13] use the Harris corner detector to extract features, the image normalization by geometric moments is used to improve the watermark robustness against geometrical distortions and the watermark data bits are embedded into the DCT domain. Kutter et al. [14] uses the Mexican hat wavelet to extract features and Voronoi diagrams to define the watermark embedding regions. Wang et al. in [15] proposed a watermarking scheme based on Harris Laplace feature detector combined with a geometric moment based image normalization and DFT domain. Considering each stable feature point as a center, a local feature region (LFR) around each point is constructed taking into account the characteristic scale of each one as well as a constant value in order to embed and detect the watermark in each LFR.

Lee et al. [16] extracted circular patches using the SIFT descriptor [9] which are employed to embed and detect a watermark pattern in an additive form into the spatial domain. The above watermarking methods provide several solutions to confront the geometric attacks. However, the experimental results of these approaches based on Harris detector, Mexican hat wavelet, Harris Laplace or SIFT descriptors present the following two shortcomings. First, some of these feature point extraction techniques are sensitive to image modification, such as some geometric and signal processing distortions. Second, in some techniques, a fixed value is used to determine the size of LFR or circular patches resulting in watermarking methods vulnerable to scale modifications, affine transformation, aspect ratio changes or shearing of the image, etc., that distorts the LFR or circular patches to elliptical shapes and, as a consequence, the watermark detection rate fell down.

2.2 Watermarking Algorithms Based on Object Matching Employing SIFT Feature Points

In this category, the key idea is to develop robust object-based watermarking algorithms employing the SIFT features [9] in conjunction with a watermarking technique into the frequency domain. Pham et al. [8] proposed a watermarking algorithm based on the SIFT feature and the DCT domain to digital image and video. The method is not oriented to a pre-definition of object-background layers with object segmentation purposes to perform a watermarking algorithm. Thus, a region of interesting denominated "object" for embedding the watermark is selected in an arbitrary form, which may be the whole image or a special region of their content. The watermark consists of a 1D binary pseudo random pattern composed by {0, 1} values generated by a secret key. The payload of the method is 83 and 50 watermark data bits in total to digital image and video respectively, which are embedded redundantly two times into the object. Later, several blocks of size 16x16 are randomly selected using a secret key, in order to prevent attackers from knowing where to attack. The watermark is embedded into the coefficients of each 16x16 DCT block obtained from the object region, taking into account a predefined embedding rules as well as two coefficients (x_0,y_0) and (x_1,y_1) selected from seven candidates (1,4), (2,3), (1,5), (2,4), (1,6), (2,5), (3,4) into the DCT domain. Finally, once that the watermarked image is obtained, the SIFT algorithm is applied to the object region in order to extract the feature points together with their invariant descriptor vector, which are registered in a database system using a register file format. In the detection stage, the SIFT algorithm is applied to the attacked watermarked image in order to extract the feature points together with their invariant descriptor vector from the object region. Then the extracted feature points are matched with the registered ones in advance. This match operation is carried out by searching the nearest feature point pairs from two objects. The nearest feature point is defined as the feature point with the minimum Euclidian distance for the invariant descriptor vector. Based on the matching results, six affine transformation parameters are calculated, which include two scaling factors, two shearing factors and two translation factors. The reason of obtaining two parameters for the same type of affine transformation is in order to be applied to both axes. Using the above affine transformation parameters, the watermarked object region is restored geometrically and then, using a predefined criterion, the watermark pattern is extracted and detected. The method presents robustness against several geometric and signal processing distortions, including general affine transformation. However, although the watermark pattern was embedded in a redundantly manner, the method is not robust against some cropping attacks, e.g. centered cropping, translation with cropping, among others, because several watermarked DCT blocks are removed when the object region is cropped, hence, the watermark cannot be recovered adequately.

3. Speeded Up Robust Feature (SURF) Algorithm

The Speeded Up Robust Feature (SURF) is a scale and rotation invariant detector and descriptor algorithm proposed by Bay et al. [10], that can be used in computer vision tasks such as object recognition. SURF algorithm is similar to the SIFT algorithm proposed by Lowe [9], although it presents notable differences. According to the authors of SURF, the method presents two main improvements with respect to SIFT: speed of calculation is considerably higher without causing loss of performance and possesses major robustness against different types of geometric and photometric transformations, such as scaling and rotation, image blur, lighting changes and JPEG compression, among others. The SURF algorithm consists of three main procedures: a) feature point extraction, b) repeatable angle calculation and c) descriptor calculation. The feature point extraction procedure begins obtaining the determinant of the Hessian matrix and extracting the local maxima. Given a point $p(x,y)$ from the original image I_o, the Hessian matrix $H(p,\sigma)$ of a point p belonging to scale σ is defined as follows:

$$H(p,\sigma)=\begin{bmatrix} L_{xx}(p,\sigma) & L_{xy}(p,\sigma) \\ L_{xy}(p,\sigma) & L_{yy}(p,\sigma) \end{bmatrix}. \tag{1}$$

where $L_{xx}(p,\sigma)$ is the convolution of the second order derivative of a Gaussian $\frac{\partial^2}{\partial x^2} g(\sigma)$ with the image I_o at point p, and similarly for the other directions $L_{xy}(p,\sigma)$ and $L_{yy}(p,\sigma)$ [10]. For computer reasons the Hessian matrix implementation is approximated by a combination of Haar basis filters of successively larger levels. Each extracted feature point is further improved by a quadratic localization. After the interest points and their scales are obtained, a repeatable angle is calculated for each interest point prior to ob-

taining the invariant descriptor vector. This procedure calculates the angle of the gradients surrounding the interest point and the maximum angular response is chosen as the direction of the feature point. This direction is then used to create a rotated square around the interest point, and regularly sampled gradients within this template are combined per grid location to form the final invariant descriptor vector [10], [17]. A performance comparison between SIFT and SURF algorithms is carried out to show the improvements of SURF with respect to SIFT algorithm, i.e., high speed of calculation and major robustness against different types of geometric and photometric transformations. The parameters used in both algorithms are the default values reported in [9] and [10] respectively. A gray-scale image with 8/bits per pixel resolution and 512x512 dimensions is used. Our experiment is carried out on a personal computer running win7© with an AMD© Athlon processor (2.7 GHz) and 4 GB RAM while the SIFT and SURF algorithms were implemented in Matlab© 7.10.0. The test consists of measurements on the creation and matching time. In the case of matching operation, in the experiment we use the feature points registered in advance and the feature points obtained after the image is rotated by 45° degrees. Tab. 1 shows the creation and matching time, reported in seconds.

Algorithm	Advantage	Disadvantage	Creation time	Matching time
SIFT [9]	Invariant to rotation, translation, scaling and illumination changes. Repeatable.	High computational cost. Discretization of Gaussian filters. Dependent on size image.	7.47 s	2.47 s
SURF [10]	Major robust and high speed of calculation with respect to SIFT. Repeatable.	Minor size that descriptor SIFT. Dependent on size image.	2.37 s	0.94 s

Tab. 1. Performance comparison between SIFT and SURF algorithms.

In Tab. 1, we show that the SURF algorithm is very fast respect to the SIFT algorithm, in the creation and matching of the feature points. It is assumed that the implementation of both algorithms on other programming language, e.g., C, C++, in conjunction with other robust computer equipment, preserves the difference between speed calculi. As a consequence of this comparative, the SURF algorithm is adopted in our robust object-based watermarking method.

4. Proposed Algorithm

The proposed watermarking method consists of the embedding and detection processes, which are explained in detail as follows.

4.1 Embedding Process

The watermark embedding process is described in the following steps: **1)** Produce the watermark W as a zero mean 1-D binary pseudo-random pattern composed by {1, 0} values generated by a secret key k_1, $W = \{w_i | i = 1, \ldots, L\}$, where L is the length of the watermark. **2)** Apply the 2D DFT transform to the original image $I(x,y)$. The 2D DFT transform of $I_o(x,y)$ of size N_1 x N_2 is given by (2):

$$F(u,v) = \sum_{x=1}^{N_1} \sum_{y=1}^{N_2} I_o(x,y) e^{-j2\pi(f_1 x/N_1 + f_2 y/N_2)} . \quad (2)$$

3) Get the magnitude $M(u,v) = |F(u,v)|$ and phase $P(u,v)$ of the 2D DFT transform $F(u,v)$. Translations in the spatial domain do not affect the magnitude of the DFT transform, as shown in (3):

$$| DFT\left[I_o(x + x_1, y + y_1)\right] | = M(u,v) . \quad (3)$$

Concerning the scaling in the spatial domain it causes an inverse scaling in the frequency domain, as shown in (4):

$$DFT\left[I_o(\rho x, \rho y)\right] = \frac{1}{\rho} F(\frac{u}{\rho}, \frac{v}{\rho}) \quad (4)$$

where ρ is the scaling factor. And rotation in the spatial domain causes the same rotation in the frequency domain, as shown in (5):

$$\begin{aligned} &DFT\left[I_o(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)\right] . \\ &= F(u\cos\theta - v\sin\theta, u\sin\theta + v\cos\theta) \end{aligned} \quad (5)$$

Thus selecting the DFT domain to embed the watermark W has a certain number of advantages for rotation, scaling and translation (RST) invariance as well as watermark robustness against common signal processing. However, the DFT domain presents weak robustness against other aggressive geometric distortions such as affine transformations, aspect ratio changes, shearing, among others. Thus, in order to increase the robustness without decreasing the watermark imperceptibility, a very promising research direction consists in developing informed watermarking algorithms [4], [8]. In this way, using the combination of the object matching by SURF feature points and the robustness of the DFT-based watermarking method; we have developed a robust object-based watermarking using SURF feature matching and DFT domain algorithm. **4)** Select a pair of radiuses r_1 and r_2 in $F(u,v)$ and compute the annular area $A=\pi(r_2^2-r_1^2)$ between r_1 and r_2 that should cover the middle frequencies components in the DFT domain around the zero frequency term; because modifications in the magnitude of lower frequencies of the DFT will cause visible distortion in the spatial domain of the image we kept these lower frequencies out of the annular area. On the other hand, the magnitudes of the higher frequencies are vulnerable to the JPEG compression that's because these higher frequencies are also kept out of the annular area. Thus, the watermark pattern should be embedded in the

band of the middle frequencies because, in this spectral region, it will be both robust against JPEG compression and at the same time imperceptible. **5)** Consider the DFT magnitude divided into four quadrants and select the middle frequencies DFT magnitude coefficients. So that to ensure the correct watermark embedding, the condition $(A/4) \geq L$ should be satisfied, where A corresponds to the annular area between radiuses r_1 and r_2, and L is the watermark length. In case that the condition $(A/4) \geq L$ is not satisfied, the pair of radiuses r_1 and r_2 can be adjusted so that the total number of magnitude coefficients in the middle frequencies is enough to embed the L watermark data bits. **6)** Scramble the watermark data bits in order to guarantee their security. **7)** Compute the magnitude difference denoted by d between the magnitude coefficients from first and second quadrants of the upper half part of the DFT magnitude respectively, $d = M_i(u_j,v_j) - M_i(-u_j,v_j)$, as shown in Fig. 2.

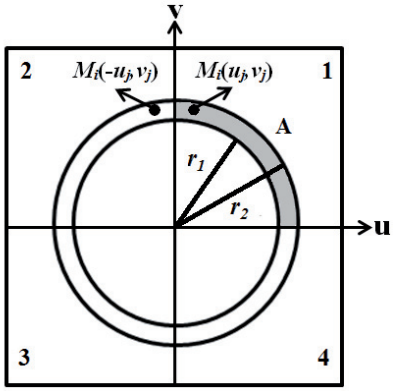

Fig. 2. Modification of DFT magnitude coefficients, shading region denotes condition $(A/4) \geq L$.

8) Once the difference d is obtained, consider a watermark strength factor α in order to modify the DFT middle frequency magnitude in a controlled manner as follows: if the watermark data bit $w_i = 0$ and $d < (-\alpha)$ then $M_i(u_j,v_j)$, and $M_i(-u_j,v_j)$ are not modified. On the other hand, if $d \geq (-\alpha)$ then $M_i(u_j,v_j)$, and $M_i(-u_j,v_j)$ are modified according to (6):

$$\begin{aligned} M'_i(u_j,v_j) &= M_i(u_j,v_j) - (\alpha + d) \\ M'_i(-u_j,v_j) &= M_i(-u_j,v_j) + (\alpha + d) \end{aligned}. \quad (6)$$

In (6) the difference d is added to the watermark strength α in order to force the compliance of the condition $d < (-\alpha)$ when $w_i = 0$, providing a large enough margin between $M'_i(u_j,v_j)$ and $M'_i(-u_j,v_j)$ with the purpose of preserving $d < (-\alpha)$ after that the watermarked image is processed by a common signal processing or a geometric distortion. If the watermark data bit $w_i = 1$and $d > \alpha$ then $M_i(u_j,v_j)$, and $M_i(-u_j,v_j)$ are not modified. On the other hand, if $d \leq \alpha$ then $M_i(u_j,v_j)$, and $M_i(-u_j,v_j)$ are modified according to (7):

$$\begin{aligned} M'_i(u_j,v_j) &= M_i(u_j,v_j) + (\alpha - d) \\ M'_i(-u_j,v_j) &= M_i(-u_j,v_j) - (\alpha - d) \end{aligned}. \quad (7)$$

In (7) the difference d is subtracted from the watermark strength α in order to force the compliance of the condition $d > \alpha$ when $w_i = 1$, providing a large enough margin between $M'_i(u_j,v_j)$ and $M'_i(-u_j,v_j)$ with the purpose of preserving $d > \alpha$ after that the watermarked image is processed by a common signal processing or a geometric distortion. In (6) and (7), $i = 1,\ldots, L$ denotes a mapping index corresponding to the w_i watermark data bits, $M_i(u_j,v_j)$, and $M_i(-u_j,v_j)$ denotes the original magnitude coefficients. And $M'_i(u_j,v_j)$ and $M'_i(-u_j,v_j)$ denote the watermarked magnitude coefficients. A larger value of α would increase the robustness of the watermark, on the other hand the watermark imperceptibility is less affected by a small value of α. Hence there is a tradeoff between robustness and imperceptibility. According to the DFT symmetrical properties in order to produce real values after the DFT magnitude modification, the watermark is embedded into the upper half part of middle frequencies of the DFT magnitude coefficients as shown in Fig. 2, and subsequently the lower half part of the middle frequency band should be modified symmetrically. By repeating the above mentioned procedure, the total L watermark data bits will be embedded in the annular region. **9)** Finally, the watermarked image $I_w(x,y)$ is obtained applying the inverse DFT (IDFT) to the watermarked magnitude $M'(u,v)$ and the corresponding original phase $P(u,v)$ as shown in (8):

$$I_w = IDFT(F'), \quad F' = (M', P). \quad (8)$$

10) Once the watermarked image is obtained, the SURF algorithm is applied to both the original $I_o(x,y)$ and the watermarked $I_w(x,y)$ images, obtaining the SURF feature points and their invariant descriptor vector for each one respectively. Empirically the parameters used in the SURF algorithm [10] are adjusted as follows: the Hessian response threshold is adjusted to 0.0009, the number of octaves is equal to 5 and the number of filters per octave is equal to 2. Because that not all SURF feature points produce a correct match, the possible SURF feature points that causes false matches need to be eliminated. Hence, a matching operation is carried out by searching for the nearest SURF feature point pairs between the original and the watermarked images. The nearest SURF feature point is defined as the feature point with the minimum Euclidean distance for the invariant descriptor vector. So, after the minimum Euclidean distances are obtained, these are sorted in an array denoted by D in an ascending order. Thus, we obtain the median value δ from the array D and, if the *l-th* Euclidean distance is greater than δ, $D_l > \delta$, then the point is discarded; therefore, the possible SURF feature points that causes false matches are eliminated. Notice that this procedure is not included in the original SURF algorithm [10]. To illustrative purposes, in Fig. 3 we show the object matching by SURF feature point pairs before (a) and after (b) the false match points are removed. In order to show this point depuration process in a more clearly manner the lower part of Fig. 3 isolates the match results.

11) Although more SURF feature points are able to do the calculation of the six affine parameters (two scaling, two rotation and two translation factors) more precise, we do not need to register all of them. Hence, the amount of

Fig. 3. Object matching by SURF feature point pairs before (a) and after (b) the false match points are removed.

the SURF feature points should be adjusted in order to acquire a register file with a small storage cost which allows a faster register and access. For this purpose, we have performed an experiment to find the trade-off between the number of the registered SURF feature points and the performance of the watermarking method. After that the described false match removal process has been applied, taking into account one thousand images with 8/bits per pixel resolution and 512 x 512 dimensions, a watermark pattern with length L = 64, the Hessian response threshold = 0.0009, the number of octaves = 5 and the number of filters per octave = 2 in the SURF algorithm. We have obtained an average of about of 160 SURF feature points. Each descriptor associated with each point is represented by its 64 dimension vector descriptor. Thus, in case of we have registered all SURF features extracted from the image after the false match removal has been applied, the average storage cost of the register file is about 45 kB (compared with the size of each image is 258 kB). In order to reduce the storage cost of the register file, in Fig. 4 we show that 120 SURF feature points are good enough for a high BCR (Bit Correct Rate) when the watermarked image is attacked by an aggressive distortion (JPEG 70+rotation by 105° with auto-crop and re-scaling), and then, the average size of the register file is reduced to about 30 kB, that is small enough for registering and having fast accessing.

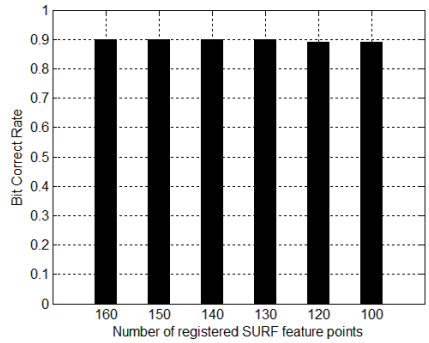

Fig. 4. Dependence of the bit correct rate and the number of registered SURF feature points when an aggressive distortion (JPEG 70+rotation by 105° with auto-crop and re-scaling) is applied to the watermarked images.

4.2 Detection Process

The detection process is described in the following steps: **1)** Empirically using a Hessian response threshold = 0.0009, a number of octaves = 5 and a number of filters per octave = 2, the SURF algorithm is applied to the watermarked image $I_w(x,y)$ in order to obtain the SURF feature points and their invariant descriptor vector.

2) Subsequently, it loads the register file with the SURF feature points registered in advance and performs the object matching by SURF feature points. **3)** Based on the matching results, we calculate the six affine parameters, i.e., two scaling, two rotation and two translation factors. The restoration matrix denoted by MR is given by (9).

$$MR = \begin{bmatrix} s_x & r_x & t_x \\ r_y & s_y & t_y \\ 0 & 0 & 1 \end{bmatrix} . \quad (9)$$

In this matrix s_x and s_y are scaling, r_x and r_y are rotation, t_x and t_y are translation affine parameters, $MR = B_w'/B_o'$, where B_w' and B_o' are the transposed matrices that contains the (x, y) coordinates pairs from the K nearest feature point pairs of both the watermarked and original images respectively, the symbol '/' denotes the division operation. **4)** Apply the restoration matrix MR to the watermarked and possible distorted image in order to obtain the watermarked version restored geometrically. In Fig. 5 we show an example of watermarked image rotated, cropped and re-scaled (a), and the corresponding geometrically restored version (b).

Fig. 5. (a) Watermarked-distorted image. (b) Geometrically restored version.

5) Once the watermarked image is restored, compute the bi-dimensional DFT transform $F'(u,v)$. Then from $F'(u,v)$ the watermarked magnitude $M'(u,v) = |F'(u,v)|$ and phase $P(u,v)$ are obtained. **6)** The annular area A is computed with the same pair of radiuses r_1 and r_2 used in the embedding process. **7)** As in the watermarking process consider the DFT magnitude $M'(u,v)$ divided in four quadrants and compute the result of applying the subtraction operation $so_i = M'_i(u_j,v_j) - M'_i(-u_j,v_j)$ of the first and second quadrants of the upper half part of the watermarked DFT magnitude in the annular region A. **8)** Recover the watermark pattern W' using the sign function as follows: if the $sign(so_i)$ is '+' or '0' then w'_i=1, otherwise w'_i=0, where i = 1,…, L. **9)** Once W' is recovered, re-arrange this using the inverse scrambling procedure respect to the used in the embedding stage. **10)** Reconstruct the original watermark pattern W with the secret key k_1 and obtain the BCR be-

tween W and W'. Assuming ergodicity the BCR is defined as the ratio between the number of correctly decoded bits and the total number of embedded bits. A threshold value T_{BCR} must be defined to determine if the watermark W is present or not into the image. In this concern, considering a binomial distribution with success probability equal to 0.5, the false alarm probability P_{fa} for L watermark data bits is given by (10), and a threshold value T must be controlled in order to this probability P_{fa} is smaller than a predetermined value [12].

$$P_{fa} = \sum_{z=T}^{L} \left(\frac{1}{2}\right)^{L} \cdot \left(\frac{L!}{z!(L-z)!}\right) \tag{10}$$

where L is the total number of watermark data bits, whose value is 64 in our experiments. Empirically we have established that the false alarm probability must be less than $P_{fa} = 3.86 \times 10^{-5}$ for a reliable detection [12] when $T = 48$, and then an adequate threshold value T_{BCR} (= T/L = 48/64) is equal to 0.75. Finally, if the BCR value is greater than the threshold value T_{BCR}, we decide the correct authentication of the watermarked image.

5. Experimental Results

In this section, the performance of the proposed algorithm is evaluated considering the watermark payload, imperceptibility and robustness grades using a variety of well-known in the literature digital images. We have used one thousand images with different texture content (e.g., Goldhill, Sailboat, Lena, Airplane, Baboon, Peppers, among others) of size 512 x 512 and grayscale resolution of 8 bits per pixel which can be found in the follow academic databases: http://sipi.usc.edu/database/, http://dsmc2.eap.gr/files/echrysochos/ and some of them in the Integrated Development Environment (IDE) Matlab ©. Our experiments are carried out on a personal computer running win7© with an AMD© Athlon processor (2.7 GHz) and 4 GB RAM while the embedding and detection procedures were implemented on Matlab© 7.10. A 1D binary pseudorandom sequence of size L = 64 bits is used as the watermark pattern W. The false alarm probability is set to $P_{fa} = 3.86 \times 10^{-5}$ when T_{BCR} =0.75. Determined by the experimentation described in the following paragraph the pair of radiuses used in the embedding process were r_1 =80 and r_2 =81. The watermark strength used in the embedding is equal to α = 55. As mentioned in previous sections the parameters used to obtain the SURF points are: the Hessian response threshold = 0.0009, the number of octaves to analyze = 5 and the number of filters per octave = 2.The watermarked image quality is measured using the following well known indices Peak Signal to Noise Ratio (PSNR), Visual Information Fidelity (VIF) and Structural Similarity Index (SSIM). Finally, our experimental results are compared with the principal methods reported previously against most common geometric and signal processing attacks.

5.1 Setting of Radiuses r_1 and r_2

Considering a watermark strength α = 55, we have considered a pair of experimental radiuses r_1 =19, r_2 =24 for low, r_1 =80, r_2 =81 for middle, and r_1 =252, r_2 =253 for high DFT magnitude frequency respectively, and a value of L = 64, in Fig. 6 we show the average PSNR after the watermark embedding in each of the selected spectral region, obtaining 39.69 dB for low, 46.85 for middle, and 47.48 for high DFT magnitude frequency respectively. Although it may be considered that an acceptable average PSNR is 39.69 dB, the modifications in the magnitude of lower frequencies of the DFT will cause visible distortion in the spatial domain of the image.

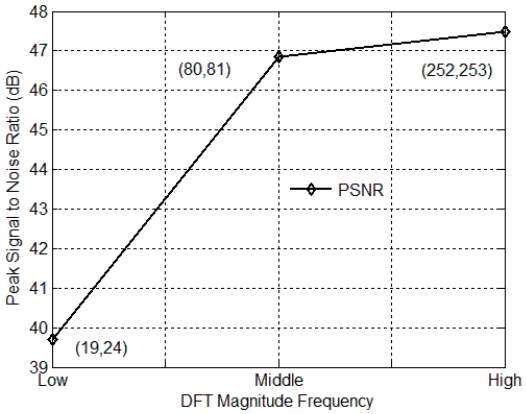

Fig. 6. Average PSNR after the watermark embedding in each spectral region. Radiuses r_1 = 19, r_2 = 24 for low, r_1 = 80, r_2 = 81 for middle, and r_1 = 252, r_2 = 253 for high DFT magnitude frequency.

To illustrate the visible distortions in the spatial domain, in Fig. 7 we show the watermarked Lena image when watermark was embedded into the low (a), middle (b), and high (c) DFT magnitude frequency, with 39.05 dB, 46.51 dB, and 48.7 6dB respectively.

Fig. 7. Visible distortions in the spatial domain from watermarked Lena image when watermark was embedded into the low (a), middle (b), and high (c) DFT magnitude frequency, with 39.05 dB, 46.51dB, and 48.76 dB respectively.

On the other hand, the magnitudes of the higher frequencies are vulnerable to the JPEG compression. Considering the same parameters used in the above experiment, in the follow experiment a JPEG compression with quality factor equal to 20 is applied to the watermarked image. In Fig. 8 we show the average BCR after the watermark embedding in each spectral region, obtaining 0.82 for low,

0.89 for middle, and 0.59 for high DFT magnitude frequency respectively.

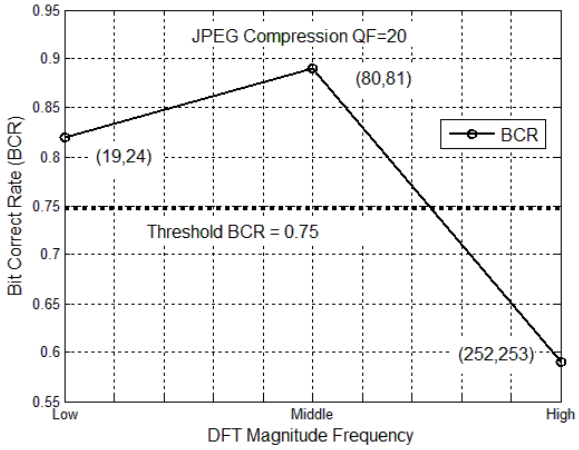

Fig. 8. Average BCR after the watermark embedding in each spectral region. BCR = 0.82 for low, BCR = 0.89 for middle, and BCR = 0.59 for high DFT magnitude frequency respectively.

In low and middle frequencies we have obtained BCR values greater than the threshold value T_{BCR} = 0.75, however, using the high frequencies, the BCR value is less than the threshold value T_{BCR} = 0.75, confirming the vulnerability of the higher frequencies against JPEG compression. As a conclusion, the watermark pattern should be embedded in the band of the middle frequencies r_1 = 80, r_2 = 81 because, in this spectral region, it will be robust against JPEG compression, and at the same time imperceptible.

5.2 Watermark Payload

Considering a watermark strength α = 55, a pair of radius r_1 = 80 and r_2 = 81, the SURF parameters mentioned above, ten watermarked test images for illustrative purposes, and variable value of L from 64 to 1024 bits, in Fig. 9 we show that a large value of L would increase the capacity of the watermarking method, however, the robustness of watermarking algorithm would decrease for large L. Hence, there is also a tradeoff between capacity and robustness.

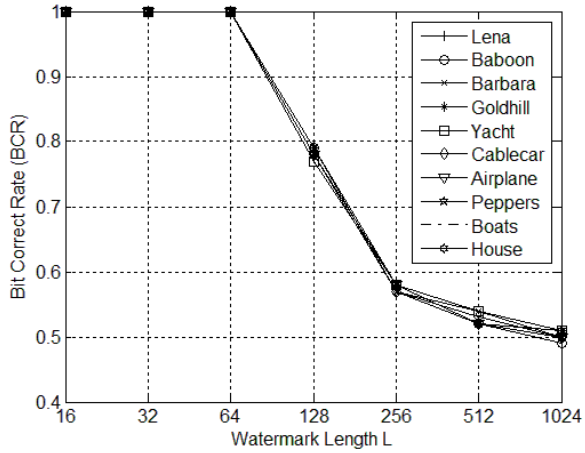

Fig. 9. Bit correct rate with watermark length L variable.

From Fig. 9 we show that for L = 16 to 64, the BCR obtained is in its limit value 1, which indicates a good performance in robustness terms. On the other hand, while the value of L is increased, the robustness is affected. According to this behavior, L = 16, 32 or 64 are considered as a suitable set of values. In order to preserve the trade-off between capacity, robustness and imperceptibility, in the proposed watermarking method we have adopted the value L = 64 in conjunction with the rest of the embedding parameters.

5.3 Watermark Imperceptibility and Setting of Watermark Strength α

Using a pair of radius r_1 =80 and r_2 =81, the SURF parameters mentioned above, a watermark length L = 64, and a variable watermark strength α from 10 to 100; the watermark imperceptibility was evaluated in terms of the PSNR, VIF [18] and SSIM [19] image quality metrics defined by (11), (12) and (13) respectively.

$$PSNR(dB) = 10\log_{10}\left(\frac{N_1 \cdot N_2 \cdot 255^2}{\sum_{x=1}^{N_1}\sum_{y=1}^{N_2}\left(I_o(x,y) - I_w(x,y)\right)^2}\right), \quad (11)$$

$$VIF = \frac{\sum_{\omega \in channels} I(\vec{C}^{Z,\omega}; \vec{G}^{Z,\omega} \mid s^{Z,\omega})}{\sum_{\omega \in channels} I(\vec{C}^{Z,\omega}; \vec{E}^{Z,\omega} \mid s^{Z,\omega})}. \quad (12)$$

In (12) we sum over the channels of interest, where $\vec{C}^{Z,\omega}$ represent Z elements of the random field RF C_ω that describes the coefficients from channel ω, and so on [18]. E and G denote the visual signal at the output of the Human Visual System Model (HVS) from the original and the watermarked images respectively, from which the brain extracts cognitive information. $I(\vec{C}^{Z,\omega}; \vec{E}^{Z,\omega} \mid s^{Z,\omega})$ and $I(\vec{C}^{Z,\omega}; \vec{G}^{Z,\omega} \mid s^{Z,\omega})$ represent the information that can ideally be extracted by the brain from a particular channel in the original and the watermarked images respectively [18].

$$SSIM(I_o, I_w) = \frac{(2\mu_{I_o}\mu_{I_w} + C_1)(2\sigma_{I_o I_w} + C_2)}{(\mu_{I_o}^2 + \mu_{I_w}^2 + C_1)(\sigma_{I_o}^2 + \sigma_{I_w}^2 + C_2)}. \quad (13)$$

I_o, I_w are the original and watermarked images respectively and C_1, C_2 are small constant values [19]. As it is known in the literature the VIF value reflects perceptual distortions more precisely than PSNR. The range of VIF is [0, 1] and the closer value to 1 represents the better fidelity respect to the original image. Also it is well known in the literature that the SSIM value reflects perceptual distortions more precisely than PSNR. The range of SSIM is [0, 1], and the closer value to 1 represents the better quality respect to the original image, a value 1 indicates that the original and the reference images are the same. In Figs. 10 and 11, the average PSNR and VIF-SSIM are plotted versus the variable watermark strength α ranging from 10 to 100 respectively.

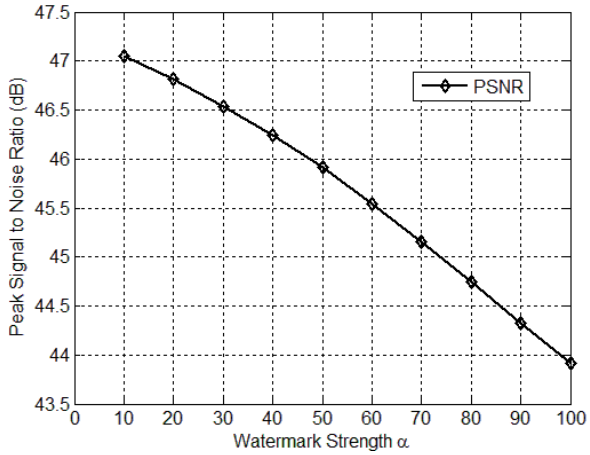

Fig. 10. Average PSNR (dB) obtained with variable watermark strength α.

A larger value of α would increase the robustness of the watermark, but as shown in Figs. 10 and 11, the watermark imperceptibility is diminished. Hence there is a trade-off between robustness and imperceptibility. To preserve the trade-off between robustness and imperceptibility, based on our experiments, we considered a watermark strength of $\alpha = 55$ as a suitable value, obtaining the follow average values: PSNR = 45.91 dB, VIF = 0.9692 and SSIM = 0.9955.

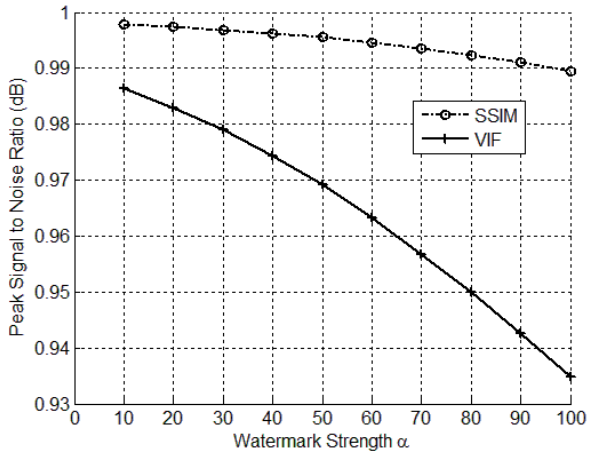

Fig. 11. Average VIF and SSIM obtained with variable watermark strength α.

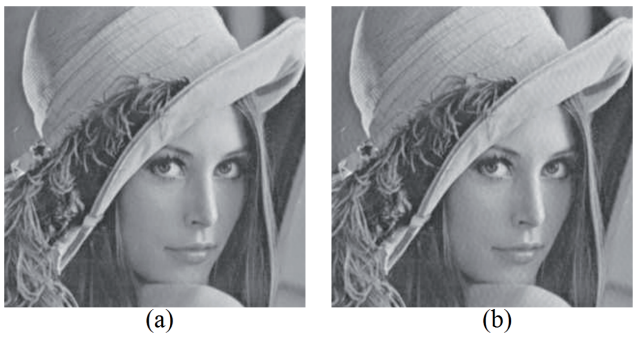

Fig. 12. Perceptible noise effect (a) Zoom region of the watermarked Lena image with α= 55 and PSNR = 46.51 dB. (b) Zoom region of the watermarked Lena image with α =100 and PSNR = 40.05 dB.

Although a PSNR above 40 dB with $\alpha = 100$ may be considered as an acceptable value, values of watermark strength greater than 60 approximately, causes a perceptible noise effect in the image. This effect is shown Fig. 12. To avoid the perceptibility of the noise effect and to preserve the trade-off between robustness and imperceptibility, based on our experiments, we considered a watermark strength $\alpha = 55$ as a suitable value.

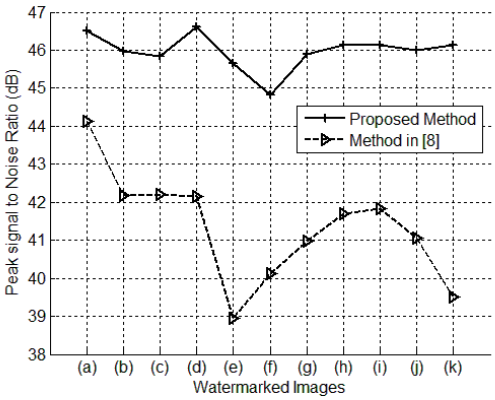

Fig. 13. PSNR (dB) obtained from the proposed method and the reported in [8].

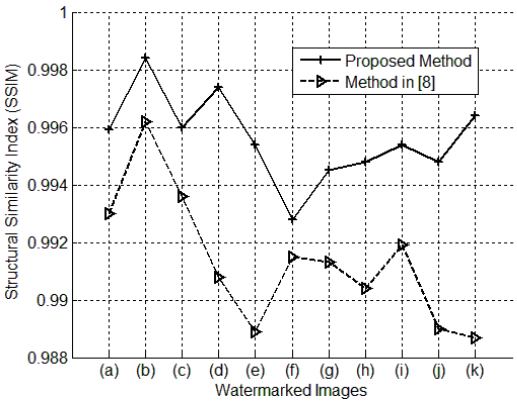

Fig. 14. SSIM obtained from the proposed method and the reported in [8].

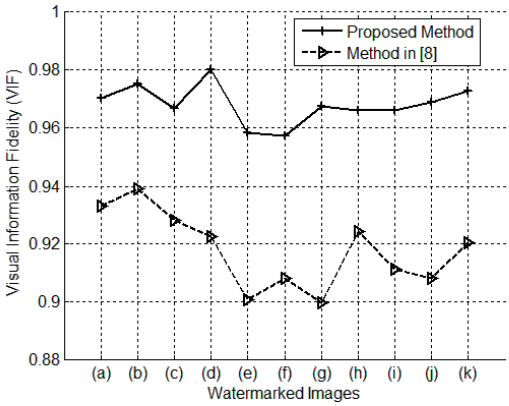

Fig. 15. VIF obtained from the proposed method and the reported in [8].

In order to carry out an equitable comparison in terms of watermark imperceptibility with respect to the related

work reported in [8], Figs. 13, 14 and 15 show the values of PSNR, SSIM and VIF respectively of eleven watermarked test images respect to the original ones. The watermarked test images are labeled as follows: (a) Lena, (b) Baboon, (c) Barbara, (d) Gold hill, (e) Yacht, (f) Cable car, (g) Airplane, (h) Peppers, (i) Boats, (j) Man and (k) House, then the x axis in Figs. 13, 14 and 15 is showed in a clearer manner.

From Figs. 13, 14 and 15 we show that our proposed method improves the watermark imperceptibility with respect to the algorithm in [8]. Thus, respect to the eleven watermarked test images, our proposed method obtain an average PSNR = 45.97 dB, SSIM = 0.9956, and VIF = 0.9682, meanwhile, using the reported method in [8] we obtain an average PSNR = 41.34 dB, SSIM = 0.9914, and VIF = 0.9179. To illustrative purposes, Fig. 16 shows one

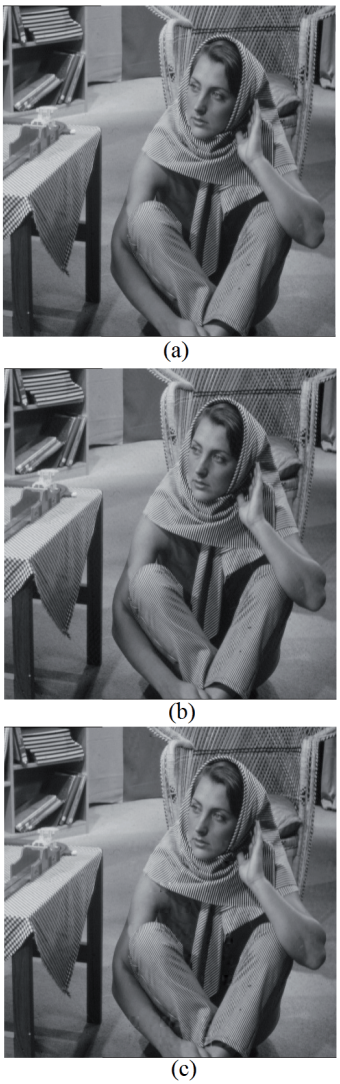

Fig. 16. Original Barbara image (a), watermarked by our proposed method (b) and watermarked using the method in [8] (c).

of the more used in the literature watermarked test image (Barbara) employing our proposed method, and the described in [8]. The original version is denoted by (a), the watermarked test image using our proposed method by (b) and finally, the watermarked image by the algorithm presented in [8] by (c).

From Fig. 16 we show that our proposed method provides a fairly good fidelity of the watermarked image. Moreover, some watermarked images by the method in [8] have shown some blocking artifacts perceptible by the Human Visual System (HVS).

5.4 Watermark Robustness

To evaluate the watermark robustness of the proposed algorithm, the StirMark Benchmark [20], combined attacks of several geometrical distortions, and common signal processing are applied. In order to carry out a representative comparison in terms of watermark robustness with respect to the related work reported in [8], we have used one thousand grayscale images with resolution of 8 bits per pixel of size 512 x 512, taking into account the whole image as the "object". Experimental results are classified in geometric, common signal processing, and combined distortions. For illustrative purposes, in Tab. 2 we show the average BCR obtained in our proposed method and the scheme reported in [8], after applying geometric distortions, and combined distortions composed by a JPEG compression with quality factor QF = 70 together with one or more geometric distortions. When the BCR value is less than the predefined threshold value T_{BCR} =0.75 (less than 48 correct bits), the watermark detection is reported in cursive typeface and corresponds to the case where the watermark detection has failed.

Analyzing the results in Tab. 2, we show that our proposed method presents good robustness against several geometric distortions, including scaling from 0.5 to 2, rotation by all angles, general affine transformation, shearing 20% in x and y directions, centered and common cropping attack with 30% and 35% respectively, aspect ratio in x and y directions by 0.8 and 1.2, respectively, translation by $x = 30$ and $y = 30$, local random bending, and combined attacks all of them with JPEG 70 compression. In all cases we have obtained BCR values greater than the predefined threshold value $T_{BCR} = 0.75$. On the other hand, the method proposed in [8] obtains a similar performance against the above mentioned geometric and combined distortions; however, the method is not robust against cropping attacks, i.e., cropping with 35% and re-scaling, centered cropping with 30%, translation by $x = 30$ and $y = 30$ with crop, and their combination with JPEG 70 compression, as well as local random bending. The obtaining BCR values are equal or less than the predefined threshold value $T_{BCR} = 0.75$. Its weakness is due to several watermarked DCT blocks, whose position was selected in a randomly manner into the object, are removed or its positions are changed when the object region is translated by x, y pixels, or cropped from the center or the edges. Thus, even though the watermark pattern was embedded in a redundantly manner, the watermark cannot be recovered adequately.

Geometric and combined distortions	Proposed Method	Method in [8]
Without distortion	1	1
Rotation by 35°	0.96	0.97
Rotation by 25°, auto-crop and re-scaling	0.93	0.90
Scale 0.5	0.90	0.88
Scale 2	1	0.96
Affine [0.9,0.2,0;0.1,1.2,0;0,0,1]	0.97	0.96
Shearing (0, 20%)	0.98	0.99
Shearing (20%, 0)	0.98	0.98
Cropping 35 % with re-scaling	0.87	*0.75*
Centered cropping 30% off	0.89	*0.70*
Aspect Ratio (1.0,1.2)	0.98	0.98
Aspect Ratio (0.8,1.0)	0.99	0.98
Translation x=30, y=30	0.98	*0.50*
JPEG 70 + Rotation 15 °	0.95	0.96
JPEG 70 + Scale 1.5	0.99	0.94
JPEG 70 + Affine[0.9,0.2,0;0.1,1.2,0;0,0,1]	0.97	0.96
JPEG 70 + Cropping 35% with re-scaling	0.89	*0.75*
JPEG 70 + Centered cropping 30% off	0.98	*0.70*
JPEG 70 + Rotation by 20° auto-crop and re-scaling	0.90	0.90
JPEG 70 + Shearing (0, 20%)	0.96	0.96
JPEG 70 + Shearing (20%, 0)	0.98	0.97
JPEG 70 + Aspect Ratio (1.0,1.2)	1	0.98
JPEG 70 + Aspect Ratio (0.8,1.0)	0.98	0.98
JPEG 70 + Translation x=30, y=30	0.97	*0.51*
Local random bending	0.76	*0.74*

Tab. 2. Average BCR obtained from watermarked images after geometric and combined distortions.

Additionally, Tab. 3 shows the average BCR obtained in our proposed method and the scheme reported in [8], after applying common signal processing, and combined attacks composed by a JPEG compression with quality factor QF = 90 together with image filtering. Similarly, when the BCR value is less than the predefined threshold value T_{BCR} =0.75 (less than 48 correct bits), the watermark detection is reported in cursive typeface and corresponds to the case where the watermark detection has failed.

Analyzing the results in Tab. 3 we show that both algorithms present good robustness against several common signal processing operations, including JPEG compression with several quality factors ranging from 70 to 30. Also both present robustness against adjust intensity grayscale, impulsive noise with a density of 0.005, Gaussian noise contamination with zero mean and variance 0.003. Several filters including median and Gaussian with window 3x3, sharpening by 3x3 and histogram equalization are also considered. In all cases both algorithms have a BCR value greater than the predefined normalized threshold value T_{BCR} = 0.75. Also, we have considered combined attacks composed by a JPEG 90 compression together with common signal processing, specifically median, Gaussian and sharpen filters, all of them with window size of 3x3. The robustness of both methods is not affected by this kind of combined attacks, obtaining BCR values greater than T_{BCR} = 0.75. However, the method in [8] is not robust against motion blurred filter, obtaining BCR values equal or less than the threshold T_{BCR} = 0.75.

Signal processing and combined distortions	Proposed method	Method in [8]
JPEG Compression QF = 70	0.96	0.95
JPEG Compression QF = 50	0.95	0.94
JPEG Compression QF = 30	0.93	0.94
Adjust intensity grayscale	0.96	0.91
Impulsive Noise, density = 0.02	0.93	0.90
Gaussian Noise, μ = 0, σ^2 = 0.005	0.88	0.90
Median filter 3x 3	0.98	0.90
Sharpening 3 x 3	0.98	0.97
Gaussian filter 3x3	0.99	0.93
Motion blurred filter	0.87	*0.75*
Histogram equalization	0.95	0.92
JPEG 90 + Median filter 3x 3	0.98	0.90
JPEG 90 + Sharpening 3 x 3	0.98	0.97
JPEG 90 + Gaussian filter 3x3	0.99	0.93

Tab. 3. Average BCR obtained from watermarked images after common signal processing, and combined distortions.

Parameters	Lei-da et al. [13]	Wang et al. [15]	Pham et al. [8]	Proposed method
JPEG (QF)	50-100	30-100	20-100	20-100
Scaling	0.7 – 1.5	0.8 – 1.2	0.4 – 1.2	0.5 – 2
Cropping	-	up to 10%	fail	up to 35%
Affine	-	-	detected	detected
Translation	detected	x=20, y=20	fail	x=110, y=110
Rotation	detected	detected	0° - 360°	0° - 360°
Median Filter	3x3	3x3	5x5	3x3
Gaussian Noise	detected	detected	detected	detected
Original image	blind	blind	semi-blind, use register file	semi-blind, use register file
Watermark length	128 bits	32 bits	83 bits	64 bits

Tab. 4. Performance comparison.

Tab. 4 shows the performance comparisons together with the watermark detection methods (depending on the method blind or original image can be required) and the watermark length associated with each scheme. These results show better performance of the proposed method compared with principal methods reported previously against most common geometric and signal processing attacks. Particularly the robustness against aggressive attacks such as affine transformation, translation and cropping image is shown. A dash '-' in this table indicates that the result is not reported in the literature.

5.5 Detector Capability

Considering the false alarm probability as the probability of detecting erroneously a watermark when actually the image is not watermarked, and the false rejection probability as the probability of that the detector cannot detect the watermark when the image is watermarked, as an evaluation of the robustness the *Receiver Operating Characteristics* (ROC) curves are obtained under each attack. To perform a fair comparison, scaling by a factor 0.4, cropping 35% with re-scaling, translation by $x = 30$, $y = 30$, JPEG compression by QF = 30, 3x3 median filtering, and Gaussian noise with $\mu = 0$ and variance $\sigma^2 = 0.005$ are considered as representative attacks in both algorithms. These comparisons are shown in Figs. 17–22, respectively. In order to appreciate in a better way the performance of both algorithms a zoom from the plot is shown into each figure.

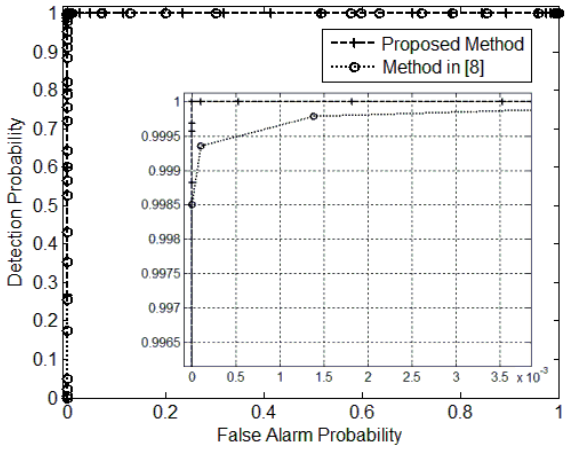

Fig. 17. ROC curves for scaling by factor 0.4.

In Fig. 17 we can observe that the method in [8] has a detection probability equal to 0.9118, meanwhile our proposed method has a detection probability equal to 1, when $P_{fa} = 3.86 \times 10^{-5}$. According to these results, both algorithms present a good detection performance against this geometric distortion.

In Fig. 18 when the watermarked image is distorted by cropping 35% with re-scaling we observe that the method in [8] has a detection probability equal to 0.3883, meanwhile our proposed method has a detection probability equal to 0.9847, when $P_{fa} = 3.86 \times 10^{-5}$. According to these results, our proposed algorithm presents a good detection performance against this attack and outperforms the method presented in [8].

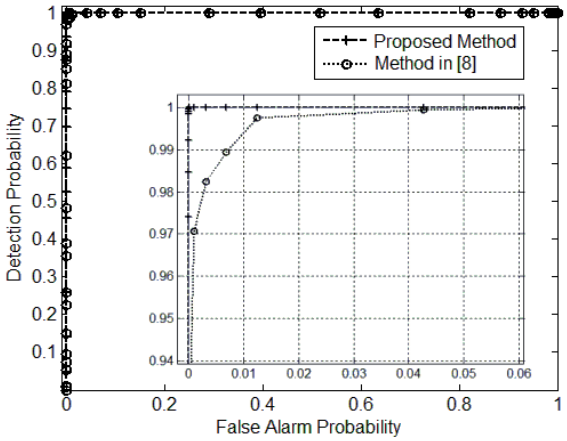

Fig. 18. ROC curves for cropping 35% with re-scaling.

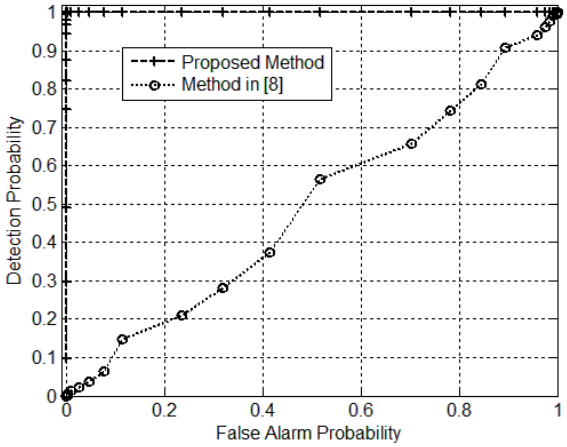

Fig. 19. ROC curves for translation by $x = 30$ and $y = 30$.

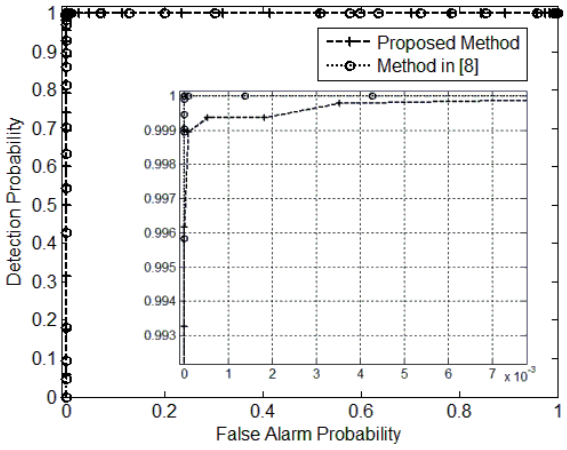

Fig. 20. ROC curves for JPEG compression with quality factor QF = 30.

In Fig. 19 when the watermarked image is distorted by a translation by $x = 30$ and $y = 30$ we observe that the method in [8] has a detection probability equal to 0, meanwhile our proposed method has a detection probability equal to 1, when $P_{fa} = 3.86 \times 10^{-5}$. According to these re-

sults, our proposed algorithm presents a very good detection performance against this attack and outperforms the method presented in [8].

In Fig. 20 we observe that the method in [8] has a detection probability equal to 0.9990, meanwhile our proposed method has a detection probability equal to 0.9933, when $P_{fa} = 3.86 \times 10^{-5}$. According to these results, both algorithms present a good detection performance against this compression method.

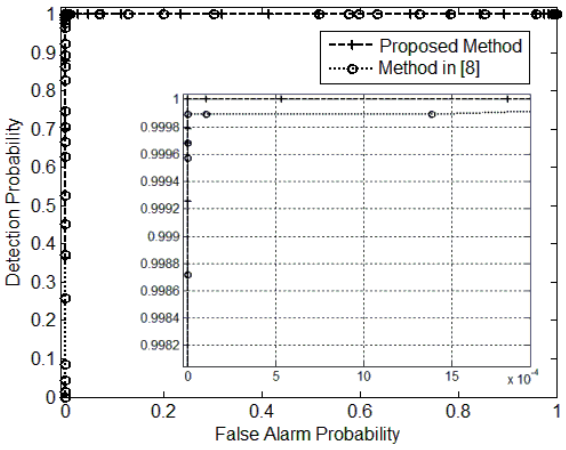

Fig. 21. ROC curves for median filtering attack with window size 3x3.

In Fig. 21 we observe that the method in [8] has a detection probability equal to 0.9774, meanwhile our proposed method has a detection probability equal to 1, when $P_{fa} = 3.86 \times 10^{-5}$. According to these results, both algorithms present a good detection performance against this signal processing attack.

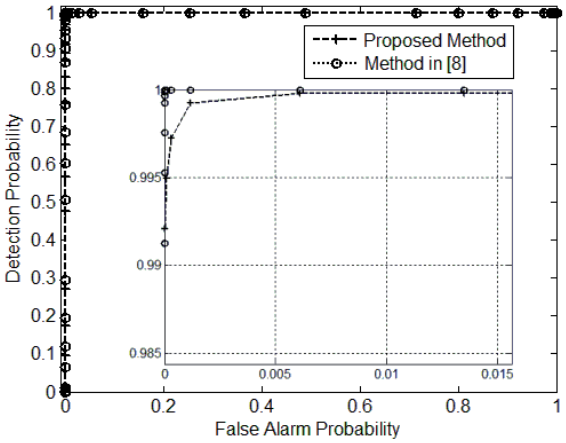

Fig. 22. ROC curves for Gaussian noise attack with $\mu = 0$ and variance $\sigma^2 = 0.005$.

In Fig. 22 when the watermarked image is corrupted by Gaussian noise with $\mu = 0$ and variance $\sigma^2 = 0.005$we observe that the method in [8] has a detection probability equal to 0.9912, meanwhile our proposed method has a detection probability equal to 0.8957, when $P_{fa} = 3.86 \times 10^{-5}$. According to these results, the proposed algorithm in [8] presents a good detection performance against this attack and outperforms the proposed method. Finally, a summary of the detector capability of both algorithms when $P_{fa} = 3.86 \times 10^{-5}$ is shown in Tab. 5.

Distortion	Proposed Method	Method in [8]
Scaling by factor 0.4	1	0.91
Cropping 35 % with re-scaling	0.98	*0.38*
Translation x=30, y=30	1	*0*
JPEG compression by QF = 30	0.99	0.99
Median filtering 3x3	1	0.97
Gaussian Noise μ=0, σ^2=0.005	0.89	0.99

Tab. 5. Detection probability for several distortions when the false alarm probability is equal to $P_{fa} = 3.86 \times 10^{-5}$.

6. Conclusions

Using the combination of the object matching by SURF feature points and the robustness of the DFT-based watermarking method; we have developed a robust object-based watermarking using SURF feature matching and DFT domain algorithm. There are three main key elements in our method: a) the speeded up robust feature points, b) DFT embedding domain, c) object matching by SURF feature points. The watermark imperceptibility of the proposed algorithm is evaluated in terms of three well known in the literature image quality assessment methods (PSNR, VIF and SSIM), concluding that the visual distortion caused by the proposed watermarking algorithm is imperceptible, providing 45.91 dB, 0.9692, and 0.9955 respectively. The watermark robustness of the proposed algorithm is evaluated using a wide range of attacks and a fairly good performance is obtained. From the evaluation results, we can conclude that our proposed algorithm outperforms the algorithm proposed in [8] that is one of the most efficient algorithms recently proposed for image watermarking. The experimental results show that our proposed method is robust against very aggressive attacks, such as scaling with a factor of 0.5, all angle rotation, translation by a given amount of pixels, cropping up to 35%, general affine transformation, aspect ratio change, local random bending, JPEG compression with quality factor equal to 20, histogram equalization, sharpening, motion blurred filter and combined attacks. Feature matching watermarking algorithms are considered as informed watermarking techniques, because they use a reference or register file to resynchronize the watermark detection stage. Although this reference may be considered as a drawback, the size of the register file is of about 30 kB, which is not a significant problem for a storage cost and accessing speed. In fact in a similar method based also on feature matching [8], the register file can be considered as a large secret key that is often used by others watermarking methods. The robustness against several geometric, signal processing, combined attacks and the high imperceptibility of our proposed method make it to be a good proposition in a wide range of applications. As a future work, the proposed method will be extended to authentication of digital video.

Acknowledgements

We thank the Post-Doctoral Scholarships Program and PAPIIT IN-112513 project from DGAPA in the National Autonomous University of Mexico (UNAM) and the National Polytechnic Institute (IPN) of Mexico by the support provided during the realization of this research.

References

[1] LANGELAAR, G. C., SETYAWAN, I., LAGENDIJK, R. L. Watermarking digital image and video data. *IEEE Signal Processing Magazine*, 2000, vol. 17, p. 20–46.

[2] BARNI, M., BARTOLINI, F. *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications*. Marcel Dekker, 2004.

[3] COX, I. J., MILLER, M. L., BLOOM, J. *Digital Watermarking*. Morgan Kaufmann, 2001.

[4] COX, I. J., MILLER, M. L. The first 50 years of electronic watermarking. *EURASIP J. of Applied Signal Processing*, 2002, vol. 2, p. 126–132.

[5] DAJUN, H., SUN, Q., TIAN, Q. A secure and robust object-based authentication system. *EURASIP J. Applied Signal Processing*, 2004, vol. 14, p. 1–14.

[6] HO, Y. K., WU, M. Y. Robust object-based watermarking scheme via shape self-similarity segmentation. *Pattern Recognition Letters*, 2004, vol. 25, no. 15, p. 1673-1680.

[7] LEE, J. S., KIM, W. Y. A new object-based image watermarking robust to geometrical attacks. In *Pacific-Rim Conference on Multimedia (PCM)*, 2004, vol. 2, p. 58–64.

[8] PHAM, V. Q., MIYAKI, T., YAMASAKI, T., AIZAWA, K. Robust object-based watermarking using feature matching. *IEICE Trans. on Information and Systems*, 2008, vol. E91-D(7), p. 2027 to 2034.

[9] LOWE, D. Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, 2004, vol. 60, no. 2, p. 91–110.

[10] BAY, H., ESS, A., TUYTELAARS, T., VAN GOOL, L. SURF: Speeded Up Robust Features. *Computer Vision and Image Understanding (CVIU)*, 2008, vol. 110, no. 3, p. 346-359.

[11] BAS, P., CHASSERY, J. M., MACQ, B. Geometrically invariant watermarking using feature points. *IEEE Transactions on Image Processing*, 2002, vol. 11, no. 9, p. 1014-1028.

[12] TANG, C. W., HANG, H. M. A feature-based robust digital image watermarking scheme. *IEEE Transactions on Signal Processing*, 2003, vol. 51, no. 4, p. 950-959.

[13] LEI-DA, L., BAO-LONG, G., LEI, G. Rotation, scaling and translation invariant image watermarking using feature points. *The Journal of China Universities of Post and Telecommunications*, 2008, vol. 15, no. 2, p. 82-87.

[14] KUTTER, M., BHATTACHARJEE, S. K., EBRAHIMI, T. Towards second generation watermarking schemes. In *Proceedings of IEEE ICIP*. Kobe (Japan), 1999, p. 320-323.

[15] WANG, X., HOU, L., WU, J. A feature-based robust digital image watermarking against geometric attacks. *Image and Vision Computing,* 2008, vol. 26, no. 7, p. 980-989.

[16] LEE, H. Y., KIM, H., LEE, H. K. Robust image watermarking using local invariant features. *Optical Engineering*, 2006, vol. 45, no. 3, 037002.

[17] CHEN, W., et al. Efficient extraction of robust image features on mobile devices. In *6th IEEE and ACM International Symposium on Mixed and Augmented Reality, ISMAR*, 2007, p. 287–288.

[18] SHEIKH, H. R., BOVIK, A. C. Image information and visual quality. *IEEE Transactions on Image Processing*, 2006, vol. 15, no. 2, p. 430-444.

[19] WANG, Z., BOVIK, A. C., SHEIKH, H. R., SIMONCELLI, E. P. Image quality assessment: From error measurement to structural similarity. *IEEE Transactions on Image Processing*, 2004, vol. 13, no. 4, p. 600–612.

[20] StirMark 4.0 available online: http://www.petitcolas.net/fabien/watermarking/stirmark/

About Authors …

Manuel CEDILLO-HERNANDEZ was born in Mexico. He received the B.S. degree in Computer Engineering, M.S. degree in Microelectronics Engineering and his PhD in Communications and Electronic in the National Polytechnic Institute IPN, Mexico in 2003, 2006 and 2011, respectively. From August 2005 to August 2011 he was in the Federal Electoral Institute (IFE) and Government Secretary (SEGOB) of Mexico in several Information Technologies areas. Currently, he courses a postdoctoral residence at the Electric Engineering Division, Engineering Faculty, National Autonomous University of Mexico UNAM. His principal research interests are image and video processing, digital watermarking, software development and related fields.

Francisco GARCIA-UGALDE was born in Mexico. He obtained his bachelor in 1977 in Electronics and Electrical System Engineering from the National Autonomous University of Mexico, his Diplôme d'Ingénieur in 1980 from SUPELEC France, and his PhD in Information Processing from Université de Rennes I, France, in 1982. Since 1983 is a full-time professor at UNAM, Engineering Faculty. His current interest fields are: Digital filter design tools, analysis and design of digital filters, image and video coding, image analysis, watermarking, theory and applications of error control coding, turbo coding, applications of cryptography, parallel processing and data bases.

Mariko NAKANO-MIYATAKE was born in Japan. She received the M.E. degree in Electrical Engineering from the University of Electro-Communications, Tokyo Japan in 1985, and her Ph.D. in Electrical Engineering from the Universidad Autonoma Metropolitana (UAM), Mexico City, in 1998. From July 1992 to February 1997 she was with the Department of Electrical Engineering, UAM Mexico. In February 1997, she joined the Graduate Department of the Mechanical and Electrical Engineering School, National Polytechnic Institute of Mexico, where she is now a Professor. Her research interests are in information security, image processing, pattern recognition and related fields.

Hector PEREZ-MEANA was born in Mexico. He received his M.S: Degree in Electrical Engineering from the Electro-Communications University of Tokyo Japan in 1986 and his Ph. D. degree in Electrical Engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1989. From March 1989 to September 1991, he was a visiting researcher at Fujitsu Laboratories Ltd, Kawasaki, Japan. From September 1991 to February 1997 he was with the Electrical Engineering Department of the Metropolitan University of Mexico City where he was a Professor. In February 1997, he joined the Graduate Studies and Research Section of the Mechanical and Electrical Engineering School, National Polytechnic Institute of Mexico, where he is now a Professor. His principal research interests are adaptive systems, image processing, pattern recognition, watermarking and related fields.