PAPER

A Visible Watermarking with Automated Location Technique for Copyright Protection of Portrait Images

Antonio CEDILLO-HERNANDEZ[†a)], **Manuel CEDILLO-HERNANDEZ**[††], **Francisco GARCIA-UGALDE**[†], **Mariko NAKANO-MIYATAKE**[††], ***Nonmembers***, ***and*** **Hector PEREZ-MEANA**[††], ***Member***

SUMMARY A visible watermarking technique to provide copyright protection for portrait images is proposed in this paper. The proposal is focused on real-world applications where a portrait image is printed and illegitimately used for commercial purposes. It is well known that this is one of the most difficult challenges to prove ownership through current watermark techniques. We propose an original approach which avoids the deficiencies of typical watermarking methods in practical scenarios by introducing a smart process to automatically detect the most suitable region of the portrait image, where the visible watermark goes unnoticed to the naked eye of a viewer and is robust enough to remain visible when printed. The position of the watermark is determined by performing an analysis of the portrait image characteristics taking into account several conditions of their spatial information together with human visual system properties. Once the location is set, the watermark embedding process is performed adaptively by creating a contrast effect between the watermark and its background. Several experiments are performed to illustrate the proper functioning of the proposed watermark algorithm on portrait images with different characteristics, including dimensions, backgrounds, illumination and texture, with the conclusion that it can be applied in many practical situations.

key words: *visible watermarking, copyright protection, portrait images, human visual system*

1. Introduction

Digital watermarking has emerged as a way to claim the ownership of an image through embedding copyright data such that this information remains on the host image even after a variety of attacks have been performed [1]–[3]. Digital watermarking techniques can be broadly classified into invisible approaches, which have yielded a lot of interesting proposals in the last decade [4]–[6]; and visible approaches where in contrast, little work has been done [7]–[10]. In invisible watermarking approaches, the copyright data is robustly embedded as a secondary signal that remains imperceptible to human vision. Since the human eye is unable to differentiate between the original and watermarked image, auxiliary modules are deployed to retrieve the embedded information and thus prove the image ownership [11]. There are some major problems that may affect the success of the above operation: the possibility to embed a counterfeited watermark signal into the already protected data [12] and the lack of an appropriate legal framework for a digital environment [13]. Since these issues have not been resolved, visible watermarking techniques are chosen in practical scenarios. In these approaches a secondary image is embedded such that it is intentionally perceptible to human observers, thus helping to prevent or at least discourage unauthorized use of copyrighted images. Contrary to what happens with invisible approaches, in visual watermarking the claim of ownership can occur immediately [13]. Nevertheless, the visible watermark inevitably alters the visual content thus reducing the readability and commercial value of the original image.

In this paper we propose an original visible watermarking approach that improves the above mentioned deficiencies for both visible and invisible watermarking methods in practical scenarios. This research is focused on providing copyright protection when a portrait image is severely edited with the misled aim to be printed for commercial purposes. With this purpose, we introduce a smart process to automatically detect the most suitable region of the portrait image where the visible watermark can be embedded by passing unnoticed to the naked eye of a viewer and being robust enough to remain visible after printing process. Our proposal is based on a detailed analysis of the spatial information of the portrait image and considering the Human Visual System (HVS) properties. HVS properties such as luminance and texture are often utilized in invisible watermarking approaches [14], [15]. Hence, the location of such regions within an image may help to adapt the distortion caused by the watermarking embedding process and permits to take advantage of the reduced capability to detect such changes by the human eye. Please note that even though our proposal is based on HVS properties, its approach is substantially different. As will be shown later, to consider HVS properties within a traditional approach may result insufficient to provide a suitable watermark location that satisfies the issues raised in this proposal. Instead, a detailed analysis of the portrait image content is performed and the final watermark location must meet with several conditions to ensure their proper operation. Once the most suitable position has been found, the visible watermark is adjusted and then embedded in the original image by creating a contrast effect with its background. Since there is no formally defined process in the literature to determine the presence of a visible

Manuscript received October 6, 2015.
Manuscript revised January 17, 2016.
Manuscript publicized March 10, 2016.

[†]The authors are with Universidad Nacional Autónoma de México, Circuito Exterior, Ciudad Universitaria, Coyoacan, 04510, Mexico City, Mexico.

[††]The authors are with Instituto Politécnico Nacional, Av. Santa Ana 1000, San Francisco Culhuacan, Coyoacan, 04430 Mexico City, Mexico.

a) E-mail: antoniochz@hotmail.com

DOI: 10.1587/transinf.2015EDP7412

watermark, watermark detection process is performed by a visual inspection of the watermarked image validated by a user key. In this way, our proposal aims to allow the detection of the visible watermark after the edition and printing process and thus is able to demonstrate the ownership of a copyrighted image. The rest of the paper is organized as follows: Sect. 2 provides a description of related works to resolve the addressed problem. In Sect. 3, the proposed algorithm including the algorithms to locate the most suitable watermark location, adjust the size of the visual watermark and the watermark embedding process are explained in detail. The results of experiments on the proposed technique are shown in Sect. 4, and finally Sect. 5 concludes this work.

2. Related Works

In practical situations, one of the most difficult challenges for digital watermarking techniques consists of getting the ability to demonstrate the property of a copyrighted image even after it is affected by an editing process in order to be printed and used by unauthorized people with commercial purposes, for example, as a cover of a magazine, book, etc. Due to their nature, portrait images belong to an important class of images that are vulnerable to such misuse. An example of the above mentioned situation is illustrated in Fig. 1, where a portrait image (Fig. 1 (a)) has been edited in order to be used as a cover of a magazine (Fig. 1 (b)). This task results in severe image distortions, thus making it very difficult to recover the watermark information previously embedded.

Considering current scientific literature, two watermarking approaches could be applied to solve this problem: a) Invisible watermarking schemes that are resilient to Print-Scan (PS) operations and b) Visible watermarking approaches. PS-resilient watermarking techniques have emerged as an attractive topic for researchers around the world. Some works deal with watermarking techniques for printed text, which are done by modifying some patterns in the printed output version like spaces between lines or words [16]. Nevertheless, these techniques cannot be extended to printed images since images are composed by pixels instead of lines of characters. In other proposals, the complex nature of the print-scan problem has been carefully analyzed under controlled conditions [17]–[19]. These applications usually focus on the distortion over the image caused by the print-scan process, such as pixel distortion, rotation and translation, and do not consider the possibility of that the watermarked image can be severely damaged and segmented by an edition process before printing.

Fig. 1 An example of one of the most difficult challenges to prove ownership through watermark techniques: (a) original portrait image and (b) its edited version in order to be printed and used as a cover of a magazine.

On the other hand, some visible watermarking approaches attempt to protect the copyrighted material by covering the whole image [7]–[9], and other ones embed a visible pattern covering only a small portion of the host image [10]. Both approaches have disadvantages when are considered for copyright protection in practical situations. If a visible pattern is embedded into a small portion of the image, the attacker has to perform a cropping operation to avoid the watermarked region and thus leaving the main material unprotected. Moreover, covering the whole original image by a visible watermark signal is obtrusive since it introduces a distracting visible element that does not correspond to the main image information. The produced effect ranges from mildly distracting, at best, to severely damaged at worst, precluding the proper use of the image content in legitimate scenarios.

Taking into account the above mentioned discussion, we perform a brief analysis in order to get a better understanding of the problem and get an appropriate solution. Since portrait images are a representation of a human being, the person itself is the most important element and the most likely area to be preserved after the publication of an edited image. Additionally, in a portrait image the face and its expression are predominant and consequently this area captures the observer's attention and decreases its ability to detect distortions over other regions of the image. Based on the above mentioned principles, we propose a strategy that consist in embedding a small visible watermarking on the portrait image within the area where the person is located, but avoiding the focus of observer's attention. With this strategy, the visual watermark belongs to the object of interest of the portrait and thus removing it will severely damage the image content. Moreover, since the visual watermark avoids the most attractive area of the portrait, it probably goes unnoticed by the naked eye of a viewer. This strategy involves the need to analyze the spatial information of the image in order to automatically detect the position where the visual watermark will be embedded. The HVS properties such as texture and luminance play an important role to achieve this objective since those properties define the region where human observers have limited ability to detect image changes. The HVS properties have been widely used in watermarking field. In [14], the watermark signal is divided in order to embed one watermark bit per each 8×8 discrete cosine transform (DCT) block of each video frame. Before the watermark embedding process, the DCT block is classified according to the HVS properties and then the

watermark strength is modulated according to such classification. In this way, a "plain" block will have less distortion than a "textured" block with the aim to limit the ability of an observer to perceive the embedded watermark signal. A similar approach is employed in [15], where an HVS-based model is used to determine the optimal strength at which the watermark signal reaches the visibility threshold. In both cases, the HVS propertiesare used to locate highly textured regions from the whole image with the main objective of adjust the watermark strength and thus regulate how perceptible is for human observers.

In contrast, the proposed method employs the HVS properties analysis with a different approach that can be summarized in two main differences. First, the HVS analysis is performed in order to define the watermark location, not to adjust its visibility. The watermark visibility is adjusted according to the spatial features of its hosting region. In addition, the analysis is carried out selectively, only over those spatial regions of the portrait image that belong to the object of interest and do not represent human skin, not over the whole image.

3. Proposed Algorithm

The proposed algorithm is comprised of three main steps: a) automatically compute the location where the visual watermark will be embedded is the first and the core process, b) fine-tuning the watermark dimensions to get a suitable relationship with the spatial resolution of the portrait image, and c) adapting the visibility of the watermark signal according to its background.

3.1 Watermark Location

The watermark location process is divided into three stages which are described in detail in following sections.

3.1.1 Isolation of the Object of Interest

The isolation of a saliency object from its background is a task that can be easily done by the human brain but that is not trivial at all for a computer. This segmentation process has been extensively studied during the last decades. In our proposal, we use the image signature descriptor defined in [20], which is an image descriptor where the foreground information is privileged and raises the possibility of detecting salient image regions in order to separate them from the image background. Formally, the image signature of an image I is given by:

$$IS(I) = sign(DCT(I)), \tag{1}$$

This operation discards the amplitude values of the whole cosine spectrum and preserves only the sign of each DCT component. In the inverse way the foreground of an image can be estimated by computing the inverse DCT of just the signs in the cosine spectrum, as follows:

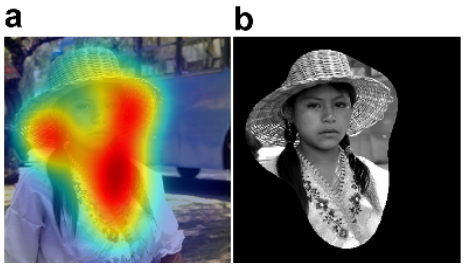

Fig. 2 Segmentation process applied to isolate the object of interest: (a) heat map representation of the visual saliency map m and (b) map O_1 representing the output of the algorithm.

$$\overline{I} = \text{IDCT}[IS(I)], \tag{2}$$

Then, a visual saliency map $m(x, y) = m$ is calculated by blurring the reconstructed image by a Gaussian kernel smooth filter $G_\sigma(x, y) = G_\sigma$ with standard deviation σ which is convolved with each color component I_i of the image I, as follows:

$$m = G_\sigma * \sum_i (\overline{I}_i \circ \overline{I}_i), \tag{3}$$

In (3) the symbol $\circ$ denotes the Hadamard product operator and $*$ the convolution. Finally, with the aim to isolate the foreground region on an image I with dimensions of $M \times N$ pixels we use its luminance component, denoted as I_LUM, to get a map O_1 which is obtained by applying a threshold T_m over the visual saliency map m as follows:

$$O_1(x, y) = \begin{cases} I_{LUM}(x, y) & m(x, y) \geq T_m \\ 0 & m(x, y) < T_m, \end{cases} \tag{4}$$

where $x = 1, \ldots, M$ and $y = 1, \ldots, N$. An illustrative example of the above explained process is shown in Fig. 2, where the saliency map m of a portrait image is represented as a heat map to get a better appreciation of the algorithm operation (Fig. 2 (a)). The map O_1 is computed by applying an empirical threshold T_m (Fig. 2 (b)).

3.1.2 Skin Detection

In the case of portrait images, the face area is a very attractive region making the observer pays his attention on it. Thus this area must be avoided in order to keep the visible watermark unnoticed to the naked eye of a viewer. Moreover, face area is often visually joined to other human body areas such as the neck, shoulders, arms or even hands that, according to the HVS properties are considered very sensitive areas where a slight modification can be easily detected.

Due to the above consideration, a skin detection process [21] is used to locate those areas that represent person's skin in the portrait in order to avoid them in the watermarking process. This five-step method exploits the spatial distribution characteristics of the human color skin based on a universal skin-color map. The accuracy of the algorithm is based on the intuitive justification that the diverse skin colors of human races are determined by the difference in the

Fig. 3 (a) Three portrait images of people with different skin color and diverse background and luminance conditions, and (b) the output bitmap O_2 of the skin detection process.

brightness of the skin color, which is governed by the luminance, and not for chrominance values. Then, the method employs a regularization procedure to overcome the limitations of color segmentation. The reader is referred to [21] for a detailed description of the skin detection process. In Fig. 3 we can appreciate the performance of the skin detection process after it is applied to three portrait images that contain people of different human races, and therefore with different human skin colors (Fig. 3 (a)). The output binary bitmap O_2 for each portrait image represents the area where an observer most likely be focusing his attention and thus corresponds to a region that should remain unmodified (Fig. 3 (b)). Note that the performance of the skin detection process is not affected by the variety of background and luminance conditions.

3.1.3 HVS-Based Masking

Once the object of interest has been located and the skin detection process was performed, the potential region where the visible watermark may be embedded without an easy detection by an observer is computed by removing O_2 from O_1. This region, denoted as O_3, is obtained by:

$$O_3(x,y) = \begin{cases} 0, & \text{if } O_2(x,y) = 1 \\ O_1(x,y), & \text{otherwise,} \end{cases} \tag{5}$$

The region O_3 is divided into N non-overlapping blocks of 8×8 pixels, denoted as B_N. Then, every block B_N is ranked by employing an HVS-based mask, in order to determine the most suitable block of the region O_3 where the watermark will be embedded, as follows:

Step 1. To embed the visible watermark within the boundaries of the object of interest, we will discard all the blocks that have at least one bit with zero value.

Step 2. To meet with the well-known luminance property of the HVS that suggests that the human sensitivity to errors is low in highly bright and very dark image regions, we introduce a fast and simple technique to locate the brighter regions in the image. We propose an adaptable procedure to determinate how bright a block B_N is, in the context of the image, this helps to prevent to discard all blocks if the image has poor lighting. The procedure is described as follows:

- Calculate the mean value of the whole luminance space in the original image (n_1)
- Calculate the mean value of each block B_N (n_2)
- The range between the maximum value (L_{MAX}) and the mean value (n_1) of the luminance space of the original image is empirically divided into three uniform parts,

$$d = \frac{(L_{MAX} - n_1)}{3} \tag{6}$$

- It was experimentally determined that the middle part of the previously range is the most appropriate section to embed the watermark signal because is more robust against aggressive signal processing attacks such as printing or brightness changes, than the most brightly section. In this way, the first score for each block B_N, represented as c_1, is calculated like this:

$$c_1 = \begin{cases} 1, & \text{if } (n_2 > n_1 + d) \text{ AND } (n_2 < 2 \times d + n_1) \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

Step 3. This step is oriented to meet with the texture masking property that suggests that human vision detect changes with less precision in highly textured regions. Each block B_N, is classified as plain, edge or texture according to the algorithm proposed in [22]. This algorithm is based on the fact that a texture condition of a DCT block can be measured by evaluating the energy of its AC coefficients. Once a block B_N, is classified as a texture block then a second score, denoted as c_2, is compute as follows:

$$c_2 = 1.25 \times \frac{E(B) - Min}{Max - Min} + 1 \tag{8}$$

where $Max = 1800$, $Min = 290$ and $E(B)$ is the texture energy for each block B_N, defined as the sum of the first six AC coefficients, according to the classical *ziz-zag* order used in DCT blocks.

Step 4. Finally, to determine each block qualification Q_N, both scores previously computed are multiplied:

$$Q_N = c_1 \times c_2 \tag{9}$$

Thus, the block B_N with the highest qualification Q_N is considered as the best position where the visible watermark will be embedded. Figure 4 shows an illustrative example of the watermark location process applied to a highly textured portrait image (Fig. 4 (a)). In Fig. 4 (b) are displayed those blocks that meet with all criteria required by the watermark location process and thus received a block qualification Q_N according to its luminance and texture characteristics. The region that contains the block with the highest qualification has been zoomed with demonstration purposes. Here, darker blocks have the higher qualification. The darkest block represents the exact position where the visible watermark will be embedded in order to be undetected by the

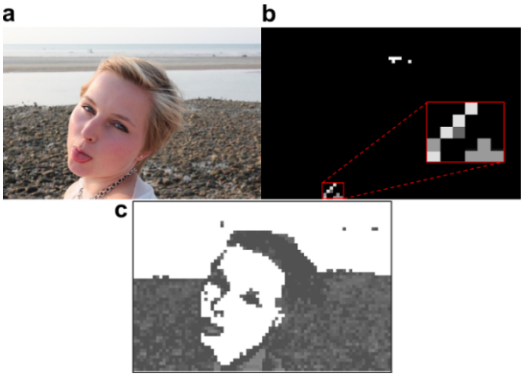

Fig. 4 (a) Original portrait image, (b) blocks that meet with watermark location criteria and (c) the texture block classification process applied over the whole portrait image.

naked eye of an observer. As we discussed before, the invisible watermarking approaches often perform an HVS analysis in order to embed a strong watermark and thus getting a more robust scheme. Figure 4 (c) shows an example of the above where a texture block classification process [22] of the whole image is performed. By comparing the obtained results in Figs. 4 (b) and (c) we can graphically appreciate the differences between this approach and the proposed one. In our proposal, the HVS analysis is performed only over those blocks that already have met with some conditions of the spatial characteristics of the portrait image not over the whole image. The focus of this analysis is to determine the most suitable watermark location, later its size and visibility are adjusted with additional processesof the algorithm.

3.2 Watermark Dimensions

Depending on the application, the portrait images are captured with different spatial resolutions, so a fixed size of a visual watermark may be inadequate in practical scenarios. The most important attack related to watermark size that must be considered by the employed strategy is the size reduction of the watermarked image since it can prevent visibility of the watermark.

To deal with this issue we consider that in practical scenarios and despite of its original resolution, a portrait image will be printed on a standard size or at least among some suitable limits and whether in such conditions the watermark remain visible, the owner has to be able to prove the property of an image. In this way, we focus on ensuring watermark visibility under adverse conditions and then adjust its dimensions as follows:

Step 1. The watermark size is adjusted considering the dimensions of the object of interest within the portrait image, which is represented by the limits of the binary map O_1. This allows focusing on protect the isolated object of interest within the portrait image and avoid the relationship between the dimensions of the object of interest and the remaining space within the image.

Step 2. The digest size (14 × 19 cm) is considered as the convenient smallest size at which a portrait image could be reduced for commercial purposes. At this size, we consider an initial watermark size of 8×8 pixels which corresponds to the DCT block B_N with the highest qualification Q_N computed in the previous section. The original watermark size is adapted by performing a linear relationship between the digest size and the dimensions of the object of interest in O_1 as follows: (1) Compute the width ratio w_r by dividing the width of the object of interest by the width of the digest size. (2) Compute the height ratio h_r by dividing the height of the object of interest by the heightof the digest size. (3) Considering the absolute ratio $\Delta = \max(w_r, h_r)$, then the new watermark dimensions, which are $A \times B$ pixels size, is calculated by using:

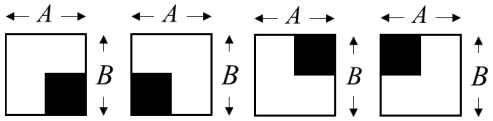

Fig. 5 Four candidate regions built to adapt visual watermark size. The black block represents the original watermark location of 8×8 pixels.

$$A = B = \left\lfloor \frac{\Delta}{0.125} \right\rfloor \tag{10}$$

This procedure ensures that the original aspect ratio of the watermark (1 : 1) will not be modified.

Step 3. Once the watermark dimensions have been determined, the original watermark location must be updated in order to host the new watermark size. To achieve this, four candidate regions are created by overlapping the new dimensions of the visual watermark to the original location and placing the latter at corners down-right, down-left, up-right and up-left respectively.

In Fig. 5 is shown a representation of the four candidate regions built to adapt the watermark size where the black block represents the original watermark location of 8×8 pixels. Then, the best candidate region R, is chosen by finding the region with the smallest variance V among the four candidates, which is defined as:

$$V = \sum_{i=1}^{A \times B} \left(p_i - \frac{1}{A \times B} \sum_{i=1}^{A \times B} p_i \right)^2 \tag{11}$$

Here, p_i indicates a pixel value of the region R with $0 \leq p_i \leq 255$.

3.3 Watermark Embedding Process

The proposed watermark embedding process diagram is shown in Fig. 6. The main steps are: (1) Isolate the luminance component, denoted as I_{LUM}, from the original image I of $M \times N$ pixels. (2) Determine the block B_N with the highest qualification Q_N where the watermark will be embedded by performing the process described in Sect. 3.1. (3) Given a binary watermark signal $W(a, b)$, with $a = 1, \ldots, A$ and $b = 1, \ldots, B$, represented by a binary image of 8×8 pixels,

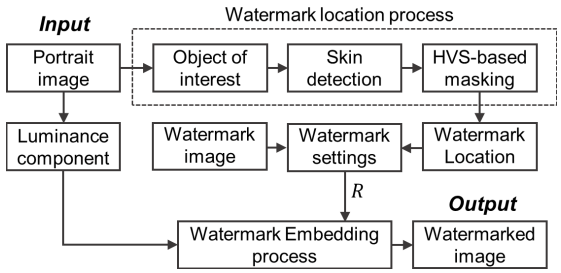

Fig. 6 Proposed watermark embedding process.

adjust its dimensions and determine the best candidate region R where it will be embedded according to the algorithm described in Sect. 3.2. (4) Perform the watermark embedding process to get the watermarked luminance component I^{w}_{LUM} as follows:

$$\begin{aligned} I^{w}_{LUM}(i,j) &= I_{LUM}(i,j), \quad i,j \notin R \\ I^{w}_{LUM}(i,j) &= \Omega(i,j), \quad i,j \in R \\ \Omega(i,j) &= \begin{cases} \alpha_1 + I_{LUM}(i,j), & \text{if } W(a,b) = 1 \\ I_{LUM}(i,j), & \text{if } W(a,b) = 0 \end{cases} \end{aligned} \tag{12}$$

where, $i = 1,\ldots,M$; $j = 1,\ldots,N$; $a = 1,\ldots,A$ and $b = 1,\ldots,B$. The adaptive scaling factor α_1 to embed the watermark signal determines how visible the watermark is, and at the same time, how much the details beneath it become obscured. The watermark scaling factor α_1 is adapted by using an adaptive computation, which produces a contrast effect between the watermark and its background. The darker the background is, the brighter the watermark is preserved and vice versa. Based on the fact that the watermarked location has been classified as a region with high luminance we apply only partially the original method proposed in [23] through which the watermark signal is adapted by producing an adequate value regarding its background. In this way, the watermark scaling factor is computed by:

$$\alpha_1 = 31 - \left\lfloor \frac{255 - n_2}{128} \times 32 \right\rfloor \tag{13}$$

where according to Sect. 3.1.3, n_2 is the mean value of the block B_{N} with the highest qualification Q_{N}. (5) Finally, the watermarked image I^{w} is obtained by restoring the watermarked luminance component I^{w}_{LUM} together with the original chrominance values.

3.4 Watermark Detection Process

To our best knowledge, it does not exist a universally accepted method to get a consistent measure of perceptibility for visible watermark. Then, a closely visual inspection is the method used in our proposal to determine the existence, or not, of the watermark signal. However, since the visible watermark should not be easily perceptible according to the objectives of the proposed method, it is necessary for the portrait image owner to keep the watermark location as a secret key to be able to do a visible inspection when required. The secret key is a copy of the original image with a pointer that determines the watermark location. Then, to check if an image is being used in an illegal way, the ownership of the image can be demonstrated by performing a visual inspection without the need to conduct changes in the watermarked image such as resize or some additional editing processes, and then locating the watermark pattern in the secret position.

Fig. 7 Binary watermark image used in conducted experiments.

4. Experimental Results

The proposed watermark algorithm has been tested on approximately fifty portrait color images obtained from different available open databases that are labeled for non-commercial reuse.

The images were selected by having different dimensions, background conditions and texture characteristics, as typically happens in real-world scenarios. Figure 7 shows the binary image used as the watermark signal in our experiments. We conduct several experiments to measure the visibility, performance and robustness of the proposed method.

4.1 Visual Inspection

The obtained results after applying the proposed algorithm on a pair of portrait images with different background conditions and different dimensions is shown in Fig. 8. The owner's key is represented as a red rectangle in both, the original and watermarked images, whose center corresponds to the central pixel of the watermarking region R obtained automatically with our algorithm. For demonstrative purposes, original and watermarked region (including its 3×3 neighborhood blocks) are zoomed and displayed in the upright corner. Looking carefully at watermarked images (Fig. 8 (b)) we can assert that the proposed embedding process works exactly as expected, thus being a very good option to be applied in practical situations, verifying the following three characteristics: a) visible watermark is part of the region of interest in all cases, which prevent it to be lost after the watermarked image is edited in order to remove the person in the portrait, b) additionally, the watermark does not belong to the face, or another skin region of the person, preventing its easy localization to the naked eye of an observer, and finally c) the small watermark is embedded into the highest textured area with high luminance value in the context of the region of interest of the image, which according to HVS properties, are necessary conditions that limit the ability of an observer to distinguish changes in the image.

Fig. 8 The proposed algorithm after it is applied to two representative portrait images (Portrait #6 and #7): a) original images including the owner's key shown as a red rectangle, and b) watermarked images. For demonstrative purposes in both images the watermarking region R obtained automatically with our algorithm and its 3×3 neighborhood blocks are zoomed and displayed at the up-right corner.

4.2 Performance Evaluation

The achieved performance of the proposed method is evaluated considering its application on images with different dimensions and its computational cost.

4.2.1 Watermark Size Adjustment

Table 1 shows the obtained results after applying the proposed method on portrait images with five representative different sizes. From Table 1 we can appreciate that, according to our proposal, the watermark size is adapted in function of the dimensions of the object of interest within the portrait image, with the idea of preventing its destruction in case of an aggressive reduction of the image. This adaption was carried out considering a digest size of 529×719 pixels at 96 dpi. In order to appreciate these results graphically, Fig. 9 shows the adaptation of the watermark size in the portrait image with the biggest size in our experiments, which corresponds to the Portrait #35 of 3000×4000 pixels size.

Table 1 Watermark size adjustment on different size images.

Test image	Spatial dimensions (pixels)		
	Portrait image	Object of interest	Watermark
Portrait #09	426 × 840	398 × 795	8 × 8
Portrait #14	600 × 900	540 × 820	9 × 9
Portrait #15	800 × 1200	800 × 1127	12 × 12
Portrait #22	1024 × 1536	947 × 1434	17 × 17
Portrait #35	3000 × 4000	2940 × 3752	44 × 44

The boundaries of the object of interest, shown with a dotted rectangle over the image, have 2940×3752 pixels size. The red rectangle in the image corresponds to the automatically obtained watermarking region R. The up-right corner of Fig. 9 shows the watermarking region R surrounded by a margin of 8 pixels, before the watermark embedding process. The same region but including the visual watermarking is shown at the down-right corner. According to Sect. 3.2 and taking into account the above mentioned dimensions for the digest size, the final watermark dimensions are 44×44 pixels.

From Fig. 9 we can note that: a) the visual watermark

Fig. 9 Watermark size adaptation to Portrait #35 with 3000×4000 pixels size: a) on the left, the portrait image with the boundaries of the object of interest in dotted rectangle and the watermarking region represented with a red rectangle, b) on the right, the zoomed watermarking region R before and after the watermark embedding process.

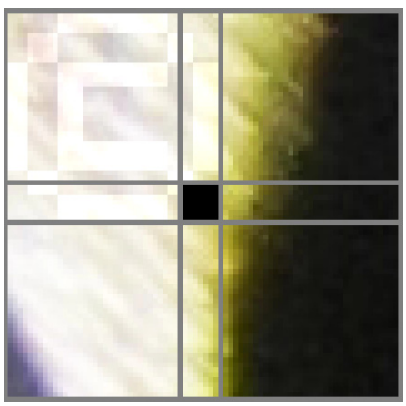

Fig. 10 Four regions created to adapt the original watermark location (black square at the center) to the final dimensions of the visual watermark.

keeps an appropriate proportion considering the portrait image dimensions. This characteristic allows protecting the portrait image in situations that require performing a life-size print and also in cases where an aggressive reduction before printing is needed. b) The embedded visual watermark is not easily perceived to the naked eye of a viewer not only by its strategic position but also its contrasting adaptation with respect to its background. The adaption of the original watermark location which is performed in order to host the final watermark size is shown in Fig. 10. According to Sect. 3.2 in Fig. 10 we can observe the four candidate regions, delimitated with gray lines, created to adapt the original watermark location. Here, we can perceive the correctness of the watermark size adaption since the original watermark location, represented with a black square in the center of the figure, has a very small size to provide protection to the portrait image in practical situations. Moreover, as explained, this adaptation process is important to determine which of the four adjacent regions best preserves the characteristics of the original watermark location and thus determining its adjusting direction.

Fig. 11 On the right, the watermarked version of the Portrait #20 including a zoomed representation of its watermarking region R in the down-right corner. On the left, the watermarking region R for each case after the watermarked image is reduced at a rate of: (a) 50%, (b) 30%, (c) reduced to the digest size, (d) 17% and (e) 10%.

Also, we perform supplementary experiments in order to appreciate how perceptible is the visible watermark, after a watermarked image is resized to different sizes related toprinted publications. On the right of Fig. 11 is shown the watermarked version of the Portrait #20 with a spatial resolution of 2536×3168 pixels. In this case, the boundaries of the object of interest match the size of the portrait image so the initial watermark dimensions are 38×38 pixels. The down-right corner of the Portrait #20 shows a zoomed representation of the watermarking region R for demonstration purposes. Then, the watermarked image is resized to different sizes and R is shown on the left of Fig. 11 for each case: a) half of its original size (1268×1584 pixels), b) 30% of its original size (888×1109 pixels) which is an estimate of the size of a magazine cover, c) The digest size (529×719 pixels), d) 17% of its original size (431×539 pixels) which is approximately a quarter of a magazine page and is considered a typical size of advertising on the front cover of a magazine, and e) 10% of its original size (254×317 pixels). Some considerations must be taken into account regarding this experiment: 1) According to the watermark size adaptation process described in Sect. 3.2, the visual watermark is clearly perceptible when the watermarked image is downsized from its original dimensions until the digest size (Figs. 11 (a)–(c)). 2) Please note that the visual watermark can be partially appreciated even if the watermarked image is reduced beyond the digest size (Fig. 11 (d)). 3) A reduction around the 90% of the original size of the watermarked image could prevent the perceptibility of the visual watermark (Fig. 11 (e)). However, in some cases this reduction could degrade the visual quality of the watermarked image such that its commercial value might be reduced as well.

4.2.2 Computational Cost

Regarding the computational cost, an analysis was carried out in order to obtain the time complexity involved by the whole watermark embedding process. Considering n as the number of images to be processed with a spatial resolution of $M \times N$ pixels, the first applied process for each image is the isolation of the object of interest which as stated is not performed over the whole image information but just in a coarse representation of 64×64 pixels, according to [20]. The computational time of this process can be represented as $O(n \cdot 64^2)$. Then, the rest of the stages involve processing the whole image information several times in order to embed the visual watermarking information. According to the sum rule of the computing asymptotic time complexities, the overall time complexity of the proposed method can be represented by a linear order as $O(n \cdot M \times N)$. In order to put this data in context, we compare the reached time complexity by our proposal with those methods based on the k-means clustering, which corresponds to a popular algorithm used to image segmentation applied in watermarking [24] and other applications [25]. The time complexity of the k-means algorithm applied to n images is given by $O(kn \cdot T)$, where k is the number of clusters and T is the number of iterations that k-means algorithm takes [26]. The lower limit for T on the k-means is exponential in k and is denoted as $2^{\Omega(k)}$ [27]. In this way, the time complexity of those methods based on k-means algorithm is given by $O(n \cdot M \times N + kn2^{\Omega(k)})$. From the above analysis we can observe that the computational cost spent by our proposed watermark embedding process is significantly less than that employed only by the segmentation process used in other proposals. In this way, the contribution of the proposed algorithm is not only in terms of the automatic accuracy on finding a strategic position to locate the visible watermark, but also in terms of the low computational cost to do it.

4.3 Robustness Evaluation

As we mentioned earlier, this work is focused to provide copyright protection for portrait images in order to prevent a misleading use, i.e. when they are processed and printed without legitimate use rights. To measure the robustness of the proposal practical situations, we implement an editing process to simulate a real-world scenario, which diagram is shown in Fig. 12 and described as follows. (1) A photomontage image is created by performing several aggressive attacks, such as signal processing operations together with geometric attacks. (2) It is simulated an illegal use by printing the previously edited image. (3) In order to proof the ownership of the image, the attacked image is scanned. (4) With the help of the owner's key, the scanned image is subjected to a process of visual inspection to determine if the correct watermark is present, or not.

In order to illustrate the performance of the proposed scheme Fig. 13 shows two portrait images that were subjected to the process described above.

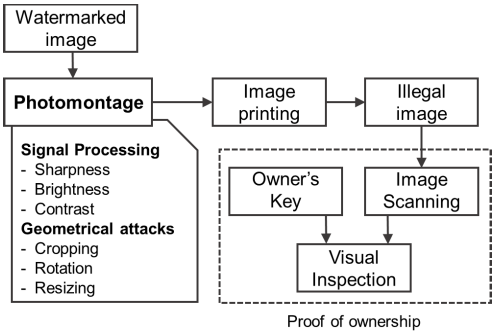

Fig. 12 Proposed watermark testing scenario.

Table 2 Detail of applied operations in experiments A and B.

	Experiment A	Experiment B
Geometric attacks		
Cropping	47.05%	42.05%
Rotation	-5°	+1°
Scaling	+20%	-50.5%
Signal processing		
Brightness	10%	12%
Contrast	-15%	+5%
Sharpness	[3 3]	[3 3]
Photomontage		
Image	Magazine	Book
Printing paper	Premium photo	Bright white
Print quality	Photo quality	Standard quality
Scanning resolution	400 ppp	200 ppp

Watermarked images without modifications and their respective owner's keys, represented by a red rectangle, are shown in Figs. 13 (a) and (c). Several distortions, including signal processing and geometric modifications, were affected in order to create a photomontage of each image. In experiment A (Fig. 13 (b)), the first image was manually separated from its background and adapted in order to be used as a cover of a magazine. In this case, the image lost almost half of its original information. In experiment B (Fig. 13 (d)) a similar process has been done in order to adapt the image as book cover page. Full details of the modifications are listed in Table 2. Later, both edited images were subjected to a print-scan process to carry out a visual inspection and thus prove the ownership. In our experiments, the print-scan process was performed by using the commercially available multifunctional equipment EPSON L455.

In experiment A, the edited image was printed using photo quality over premium photo paper, and then scanned with 400 points per pixel resolution. By other hand, a standard quality printing on bright white paper and 200 points per pixel resolution were selected for experiment B. The obtained results are graphically shown in Fig. 14. For demonstration purposes, the watermark region R and its 3×3 neighborhood blocks are extracted and zoomed from the original image (Fig. 14 (a)), the watermarked image before modifications (Fig. 14 (b)), the watermarked image after editing process (Fig. 14 (c)) and the watermarked image after the print-scan process (Fig. 14 (d)). From these results, we can appre-

Fig. 13 A real-world scenario where two watermarked portrait images (a) and (c) were adapted in order to be used as a first page magazine (b) or a cover page book (d).

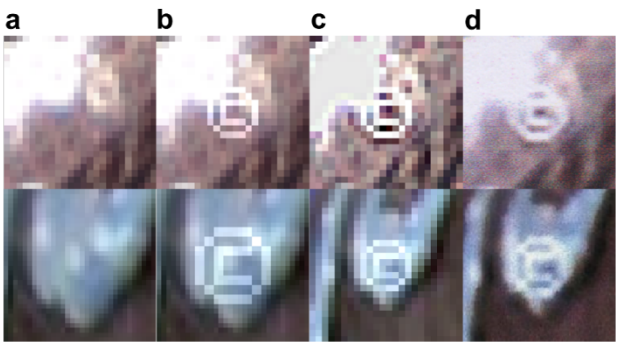

Fig. 14 Zoomed representations of the watermark region during the different stages of the process: (a) before the watermark embedding process, (b) watermarked region before attacks, (c) watermarked region after the edition process and (d) watermarked region after the print-scan process.

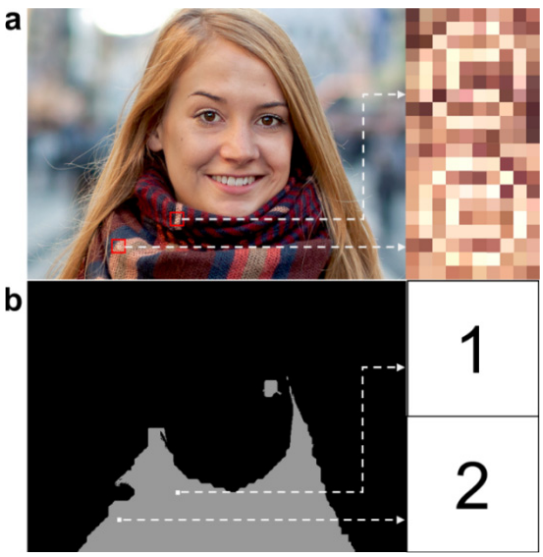

Fig. 15 A portrait image where the visual watermark pattern has been embedded twice: (a) watermarked image and (b) the region O_2 to embed the visual watermark in gray and the best ranked blocks in white.

ciate that after the print-scan process the watermark can be perceived yet even though it has been severely altered by the edition process. The signal processing attack is performed uniformly all over the image which allows the watermark remains visible after these operations. Geometric attacks are more aggressive since the spatial configuration of the image is distorted due to the interpolation process. As we mentioned early, a big image can be reduced to below half in order to be printed with commercial purposes, this condition is simulated in experiment B (Fig. 13 (d)). In practice, the rotation is carried out with small angles because it is desired to preserve the natural position of the person in the portrait image. Aggressive cropping attack does not affect the proposed technique because the visible watermark belongs to the object of interest.

Under all these adverse conditions, the visible watermark signal can still be perceived, allowing to properly proving the ownership of the original image. Furthermore, the above mentioned experiments were not influenced by any hardware specifications as it happens in most current proposals that are robust against PS operations. Finally, it is important to note that the proposed method allows the owner of a portrait image to embed the visual watermark pattern multiple times for the sake of the better protection of the object of interest. As we can observe in Fig. 13 (b), an aggressive edition of the watermarked portrait image raises the possibility that the visibility of the watermark pattern will be partially or totally obstructed through the inclusion of external elements beyond the portrait image. In this case, performing the portrait image protection by embedding the visual watermark pattern twice or more will increase the likelihood that the owner can claim for the ownership of the portrait image even after aggressive attacks are carried out. Figure 15 (a) shows a graphical example of a portrait image that is protected by embedding the visible watermark twice. In Fig. 15 (b), the potential region where the visible watermark may be embedded without an easy detection is shown in gray. Then, in order to embed the visual watermark multiple times, the best ranked blocks B_N should be considered,

i.e. those blocks with the highest qualifications Q_N. These blocks correspond to the displayed in white in Fig. 15 (b). It is important to note that it is not required to perform additional modifications or adjustments to the original proposed method in order to provide enhanced protection to portrait images, if necessary.

5. Conclusions

A visible watermark technique which takes a new approach from traditional watermarking methods is proposed in this paper. The main contribution of this proposal is the definition of an automated process that is able to compute the best position where the visible watermark can be embedded, corresponding to a region where the embedded signal cannot be easily perceived by an observer. The calculation of this process is based on objective criteria yielded by our analysis of portrait image spatial characteristics and HVS properties. Considering the size of the portrait image being processed the watermark dimensions are adjusted in order to preserve its original aspect ratio and robustness against aggressive attacks. A computational cost analysis was performed to confirm that the contributions of the proposed algorithm include greater accuracy in finding the strategic position to locate the visible watermark and a low computational cost to do it. In real-world scenarios, portrait image are captured with different background, illumination and texture conditions, and also captured with different spatial resolutions. For these reasons, the proposed watermark algorithm has been implemented and tested on approximately fifty portrait images in many different conditions. Several experiments were carried out in order to demonstrate the proper functioning of the algorithm according to different portrait image environments, their correct adaption to portrait images with different spatial resolutions and to measure its robustness, concluding that the embedded visual watermark is robust enough to remain in the portrait image even after aggressive attacks.

Acknowledgments

Authors thank the Post-Doctorate Scholarships Program from DGAPA at Universidad Nacional Autónoma de México (UNAM) as well as Instituto Politécnico Nacional (IPN) and the Consejo Nacional de Ciencia y Tecnología de México (CONACYT) by the support provided during the realization of this research.

References

[1] I.J. Cox, M.L. Miller, and J.A. Bloom, Digital watermarking, Morgan Kaufmann, San Francisco, 2002.
[2] J.-S. Sai, W.-B. Huang, and Y.-H. Kuo, "On the selection of optimal feature region set for robust digital image watermarking," IEEE Trans. Image Process., vol.20, no.3, pp.735–743, 2011.
[3] C.-W. Tang and H.-M. Hang, "A feature-based robust digital image watermarking scheme," IEEE Trans. Signal Process., vol.51, no.4, pp.950–959, 2003.
[4] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: Its formal model, fundamental properties and possible attacks," EURASIP J. Adv. Sig. Process., vol.2014, no.1, pp.1–22, 2014.
[5] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," IEEE Signal Process. Mag., vol.30, no.2, pp.87–96, 2013.
[6] A. Cheddad, J. Condell, K. Curran, and P.M. Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Process., vol.90, no.3, pp.727–752, 2010.
[7] Y. Hu and S. Kwong, "Wavelet domain adaptive visible watermarking," Electron. Lett., vol.37, no.20, pp.1219–1220, 2001.
[8] Y. Yang, X. Sun, H. Yang, and C. Li, "Removable visible image watermarking algorithm in the discrete cosine transform domain," J. Electron. Imaging, vol.17, no.3, 033008, 2008.
[9] M.-J. Tsai and J. Liu, "A game-theoretic architecture for visible watermarking system of ACOCOA (adaptive content and contrast aware) technique," EURASIP J. Adv. Sig. Process., vol.2011, no.1, pp.1–22, 2011.
[10] Y. Yang, X. Sun, H. Yang, C.-T. Li, and R. Xiao, "A contrast-sensitive reversible visible image watermarking technique," IEEE Trans. Circuits Syst. Video Technol., vol.19, no.5, pp.656–667, 2009.
[11] P.-Y. Lin, "Imperceptible visible watermarking based on postcamera histogram operation," J. Syst. Softw., vol.95, no.1, pp.194–208, 2014.
[12] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," IEEE Trans. Image Process., vol.9, no.3, pp.432–441, 2000.
[13] M.S. Kankanhalli and K.R. Ramakrishnan, "Adaptive visible watermarking of images," Proc. IEEE International Conference on Multimedia Computing and Systems (ICMCS), vol.1, pp.568–573, 1999.
[14] A. Cedillo-Hernandez, M. Cedillo-Hernandez, M. Garcia-Vazquez, M. Nakano-Miyatake, H. Perez-Meana, and A. Ramirez-Acosta, "Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT," Signal Process., vol.97, no.1, pp.40–54, 2014.
[15] M. Urvoy, D. Goudia, and F. Autrusseau, "Perceptual DFT watermarking with improved detection and robustness to geometrical distortions," IEEE Trans. Inf. Forensics Security, vol.9, no.7, pp.1108–1119, 2014.
[16] L. Tan, X. Sun, and G. Sun, "Print-scan resilient text image watermarking based on stroke direction modulation for Chinese document authentication," Radioengineering, vol.21, no.1, pp.170–181, 2012.
[17] L. Yu, X. Niu, and S. Sun, "Print-and-scan model and the watermarking countermeasure," Image Vision Comput., vol.23, no.9, pp.807–814, 2005.
[18] K. Solanki, U. Madhow, B.S. Manjunath, S. Chandrasekaran, and I. El-Khalil, "Print and scan resilient data hiding in images," IEEE Trans. Inf. Forensics Security, vol.1, no.4, pp.464–478, 2006.
[19] A. Keskinarkaus, A. Pramila, and T. Seppänen, "Image watermarking with feature point based synchronization robust to print-scan attack," J. Vis. Commun. Image R., vol.23, no.3, pp.507–515, 2012.
[20] X. Hou, J. Harel, and C. Koch, "Image signature: Highlighting sparse salient regions," IEEE Trans. Pattern Anal. Mach. Intell., vol.34, no.1, pp.194–201, 2012.
[21] D. Chai and K.N. Ngan, "Face segmentation using skin-color map in videophone applications," IEEE Trans. Circuits Syst. Video Technol., vol.9, no.4, pp.551–564, 1999.
[22] H.H.Y. Tong and A.N. Venetsanopoulos, "A perceptual model for JPEG applications based on block classification, texture masking, and luminance masking," Proc. International Conference on Image Processing (ICIP), vol.1, pp.428–432, 1998.
[23] H.-M. Tsai and L.-W. Chang, "Secure reversible visible image watermarking with authentication," Signal Processing: Image Communication, vol.25, no.1, pp.10–17, 2010.
[24] N.V. Boulgouris, I. Kompatsiaris, V. Mezari, D. Simitopoulos, and M.G. Strintzis, "Segmentation and content-based watermarking for color image and image region indexing and retrieval," EURASIP J. Adv. Signal. Process., vol.2002, no.1, pp.418–431, 2002.

[25] A. Cedillo-Hernandez, M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, and H. Perez-Meana, "An efficient content-based video retrieval for large databases," Proc. IEEE International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE), pp.15–19, Cuernavaca, Morelos, Nov. 2015.
[26] N. Ejaz, T.B. Tariq, and S.W. Baik, "Adaptive key frame extraction for video summarization using an aggregation mechanism," J. Vis. Commun. Image R., vol.23, no.7, pp.1031–1040, 2012.
[27] A. Vattani, "K-means requires exponentially many iterations even in the plane," Discrete Comput. Geom., vol.45, no.4, pp.596–616, 2011.

Antonio 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 National Polytechnic Institute from Mexico in 2005, 2007 and 2013, respectively. He has around seven years of professional experience in various strategic positions related to IT. Currently, he has a postdoctoral position at National Autonomous University of Mexico (UNAM). His principal research interests are video and image processing, information security, watermarking and related fields.

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 Instituto Politécnico Nacional (IPN) from Mexico in 2003, 2006 and 2011, respectively. He has around six years of professional experience at Government positions related to IT. From September 2011 to December 2015 he was with the Engineering Faculty of the UNAM where he was a Professor. Currently, he is a full-time researcher at IPN. His principal research interests are image and video processing, watermarking, software development and related fields.

Francisco Garcia-Ugalde was born in Mexico. He obtained his bachelor degree in 1977 in electronics and electrical system engineering from UNAM. His Diplôme d'Ingénieur in 1980 from SUPELEC France, and his PhD in 1982 in information processing from Université de Rennes I, France. Since 1983, he is a full-time professor at Engineering Faculty, UNAM. His current interest fields are: Digital filter design tools, analysis and design of digital filters, image and video processing, theory and applications of error control coding, turbo coding, cryptography applications, watermarking, 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 PhD in Electrical Engineering from Metropolitan Autonomous University (UAM), Mexico City, in 1998. From July 1992 to February 1997 she was at Department of Electrical Engineering in UAM. In February 1997, she joined the Graduate Department of The Mechanical and Electrical Engineering School at 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 on Electrical Engineering from The University of Electro-Communications, Tokyo, Japan in 1986 and his PhD 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 UAM where he was a Professor. In February 1997, he joined the Graduate Studies and Research Section of The Mechanical and Electrical Engineering School, of the 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.