Robust Dual Digital Watermark Applied to Antique Digitized Cinema Images: Resistant to Print-Scan Attack

Laura Reyes-Ruiz [1], Eduardo Fragoso-Navarro [1], Francisco Garcia-Ugalde [1], Oswaldo Juarez-Sandoval [2], Manuel Cedillo-Hernandez [2,*], and Mariko Nakano-Miyatake [2]

[1] Universidad Nacional Autónoma de México, Facultad de Ingeniería, Ciudad de México, Mexico
[2] Instituto Politécnico Nacional, SEPI ESIME Culhuacán, Ciudad de México, Mexico
*Correspondence: mcedilloh@ipn.mx (M.C.H.)

***Abstract*—Nowadays, advances in information and communication technologies along with easy access to electronic devices such as smartphones have achieved an agile and efficient storing, edition, and distribution of digital multimedia files. However, lack of regulation has led to several problems associated with intellectual property authentication and copyright protection. Furthermore, the problem becomes complex in a scenario of illegal printed exploitation, which involves printing and scanning processes. To solve these problems, several digital watermarking in combination with cryptographic algorithms has been proposed. In this paper, a strategy of robust watermarking is defined consisting of the administration and detection of unauthorized use of digitized cinematographic images from Mexican cultural heritage. The proposed strategy is based on the combination of two types of digital watermarking, one of visible-camouflaged type based on spatial domain and another of invisible type based on frequency domain, together with a particle swarm optimization. The experimental results show the high performance of the proposed algorithm faced to printing-scanning processes or digital-analogue attack, and common image geometric and image processing attacks such as JPEG compression. Additionally, the imperceptibility of the watermark is evaluated by PSNR and compared with other previously proposed algorithms.**

***Keywords*—digital watermarking, image processing, information security, authentication, copyright protection, cultural heritage**

I. Introduction

Currently, more and more information are transferred electronically. Multimedia data such as image, video, and audio can be transmitted by different means, for instance, via the internet, to be visualized in different devices. One of the issues associated with intellectual property occurs when someone has access to all the data, and then copy and retransmit it to unauthorized users without restriction. This will always be possible because digital data can be reproduced identically and unlimitedly. A promising solution to protect information, intellectual property and copyright against unauthorized users is the use of digital watermarking, which in general terms hides certain information associated with the owner and/or distributor, in such a way that only authorized users can make legal use of the data in question [1–8]. Thus, digital watermark in an image can contain information about the author, or the distributor, or even information of the image itself.

Watermarks can be visible or invisible, depending on the application. In the visible case, the embedding location could be chosen based on properties of human vision [9] in such a way that the watermark is unperceived by the naked eye and can be found just with the location information. This feature, in conjunction with visible watermark robustness, are especially useful for certain intentional attacks with optical disturbance equipment, e.g. scanning and printing processes on paper [10]. On the one hand, an invisible mode watermarking algorithm is composed by three elements: the watermark, the encoder (embedding algorithm), and the decoder (detection algorithm). On the other hand, a visible watermarking algorithm consists of only two parts, the watermark, and the embedding algorithm since detection can be performed by bare eye. In a digital imaging context, invisible watermarks can be embedded both in spatial domain as well as in frequency domain. Meanwhile, visible watermarks are usually embedded in the spatial domain.

One of the main objectives of both modalities is that a watermarked image must withstand several manipulations that attempt to remove the digital watermark from the image content. For instance, lossy compression, transmission in a noisy channel, geometric distortions, as well as print-scan processes. Given all these attack possibilities, the problem does not have a single and universal solution; therefore, the research in this field will always be a challenged for new proposals and advances, depending on the evolution of applications and technologies over time.

Considering the foregoing, this article proposes an algorithm that involves the administration and detection of

Manuscript received July 11, 2022; revised August 30, 2022; accepted November 20, 2022.

doi: 10.18178/joig.11.1.61-71

infringement of the use of digitized cinematographic images from Mexican cultural heritage. The proposal consists of two modalities of digital watermarking: the first one consists of a visible-camouflaged watermarking based on spatial domain and the second one belonging to invisible watermarking based on frequency domain together with particle swarm optimization. Experimental results show the versatility of the proposed algorithm after printing and scanning processes, considering an evaluation from the points of view of imperceptibility and robustness requirements, preventing dependencies on the use of specific hardware.

The main contributions of this proposal are: the development of a visible-camouflaged watermarking for particular features of digitized cinematographic images which is resistant to print-scan processes; combined with invisible watermarking using Discrete Fourier Transform (DFT) and the particle swarm optimization (PSO) algorithm [11, 12], allowing to adjust automatically its key operation parameters, improving thus its performance. Fig. 1 shows the general process of the proposed algorithm.

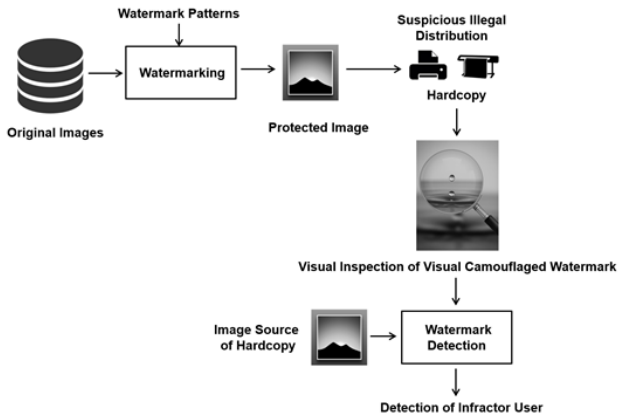


Figure 1. General diagram of the proposed watermarking method.

II. Literature Survey

Visible and invisible watermarks are the two main components of the present dual watermark algorithm, as mentioned in previous section. In this section, some existing algorithms are described and compared.

Visible watermarks, such as the one proposed in [13], are resistant to print-scan attack and do not require any extraction algorithm. Even though they aim to achieve balance between robustness, visibility, and transparency, they visually interfere with the watermarked image, and they are easier to attack due to its conspicuous nature; also, there are many algorithms to remove these kinds of watermarks. Otherwise, imperceptible visible watermarks [14, 15] have the advantage of not being noticeable to naked eye but they need a revelation process, and they are not resistant to print-scan attack. Besides, camouflaged visible watermarks [16] have the advantages of visible watermarks and imperceptible watermarks, but not their drawbacks.

Invisible watermarks algorithms use different transforms or coefficient decomposition, such as, Fast Hadamard Transform (FHT) [17], Discrete Cosine Transform (DCT) [18], Discrete Fourier Transform (DFT) [19], Singular Value Decomposition (SVD) [20], spectral coefficients [21, 22] and so on. Most of these algorithms are not designed to resist print-scan attack and need both embedding and extraction processes. Some of them employ more than one domain to embed the watermark.

To the best of our knowledge there are few dual watermarking algorithms in the literature that combine visible and invisible watermark resistant to print-scan attacks, and they commonly use watermarks that visually interfere the watermarked image [23].

III. Materials and Methods

In this section, dual watermarking method and the main contribution of the proposed algorithm are explained in detail. The application is focused on a data set composed by more than 900 images in TIFF format with an average spatial resolution of 3800×3000 pixels and depth on a scale of 8 bit/pixel grey from Mexican cinema. In Fig. 1, "Watermarking" includes the embedding of both watermarks invisible and visible; "Visual inspection of Visual Camouflaged Watermark" only refers to visible watermark; and "Watermark Detection" corresponds only to the invisible watermark.

In Fig. 2, the proposed algorithm is represented in a more detailed form. Blocks inside blue rectangle correspond to the "Watermarking" process shown in Fig. 1; first block, "Camouflaged Watermarking", represents original image processing to embed the visible watermark, W1, in the best region that best camouflages it, and generating secret key K1; second block, "Watermark Generation", uses K1 and user's data to create the invisible watermark W2; third block, "Invisible Watermarking", represents invisible watermark embedding in watermarked image obtained from first block, resulting in the dual watermarked image. "Watermark Extraction" block corresponds only to invisible watermark recovery using K2. Block inside orange lines corresponds to the "Visual Inspection of Visual Camouflaged Watermark" method shown in Fig. 1; where "Visual Inspection" block corresponds only to visible watermark identification by visual inspection using K1. Blocks inside pink rectangle corresponds to "Watermark Detection" of Fig. 1; here there are two decisions to make in order to detect whether or not there was an image misuse, first diamond decision determines if there is any doubt of infringement; if there is, then we proceed to look for invisible watermark, represented by block "Watermark Detection"; second diamond decision compares recovered watermark with reference and determines if indeed there has been an image infraction.

The parameters used in this proposal are shown in Table I and Fig. 3 shows the sample pictures of dataset.

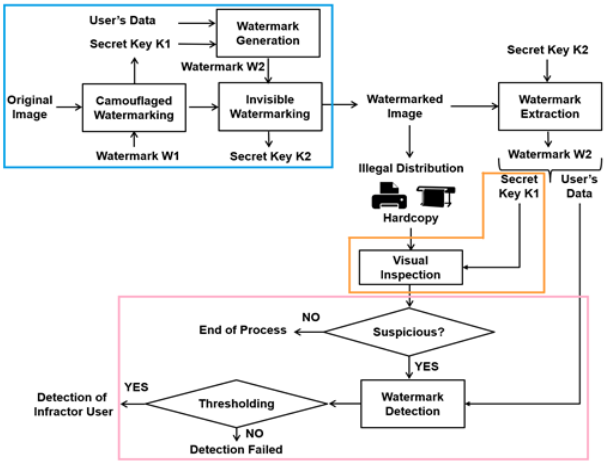
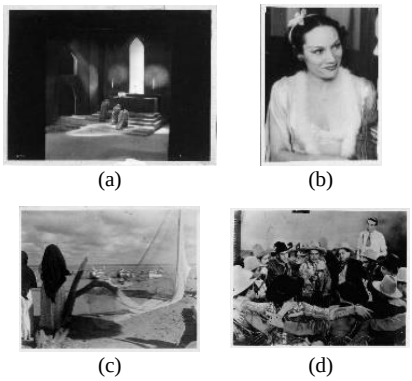


Figure 2. Block diagram of the proposed dual watermarking method.

TABLE I. SUMMARY OF PARAMETERS USED IN THE PROPOSED METHOD

Parameter	Value
Secret key K_1	Spatial coordinates of the logo watermark W_1
Watermark W_2	80 bits when RIPEMD-160 is applied to key information of authorized users
Secret key K_2	Pair of radiuses r_1 and r_2, as well as the watermark strength α used in by invisible watermarking, defined in a dynamically automatic manner based on the PSO algorithm optimization
Decision threshold value T_d	$T_d = 0.75$



(a) (b) (c) (d)

Figure 3. Sample pictures of dataset. (a) Image obtained from "Dos monjes" film, (b) image obtained from "La mancha de sangre" film, 1937, (c) Image obtained from "Redes" film, 1936, and (d) Image obtained from "Vamonos con Pancho Villa" film, 1936 (film titles are between quotation marks and in Spanish). Using a dataset Photographs courtesy of Filmoteca, property of Filmoteca UNAM.

A. *Camouflaged Watermarking*

The dataset used for the study case is composed by more than 900 digital TIFF images obtained by scanning of antique photographs and posters from cultural heritage of Mexican cinema, whose digital dimensions fluctuate between 1455 ×1950 and 22484 × 16614 pixels. The characteristics of this dataset represent different challenges: scanning process was done by different individuals resulting in grayscale images with 3 layers, additionally, scanning introduces artifacts, content is heterogeneous (portraits, landscapes, buildings, groups of people, etc.) and orientation also varies. Then, considering these characteristics, the robust visible watermark was developed for grayscale images to embed a binary watermark in spatial domain for copyright protection.

B. *Embedding Algorithm*

Visible watermark is embedded in spatial domain by selecting the area with the best features to achieve proper camouflage and visibility.

According to Fig. 4, during the first step called, *Noise reduction*, the image to be protected, I_o, is decomposed by cartoon-texture decomposition [24] into two components; Cartoon image, I_e, also known as Structure image that is a noise reduced image, and Texture image, $I_t = I_o - I_e$, which is binarized using Otsu threshold for practical purposes. The fixed parameters used in this step are the number of iterations It = 10 and the Lagrange multiplier λ = 0.1, this is done to balance blurriness and information extraction for suitable feature calculation. Both parameters control the amount of noise extracted from I_o, the bigger number of iterations It is, the more blurred I_e will be, resulting in more homogeneous regions for segmentation, additionally, the smaller λ is, more information I_t will have, resulting in artificial texture for segmentation.

In second step, *Visual Attention area*, saliency map algorithm [25] is applied to I_e, which has less noise than I_o, obtaining the saliency map, i.e., AV_m. Then, AV_m is binarized to get the visual attention mask, i.e., $AV_{m_{bin}}$, using a dynamic threshold to keep 50% of image's pixels, this percentage was chosen empirically to preserve enough area to embed visible watermark. Finally, this $AV_{m_{bin}}$ mask is applied to I_e to obtain the Visual Attention area, AV. Since pixels inside AV are assumed to have less probability to suffer cut attack, the working area is restricted to AV in both I_e and I_t, resulting in $I_{e_{AV}}$ and $I_{t_{AV}}$, which are the pixels inside the visual attention area of cartoon image, I_e, and texture image, I_t, respectively.

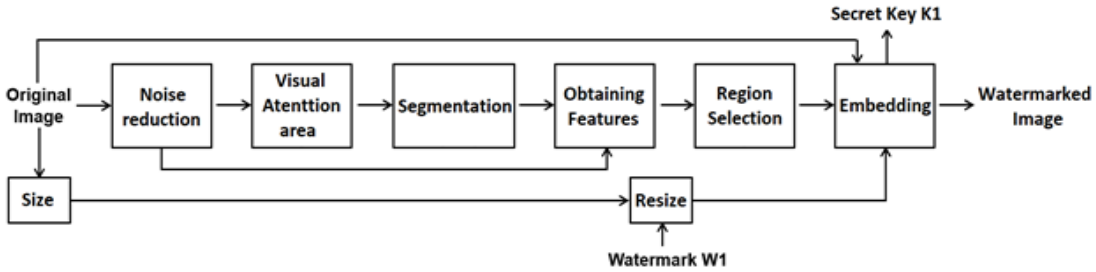


Figure 4. Visible camouflaged watermark embedding process.

In third step, *Segmentation*, superpixel SLIC segmentation is applied to $I_{e_{AV}}$, the resulting superpixel mask, i.e., SP_m, is used to divide in subregions both images: texture, $I_{t_{AV}}$, and structure, $I_{e_{AV}}$. Superpixel divides the image into homogeneous regions in terms of texture, grayscale, and visual semantics, which is desirable for watermarking. Furthermore, the parameters of this algorithm could be linked to the watermark size, which is done in this work.

In fourth step, *Obtaining Featur*e, numerical parameters are calculated, for each i^{th} subregion SP from $I_{e_{AV}}$ and $I_{t_{AV}}$, to obtain feature vectors V_c as shown in Table II. The numerical parameters represent desirable characteristics of $SP(i)$ for embedding the visible watermark, $SP_{tam}(i)$ represents the number of pixels, $SP_{ent}(i)$ represents the entropy, $SP_{var}(i)$ represents the variance, $SP_{prom}(i)$ represents the average of tones of grey, and $SP_{sum}(i)$ represents the average of value's pixels of binarized texture image.

TABLE II. NUMERICAL PARAMETERS OF V_c FOR EACH SUPERPIXEL WITHIN THE VISUAL ATTENTION AREA, $SP_{tAV}(i)$ AND $SP_{eAV}(i)$.

Parameter	Calculation
Size	$SP_{tam}(i) = numel(SP_{eAV}(i))$
Clean Texture	$SP_{ent}(i) = H(SP_{eAV}(i))$ $SP_{var}(i) = \sigma^2(SP_{eAV}(i))$
Grayscale	$SP_{prom}(i) = \mu(SP_{eAV}(i))$
Noise Texture	$SP_{sum}(i) = \overline{SP_{tAV}(i)}$

In fifth step, *Region Selection*, once all the feature vectors, V_c, have been calculated, the SP that are within the ranges indicated in the following equations are eliminated.

$$SP_{tam}(i) < (n \times 1.5)^2 \quad (1)$$

$$SP_{prom}(i) \leq 38 \parallel SP_{prom}(i) \geq 217 \quad (2)$$

$$SP_{ent}(i) < \text{median}(SP_{ent}) \quad (3)$$

In Eq. (1), if SP values are too small to contain the binary watermark, less than 2.25 watermark area, then they are discarded. In Eq. (2), SP with mean colour of grey out of ranges are discarded, eliminating 30% of shades of grey, since the mean colour of grey is very close to white or black, the SP is not usable to embed the camouflage watermark because this means it has little texture. In Eq. (3), SP with poor texture are removed using median of SP_{sum} as threshold. Afterwards, the remaining SP are ordered from highest to lowest, separately by the texture values of SP_{var}, the variance of subregion, and SP_{ent}, the entropy of subregion. Finally, they are intersected, and the first SP listed as the optimum is chosen as the embedding region.

Before embedding the watermark, I_o size, i.e., $I_{tam} = [M, N]$, must be considered to modify the dimensions, i.e., n, of the square watermark according to the following equation [16]:

$$n = \left\lfloor \frac{\Delta}{0.125} \right\rfloor \quad (4)$$

where $r_M = \max(I_{tam})/719$, $r_m = \min(I_{tam})/529$, and $\Delta = \max(r_M, r_m)$.

Integers 719 and 529 refers to digest size, which is one of the most common printed formats. Constant 0.125 denotes 8 × 8 pixel square watermark related to digest size. A recommendation for better results is to manually improve the smallest binary watermark, especially if the watermark is complex. Used watermarks in experimentation are shown in Fig. 5.

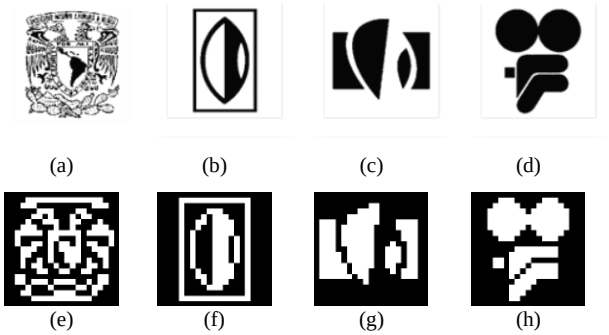


Figure 5. Square binary watermarks, size 250×250 pixels with white background (upper line) and square binary watermarks, size 21×21 pixels with black background (bottom line). From left to right UNAM shield (a and e), Cultural diffusion logos (b, f, c, and g) and Filmoteca logo (d and h). Images are property of UNAM.

In Fig. 6, results of different steps of the proposed algorithm are shown. Images a), e) and i) are original images; b), f) and j) correspond to $I_{e_{AV}}$, i.e., pixel inside visual attention area of structure image; c), g) and k) show the superpixel mask apply to $I_{e_{AV}}$; and d), h) and l) indicates the subregion selected to embed the watermark.

Before embedding, we make a last adjustment in the watermark depending on the value SP_{prom} of selected superpixel with the aim of improve the robustness as indicated in (5), threshold was selected simply dividing greatest grayscale value, 255, into two. This procedure increases the contrast between the watermark to be embedded, W_o, and the image to be watermarked I_o.

$$W_o = \begin{cases} W_N \rightarrow (\overline{\boldsymbol{W_N}} \leq \overline{\boldsymbol{W_B}} \,\&\, \overline{SP_{prom}} \in [127.5,\ 255]) \parallel (\overline{\boldsymbol{W_N}} > \overline{\boldsymbol{W_B}} \,\&\, \overline{SP_{prom}} \in [0,\ 127.5) \\ W_B \rightarrow (\overline{\boldsymbol{W_N}} \leq \overline{\boldsymbol{W_B}} \,\&\, \overline{SP_{prom}} \in [0,\ 127.5) \parallel (\overline{\boldsymbol{W_N}} > \overline{\boldsymbol{W_B}} \,\&\, \overline{SP_{prom}} \in [127.5,\ 255]) \end{cases} \quad (5)$$

Figure 6. Original images (1st column), Visual attention area $I_{e_{AV}}$ corresponding to second step (2nd column), Segmentation applying SP_m corresponding to third step (3rd column) and selected embedding region corresponding to fourth step (4th column). First and second row photographs from "Redes" film, and bottom row photograph from "El compadre Mendoza" (film titles are between quotation marks and in Spanish). Used Photographs are courtesy of Filmoteca, and property of Filmoteca UNAM.

where W_N is the watermark with black background (Figure 5h). W_B is the watermark with white background (Figure 5d). W_o is the watermark that is embedded.

For embedding, the centroid of the chosen SP is calculated and matched with the centre of the watermark, the embedding is being carried out using the following equation:

$$I_w = \alpha \times I_o + \beta \times W_o \quad (6)$$

where the embedding force parameters are α=0.80 and β=0.2. If β is too bigger watermark will be very noticeable, which is not desirable.

C. Visual Inspection Remarks

The visible watermark is intended to be imperceptible with naked eye for someone unaware of its existence, therefore it is embedded in a region with high texture, as can be observed in Fig. 7. Only the owner, who knows the watermark existence can have the secret key K_1. This K_1 could be both a JPEG image that is a miniature of the original image (visual Key), and the coordinates, represented in percentages and included in K_2, with the origin in the upper left corner (numeric Key), as it can be seen in Fig. 8. Furthermore, being camouflaged the visible watermark avoid intentional attacks designed to remove visible watermarks.

Our algorithm admits some variations that could increase the robustness of watermarking, such as choosing randomly one superpixel from the top five instead of the first one or embedding multiple watermarks using second or third top superpixels as illustrated in Fig. 9.

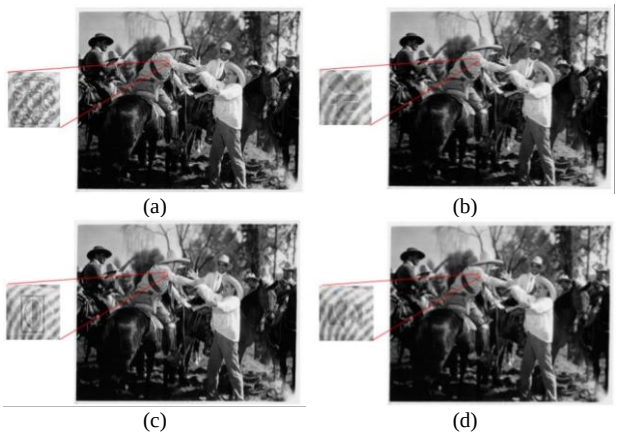


Figure 7. Watermarked images, using a photograph from "Vamonos con Pancho Villa" film (film titles are between quotation marks and in Spanish), courtesy of Filmoteca, property of Filmoteca UNAM.

Figure 8. Small red square visual Key (left) and numeric Key (right).

Figure 9. Image with multiple camouflaged watermarks, using a photograph from "Vamonos con Pancho Villa" film (film titles are between quotation marks and in Spanish), courtesy of Filmoteca, property of Filmoteca UNAM.

D. Invisible Watermarking

A robust invisible watermark is embedded in frequency domain after the camouflaged watermark has been embedded to conform the dual watermark.

1) Watermark generation

The invisible watermark is generated considering a set of data, *UD*, that is associated with authorized user of the digital image. This *UD* is made up of enunciative, but not limiting way, of the full name of the user, date of loan, requesting company, identifiers, such as, the federal taxpayer registry and the unique population registry, among others. Generation process of Watermark W_2 is as follows:

(1) Obtain the cryptographic summary of UD applying the RIPEMD-160 algorithm [26, 27], which binary result is stored in MD (Message-Digest Algorithm).

(2) Divide MD into 2 parts of 80 bits each and apply the exclusive- or operation- between both parts. The result of this operation is concatenated with the binary representation of the numeric secret key K_1 and the resulting string of bits constitutes the watermark W_2. In this way, in the extraction process when W_2 is recovered, the first 80 bits will be used for the detection of the possible use violation, while the rest of the bits of W_2 belong to the secret key K_1.

2) Embedding and extraction/detection algorithm

For the sake of briefness, we make use of our work previously published in [12] for the invisible watermarking stage in its insertion and extraction/detection stages, whose basis of operation are the domain of the Discrete Fourier Transform (DFT) and the Particle Swarm Optimization (PSO) algorithm [11], the latter is used to find the optimized values of the key parameters in 2D DFT-based invisible watermarking domain (Fig. 10), a pair of radii r_1 and r_2 and the annular area $A = \pi(r_2^2 - r_1^2)$.

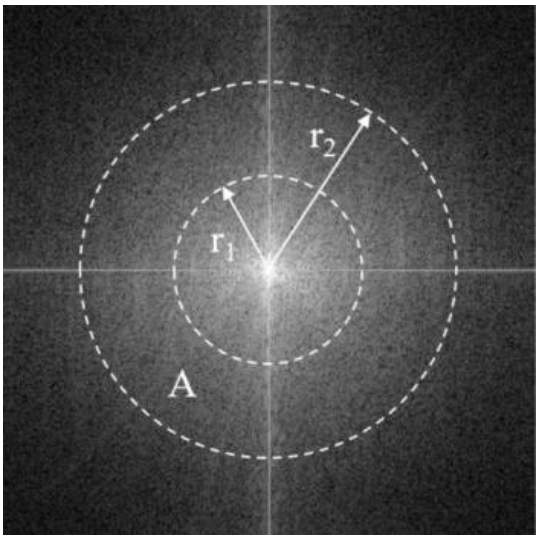


Figure 10. Parameters in 2D DFT-based invisible watermarking domain.

In general terms, the invisible watermarking based on PSO [12], determines the optimal values of the homocentric radii r_1 and r_2 used to define an annular insertion region *A* within the magnitude of the DFT of the image to be protected, thus as the optimal value of the insertion force factor α. To increase the robustness of the method, the watermarking algorithm implements the spread spectrum technique known as Direct Sequence Spread Spectrum (DS-CDMA) [28]. For its part, the objective fitness function of the PSO algorithm uses the Bit Correct Rate (BCR) criterion [29] as well as the Visual Information Fidelity (VIF) metric [30]. For further details, interested readers can refer to reference [12]. In this article, the images to be protected consider a depth of 8-bits per

pixel, and for the execution of the objective fitness function, the signal processes defined in Table III are considered.

TABLE III. DISTORTIONS CONSIDERED IN THE OBJECTIVE FITNESS FUNCTION OF THE PSO ALGORITHM

Attack	Tolerance
Average filter.	5×5 window
Scaling	Factor 0.6
JPEG compression	Quality factor 30
Gaussian noise	Mean = 0, Variance = 0.01

IV. EXPERIMENTAL RESULTS

The trade-offs between imperceptibility and robustness of both camouflaged watermark and invisible watermark is a challenging issue for researchers to overcome [31]. In this section, experimental results of the proposed method in terms of these requirements are shown. To do this, images of the Mexican cultural heritage under the protection of the Dirección General de Actividades Cinematográficas (Filmoteca) of the Universidad Nacional Autonóma de México (UNAM) were considered, in TIFF format with an average spatial resolution of 3800 × 3000 pixels and depth on a scale of 8 bit/pixel grey. The camouflage and invisible watermarking algorithms were implemented using Matlab © R2021b on a computer with Microsoft Windows © 11 operating system, Intel © Core i7 1.8Ghz processor and 16 GB RAM.

A. Watermark Imperceptibility Evaluation

Imperceptibility requires that the perceptual quality of the watermarked images, is preserved the best possible, aiming the watermarking to go unnoticed.

1) Invisible watermarking

The watermark imperceptibility was evaluated in terms of the Visual Information Fidelity (VIF) [30], Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM) [32] and the image quality metrics are defined by Eqs. (7−9), respectively.

$$PSNR(dB) = 10\,log_{10}\left(\frac{Max\ Pixel\ Value^2}{\frac{1}{N\cdot M}\left(\sum_{x=1}^{N}\sum_{y=1}^{M}(I(x,y)-I_w(x,y))^2\right)}\right), \quad (7)$$

$$SSIM(I,I_w)=\frac{(2\mu_I\mu_{Iw}+C_1)(2\sigma_{I\,Iw}+C_2)}{(\mu_I^2+\mu_{Iw}^2+C_1)(\sigma_I^2+\sigma_{Iw}^2+C_2)}. \quad (8)$$

In Eqs. (7) and (8), I and I_w are the original and the watermarked cinema images respectively, N and M denoted the spatial resolution of I. In Eq. (8) C_1 and C_2 are small constant values [32]. The SSIM value reflects perceptual distortions more precisely than the PSNR value. The range of SSIM values is [0, 1], and values closer to 1 represent better quality with respect to the original image. A value of 1 indicates that the original and the reference image are the same.

$$VIF=\frac{\sum_{t\in channels} I(\vec{C}^{R,t};\vec{F}^{R,t}\mid s^{R,t})}{\sum_{t\in channels} I(\vec{C}^{R,t};\vec{E}^{R,t}\mid s^{R,t})}. \quad (9)$$

As it is known in the literature [30], the VIF value Eq. (9) reflects perceptual distortions more precisely than the PSNR metric. The range of VIF values is [0, 1], and a closer value to 1 represents a better fidelity regarding the original image. Interested readers could refer to Ref. [30] to obtain more details about VIF metric. Table IV shows the imperceptibility results in terms of average values of PSNR, SSIM, and VIF respectively. In general, a PSNR value greater than 37dB [33] or an SSIM value greater than 0.9300 [32] means that the two compared images are not visibly different. In terms of SSIM, the average values are approximate to 0.99, which are quite satisfactory. For visible watermark qualitative methods were applied.

TABLE IV. AVERAGE VALUES OF PSNR, SSIM AND VIF

Metric	Average Value
PSNR	46.91 dB
SSIM	0.9952
VIF	0.9564

2) Visible camouflaged watermarking

The watermark imperceptibility was evaluated quantitatively calculating the mean value for watermarked data base, resulting in PSNR=58 dB and SSIM=0.99. To measure qualitatively the imperceptibility of the embedded watermarks, a questionnaire was applied to 22 people who evaluates 20 images. The results of this survey are shown in Table V. Additionally, we observed that the less texture the image has the easier to identify the watermark.

TABLE V. SURVEY OF IMPERCEPTIBILITY OF VISIBLE WATERMARK

Question	Yes	No
Identify watermarked image unaware it is watermarked	0%	100 %
Recognize watermark knowing image is watermarked without know the watermark	40%	60%
Recognize watermark knowing image is watermarked and know the watermark	50%	50%
Recognize watermark knowing the watermark and its localization	73%	27%

B. Watermark Robustness Testing

Robustness requires that the watermark can survive several attacks. Different attacks were performed over watermarked images to proof its robustness, such as geometric attacks, image processing, print-scan process.

1) Visible camouflaged watermarking

A representative sample of attacked visible watermark is shown in Fig. 11, the top right image from Fig. 7 is the one that receives the attacks, results are displayed in Fig. 11 where: (a) is the watermark without any attack; (b-q) correspond to print-scan attack which details are listed in Table VI; (r) increase in sharpness; (s) contrast enhancement; (t) increase in brightness; (u) blurring by median filter; JPEG lossy compression by (v) 90%; (w) 70%; (x) 50%; (y) 30%; (z) 10%; (aa) complement; (ab)

30% size reduction; and (ac) 50% size reduction. The experimental results show that visible watermark can resists several attacks since it is recognizable in attacked watermarked images.

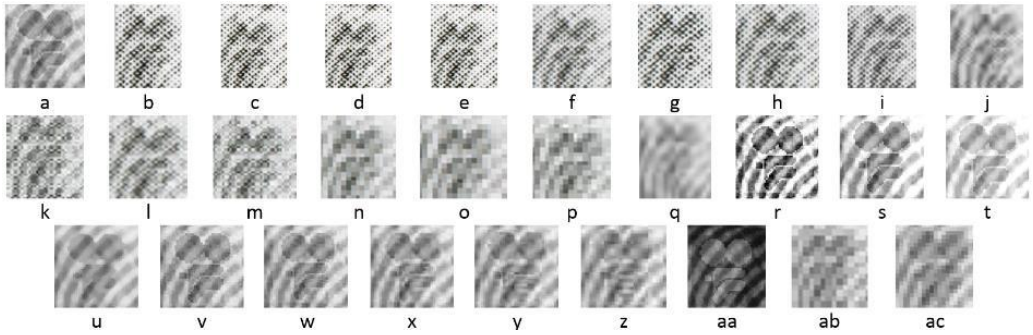


Figure 11. Extracted watermarks from image shown in Figure 7. (a) Watermark without attacks and (b-ac) attacked watermarks.

TABLE VI. DETAILED PRINT-SCAN ATTACKS SHOWN IN FIG. 11

Printer	Scanner Epson Perfection V600 Photo	Format	Letter
HP TopShot LaserJet Pro M275	150 ppi	PDF	b
		JPEG	c
		TIFF	d
		BMP	e
	300 ppi	BMP	f
		TIFF	g
		JPEG	h
		PDF	i
	600 ppi	PDF	j
		JPEG	k
		TIFF	l
		BMP	m
	1200 ppi	BMP	n
		TIFF	o
		JPEG	p
		PDF	q

2) Invisible watermarking

A decision threshold value T_d must be defined to determine if W_2 is present or not into the image I_w. Considering a binomial distribution with success probability equal to 0.5, a false alarm probability P_{fa} for L watermark data bits is given by Eq. (10), where a threshold value T must be controlled to get a smaller value of P_{fa} is define as follows:

$$P_{fa} = \sum_{\lambda=T}^{L} (0.5)^{L} \cdot \left(\frac{L!}{\lambda!(L-\lambda)!} \right) \quad , \tag{10}$$

where L = 80 is the length of W_2. Based on the Bernoulli trials assumption, λ is an independent random variable with binomial distribution [34].

The false alarm probability must be less than 10^{-6} which is set to satisfy the requirements of most watermarking applications for a reliable detection [34], and then an adequate decision threshold value T_d is defined by Eq. (11):

$$T_d = 1 - \left(\frac{T}{L} \right) \quad , \tag{11}$$

From Eq. (10), considering L = 80 and T = 60, then T_d = 0.75, according to the fact that BER + the Bit Correct Rate (BCR) must be equal to 1. If the BCR value between W_2 and W_2' is less than 75%, the detection process considers the absence of W_2, otherwise, W_2 is detected in a successful manner, detecting the infringer user. The robustness testing is classified in signal processing and geometric distortions, as well as combined attacks composed by JPEG compression with quality factor 70 + either signal processing or geometric distortions. The robustness testing is shown in Tables VII, VIII and IX, respectively.

TABLE VII. AVERAGE BCR VALUES TO GEOMETRIC DISTORTIONS

Geometric distortion	Average BCR Value
Rotation 45°	0.99
Rotation 135°	0.99
Scaling 0.6	0.99
Scaling 2	1
Central cropping 256×256	1
Translation x= 200, y=200	1

TABLE VIII. AVERAGE BCR VALUES TO SIGNAL PROCESSING

Signal processing	Average BCR Value
Without attack	1
JPEG QF = 20	0.90
JPEG QF = 30	0.98
JPEG QF = 50	0.99
Gaussian noise μ=0, σ^2=0.01	0.94
Gaussian noise μ=0, σ^2=0.05	0.86
Impulsive noise density=0.09	0.79
Speckle noise μ=0, σ^2=0.15	0.78
Speckle noise μ=0, σ^2=0.09	0.80
Average filtering 3×3	0.99
Average filtering 5×5	0.99
Histogram equalization	1
Gaussian filtering 7×7	1
Sharpening	1
Brightness reduction	0.99
Brightness increase	0.99
Median filtering 3×3	0.99
Motion filtering 5×5	0.99
Gamma correction γ=2	1
Gamma correction γ=0.5	0.99

TABLE IX. AVERAGE BCR VALUES TO COMBINED DISTORTIONS

Combined distortions JPEG 70 +	Average BCR Value
Gaussian noise μ=0, σ^2=0.01	0.93
Gaussian noise μ=0, σ^2=0.05	0.76
Impulsive noise density=0.09	0.77
Speckle noise μ=0, σ^2=0.09	0.76
Average filtering 3×3	0.99
Average filtering 5×5	0.96
Histogram equalization	1
Gaussian filtering 7×7	0.99
Sharpening	1
Brightness reduction	0.98
Brightness increase	0.98
Median filtering 3×3	0.98
Motion filtering 5×5	0.99
Gamma correction γ=2	0.99
Gamma correction γ=0.5	0.99
Rotation 45°	0.98
Rotation 135°	0.98
Scaling 0.6	0.99
Scaling 2	0.99
Central cropping 256×256	0.98
Translation x= 200, y=200	0.98

C. Performance Comparison with Similiar Dual Watermarking Methods

Different dual watermarking technics were studied, compared data is shown in Table X. It is remarkable that none were tested for print-scan attack and our proposal has the best PSNR.

In [35], a blind invisible dual watermarking mechanism for colour images is presented, consisting in one robust watermark into YCbCr colour space applying DWT and one fragile watermark into the RGB space. In [36] a dual robust watermarking scheme for copyright protection is proposed by embedding one image watermark into the RGB colour space and other binary watermark into the YCbCr colour space of a host colour image. In [23] a dual watermarking scheme for intensive copyright protection is presented, this scheme consists in a visible watermark image directly embedded on the spatial domain of the host image, and an invisible watermark image hidden in the frequency domain by utilizing the just notable distortion technique. In [37] a blind watermarking scheme is proposed by embedding robust and fragile watermarks in a host image for simultaneous copyright protection and image authentication.

TABLE X. COMPARISON WITH OTHER DUAL WATERMARKING ALGORITHMS

Methods	Images	Robustness	Embedding domain	Visibility	Extraction	Copyright protection	Image authentication	PSNR
Proposed scheme	Grayscale	Robust Robust	Spatial DFT	Visible Invisible	Blind Non blind	Yes	No	~47 dB
Liu *et al.* [35]	Colour	Fragile Robust	Spatial DWT	Invisible Invisible	Blind Blind	Yes	Yes	~40 dB
Lusson *et al.* [36]	Colour	Robust Robust	Spatial Spatial	Invisible Invisible	Blind Non blind	Yes	No	~39 dB
Lin *et al.* [23]	Grayscale	Robust Robust	Spatial DCT	Visible Invisible	Blind Blind	Yes	No	~30 dB
Lu and Liao [37]	Colour	Fragile Robust	DWT DWT	Invisible Invisible	Blind Non blind	Yes	Yes	~40 dB

V. CONCLUSIONS

This research proposed a watermark embedding and extracting for dual watermarking scheme applied to antique digitized cinema images described in Sect. III. We implemented embedded authorized user data using Discrete Fourier Transform, the particle swarm optimization (allowing to adjust in an automatic form its key operation parameters) and Direct Sequence Spread Spectrum for invisible watermarking. On the other hand, for visible watermarking we use cartoon-texture decomposition, saliency map, and superpixel SLIC. The experimental results have been shown in Sect. IV, and these results are compared to the equivalent of some state-of-the-art existing watermarking techniques demonstrating good performance. Then, in this paper, the main contribution corresponds to the development of a visible watermark that is camouflaged and resistant to print-scan. Such visible watermark is combined with an invisible watermark containing important data to track copies, providing a high security robustness. The copyright protection of images has not been extensively explored for print-scan attacks. However, a real security problem was identified over Mexican cultural heritage digitized cinema images, that may be printed, then scanned, and distributed without authorization. For this reason, this proposal uses a camouflaged watermark in conjunction with an invisible watermark. Both watermarks work together to identify if a distributed image is authorized to be used. Results showed that the embedded information has high robustness and can be used to track image copies effectively. Furthermore, the additional security information does not affect the quality of the image, obtaining PSNR values greater than other dual-watermark proposals. This research is important because implements a watermarking solution for a specific set of images with features giving solution to Filmoteca's necessity, and to the best of our knowledge, it does not exist any algorithm as the one we present, thus contributing to watermarking field.

CONFLICT OF INTEREST

On behalf of all authors, the corresponding author states that there is no conflict of interests.

AUTHOR CONTRIBUTIONS

Conceptualization: Laura Reyes-Ruiz, and Manuel Cedillo-Hernandez; validation Oswaldo Juarez-Sandoval, Eduardo Fragoso-Navarro, Laura Reyes-Ruiz, and Manuel Cedillo-Hernandez; investigation: Francisco Garcia-Ugalde, Oswaldo Juarez-Sandoval, Eduardo Fragoso-Navarro, Laura Reyes-Ruiz, and Manuel Cedillo-Hernandez; resources: Francisco Garcia-Ugalde, and Mariko Nakano-Miyatake; data curation: Laura Reyes-Ruiz, and Manuel Cedillo-Hernandez; writing—original draft preparation, Laura Reyes-Ruiz, and Manuel Cedillo-Hernandez; writing—review and editing: Oswaldo Juarez-Sandoval, Eduardo Fragoso-Navarro, Francisco Garcia-Ugalde, and Mariko Nakano-Miyatake; funding acquisition: Francisco Garcia-Ugalde. All authors have read and agreed to the published version of the manuscript.

ACKNOWLEDGMENT

Authors would like to thank the Dirección General de Actividades Cinematográficas (Filmoteca) of the Universidad Nacional Autónoma de México (UNAM) that kindly gave us the authorization to use their dataset images to carry out this work, the Consejo Nacional de Ciencia y Tecnología de México (CONACYT), the PAPIIT IT-100123 research project and Postdoctoral Scholarship Program from DGAPA-UNAM, as well as the Instituto Politécnico Nacional (IPN) by the support provided during the realization of this research.

REFERENCES

[1] M. Barni and F. Bartolini, "Applications," in *Watermarking Systems Engineering:* Enabling *Digital Assets Security and Other Applications*, 1st ed., Boca Raton, New York: CRC Press, 2004, pp. 23–44. doi: https://doi.org/10.1201/9780203913512

[2] P. Bas, T. Furon, F. Cayre, *et al.*, "A quick tour of watermarking techniques," in *Watermarking Security : Fundamentals, Secure Designs and Attacks*, W. S. Gan, C. C. J. Kuo, T. F. Zheng, and M. Barni, Eds., Singapore: Springer, 2016, pp. 13–31. doi: https://doi.org/10.1007/978-981-10-0506-0

[3] M. Barni, I. J. Cox, T. Kalker, *et al.*, "Digital watermarking," in *Lecture Notes in Computer Science*, 2005. doi: https://doi.org/10.1007/11551492

[4] I. J. Cox, M. L. Miller, and J. A. Bloom, "Applications and Properties," in *Digital Watermarking*, USA: Morgan Kaufmann, 2002, pp. 11–40. doi: 10.1016/B978-155860714-9/50003-1

[5] I. Cox, M. Miller, J. Bloom, *et al.* (2008). *Digital Watermarking and Steganography (Series in Multimedia Information and Systems)*, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann. [Online]. Available: https://www.elsevier.com/books/digital-watermarking-and-steganography/cox/978-0-12-372585-1

[6] M. Cedillo-Hernandez, A. Cedillo-Hernandez, F. Garcia-Ugalde, *et al.*, "Digital color images ownership authentication via efficient and robust watermarking in a hybrid domain," *Radioengineering*, vol. 26, no. 2, pp. 536–551, 2017. doi: https://doi.org/10.13164/re.2017.0536

[7] L. Ji and S. Kumar, "Robust digital watermarking techniques for copyright protection of digital data: A survey," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 3, pp. 3819–3825, 2021. doi: 10.1007/s11277-021-08177-w

[8] H. Tao, L. Chongmin, J. M. Zain, *et al.*, "Robust image watermarking theories and techniques: A review," *J. Appl. Res. Technol.*, vol. 12, no. 1, pp. 122–138, 2014. doi: 10.1016/S1665-6423(14)71612-8

[9] O. U. Juarez-Sandoval, M. Cedillo-Hernandez, M. Nakano-Miyatake, *et al.*, "Digital image ownership authentication via camouflaged unseen-visible watermarking," *Multimed. Tools Appl.*, vol. 77, pp. 26601–26634, 2018. doi: https://doi.org/10.1007/s11042-018-5881-0

[10] F. Ahmad and L. M. Cheng, "Authenticity and copyright verification of printed images," *Signal Processing*, vol. 148, pp. 322–335, 2018, doi: 10.1016/j.sigpro.2018.02.029

[11] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proc. International Conference on Neural Networks*, 1995, pp. 1942–1948, doi: 10.1002/9780470612163

[12] M. Cedillo-Hernandez, A. Cedillo-Hernandez, and F. J. Garcia-Ugalde, "Improving DFT-based image watermarking using particle swarm optimization algorithm," *Mathematics*, vol. 9, no. 1795, pp. 1–20, 2021, doi: 10.3390/math9151795

[13] W. Qi, Y. Liu, S. Guo, *et al.*, "An adaptive visible watermark embedding method based on region selection," *Security and Communication Networks*, vol. 2021, 2021.

[14] W. F. Hsieh and P. Y. Lin, "Imperceptible visible watermarking scheme using color distribution modulation," in *Proc. IEEE 9th Int. Conf. Ubiquitous Intell. Comput. IEEE 9th Int. Conf. Auton. Trust. Comput.*, 2012, vol. 1, pp. 1002–1005, doi: 10.1109/UIC-ATC.2012.13

[15] O. Juarez-Sandoval, E. Fragoso-Navarro, M. Cedillo-Hernandez, *et al.*, "Improved imperceptible visible watermarking algorithm for auxiliary information delivery," *IET Biometrics*, vol. 7, no. 4, pp. 305–313, 2018, doi: 10.1049/iet-bmt.2017.0145

[16] A. Cedillo-Hernandez, M. Cedillo-Hernandez, F. Garcia-Ugalde, *et al.*, "A visible watermarking with automated location technique for copyright protection of portrait images," *IEICE*, vol. E99-D, no. 6, pp. 1541–1552, 2016.

[17] E. E. Abdallah, A. B. Hamza, and P. Bhattacharya, "A robust block-based image watermarking scheme using fast Hadamard transform and singular value decomposition," in *Proc. Int. Conf. Pattern Recognit.*, 2006, vol. 3, pp. 673–676. doi: 10.1109/ICPR.2006.167

[18] M. A. Suhail and M. S. Obaidat, "Digital watermarking-based DCT and JPEG model," *IEEE Trans. Instrum. Meas.*, vol. 52, no. 5, pp. 1640–1647, 2003, doi: 10.1109/TIM.2003.817155

[19] N. Jimson and K. Hemachandran, "DFT based coefficient exchange digital image watermarking," in *Proc. Second Int. Conf. Intell. Comput. Control Syst.*, 2018, pp. 567–571.

[20] N. Singh, S. Joshi, and S. Birla, "Suitability of singular value decomposition for image watermarking," in *Proc. 6th Int. Conf. Signal Process. Integr. Networks*, 2019, pp. 983–986, doi: 10.1109/SPIN.2019.8711749

[21] E. E. Abdallah, A. B. Hamza, and P. Bhattacharya, "Watermarking 3d models using spectral mesh compression," *Signal, Image Video Process.*, vol. 3, no. 4, pp. 375–389, 2009, doi: 10.1007/s11760-008-0079-y

[22] E. E. Abdallah, A. B. Hamza, and P. Bhattacharya, "Spectral graph-theoretic approach to 3D mesh watermarking," in *Proc. Graph. Interface*, 2007, pp. 327–334, doi: 10.1145/1268517.1268570

[23] P. Y. Lin, J. S. Lee, and C. C. Chang, "Dual digital watermarking for internet media based on hybrid strategies," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 8, pp. 1169–1177, 2009, doi: 10.1109/TCSVT.2009.2020263

[24] C. A. Micchelli, L. Shen, Y. Xu, *et al.*, "Proximity algorithms for the L1/TV image denoising model," *Adv. Comput. Math.*, vol. 38, no. 2, pp. 401–426, 2013, doi: 10.1007/s10444-011-9243-y

[25] L. Itti, C. Koch, and E. Niebur, "A model of saliency-based visual attention for rapid scene analysis," vol. 20, no. 11, pp. 1254–1259, 1998.

[26] H. Dobbertin, A. Bosselaers, and B. Preneel, "RIPEMD-160: Astrengthened version of RIPEMD," *Lect. Notes Comput. Sci.*, vol. 1039, pp. 71–82, 1996, doi: 10.1001/archsurg.1983.01390100008003

[27] A. Bosselaers, H. Dobbertin, and B. Preneel, "The RIPEMD-160 cryptographic hash function," *Dr. Dobb's J.*, vol. 22, no. 1, pp. 24–28, 1997.

[28] J. G. Proakis and M. Salehi, "An introduction to information theory," in *Digital Communication*, 5th ed., McGraw-Hill, 2008, p. 336–361, doi: 10.4018/978-1-7998-6745-6.ch010

[29] O. E. Okman and G. B. Akar, "Quantization index modulation-based image watermarking using digital holography," *J. Opt. Soc. Am. A*, vol. 24, no. 1, pp. 243–252, 2007, doi: 10.1364/JOSAA.24.000243

[30] H. R. Sheikh and A. C. Bovik, "Image information and visual quality," *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process-*

in *Proc.*, vol. 15, no. 2, pp. 430–444, 2006, doi: 10.1109/icassp.2004.1326643
[31] A. Bhowmick and S. M. Hazarika. (May. 2018). *Advances in Electronics,* Communication *and Computing*. [Online]. Available: http://arxiv.org/abs/1606.01042%0Ahttp://link.springer.com/10.1007/978-981-10-4765-7
[32] Z. Wang, A. C. Bovik, H. R. Sheikh, *et al.*, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, 2004, doi: 10.1109/TIP.2003.819861
[33] H. A. Chang and H. H. Chen, "Stochastic color interpolation for digital cameras," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 8, pp. 964–973, 2007, doi: 10.1109/TCSVT.2007.897471
[34] C. W. Tang and H. M. Hang, "A feature-based robust digital image," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 950–959, 2003, doi: https://doi.org/10.1109/TSP.2003.809367
[35] X. L. Liu, C. C. Lin, and S. M. Yuan, "Blind dual watermarking for color images' authentication and copyright protection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 5, pp. 1047–1055, 2018, doi: 10.1109/TCSVT.2016.2633878
[36] F. Lusson, K. Bailey, M. Leeney, *et al.*, "A novel approach to digital watermarking, exploiting colour spaces," *Signal Processing*, vol. 93, no. 5, pp. 1268–1294, 2013, doi: 10.1016/j.sigpro.2012.10.018
[37] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579–1592, 2001, doi: 10.1109/83.951542

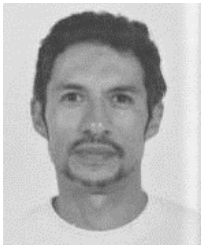
Laura Reyes-Ruiz was born in México. In 2007 she received the B.S. degree in mechatronic engineering from the Universidad Panamericana (UP), the M. S. degree in Engineering in the 2016 from the Universidad Nacional Autónoma de Mexico (UNAM). Currently she is a PhD student in the codification and security of the Systems Communication Laboratory (CSSCL) in the Engineering Faculty of the UNAM and part time professor at Instituto Tecnológico de Tláhuac. Her current research interests include video, image and signal processing, multimedia applications and mechatronic systems. Prof. Reyes-Ruiz is a member of IEEE and ACM.

Eduardo Fragoso-Navarro was born in Mexico. He received the M. S. degree in microelectronics and the PhD. degree in electronics and communications engineering from the Mechanical–Electrical Engineering School of the Instituto Politécnico Nacional (IPN) of Mexico, Mexico City, in 2017 and 2022, respectively. Currently, he continues his research career in a posdoctoral stay at Universidad Nacional Autónoma de México (UNAM), Mexico City. His research interests are digital image processing, information security, data hiding and watermarking.

Oswaldo Juarez-Sandoval was born in Mexico. He received the B.S. degree in communication and electronics engineering, the M.S. degree in microelectronics engineering and the PhD in the communication and electronic in the 2009, 2013 and 2018 respectively from the Instituto Politécnico Nacional of Mexico (IPN) where he is professor. Currently he is works at the ESIME Culhuacan of the IPN. His principal research interest is security information, image and signal processing, hidden information, steganography and steganalysis, informatics forensic, hardware security and related fields.

Manuel Cedillo-Hernandez was born in Mexico. He received the B.S. degree in computer engineering, the M.S. degree in microelectronics engineering and his PhD in communications and electronic from the Instituto Politecnico Nacional of Mexico (IPN) in the years 2003, 2006 and 2011, respectively. He has six years of professional experience at Government positions related to IT. From September 2011 to December 2015, he was with the Engineering Faculty of 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.

Mariko Nakano-Miyatake was born in Japan. She received the B.S. degree in applied mathematics, the M.S. degree in and master of engineering from the University of Electro-Communication in Japan in the years 1983 and 1985, respectively, her PhD in sciences from the Universidad Autónoma Metropolitana, Iztapalapa Campus (UAM-I) in 1988. Currently she is a research professor at the Postgraduate Study and Research Section (SEPI) of the Instituto Politécnico Nacional (IPN), Culhuacán Campus.



Francisco Garcia-Ugalde was born in Mexico. He received the B.S. degree in electronics and electrical system engineering from UNAM in 1977, his Diplôme d'Ingénieur from SUPELEC France in 1980, and his PhD in 1982 in information processing from Université de Rennes I, France since 1983. Currently he is a full-time professor, and he was appointed to head of the Codification and Security of the Systems Communication Laboratory (CSSCL) in the Engineering Faculty of the Universidad Nacional Autónoma de México (UNAM). His current research 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, hidden information, parallel processing and data bases.