

Digital image ownership authentication via camouflaged unseen-visible watermarking

Oswaldo Ulises Juarez-Sandoval¹ • Manuel Cedillo-Hernandez¹ Mariko Nakano-Miyatake¹ • Antonio Cedillo-Hernandez¹ • Hector Perez-Meana¹

Received: 8 March 2017 / Revised: 10 January 2018 / Accepted: 13 March 2018 © Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract In recent years, end users can easily capture digital images using several devices, such as smartphones, mobile devices and digital imaging cameras, allowing such images to be easily copied, manipulated, transmitted or format converted without any restrictions. This fact suggests the necessity to develop digital tools, such as digital watermarking, to solve the issues associated with copyright protection and ownership authentication of digital images. To claim the ownership of a digital image, we propose a camouflaged, unseen-visible watermarking technique based on luminance and texture properties in conjunction with an image enhancement criterion. The proposed method has some advantages over invisible and visible watermarking methodologies in terms of readability and imperceptibility of the watermark, respectively. The experimental results demonstrate that the proposed scheme is effective and applicable for digital images on a variety of topics, including natural scenes and man-made objects, both indoors and outdoors. A comparison with previously reported methods based on unseen-visible watermarking techniques is also provided.

Keywords Watermarking \cdot Image-processing \cdot Information security \cdot Unseen-visible watermarking \cdot Ownership authentication

1 Introduction

Currently, digital image processing is a speedily growing technology. With the exponential growth of networked multimedia systems, end-users have found new applications for digital

Manuel Cedillo-Hernandez mcedilloh@ipn.mx

¹ Instituto Politecnico Nacional SEPI ESIME Culhuacan, Avenida Santa Ana 1000, San Francisco Culhuacan Coyoacan, Ciudad de Mexico, Mexico

images in fields such as entertainment, business, and education. This behavior has increased the need for developing efficient methods to address copyright protection problems [3, 4, 14, 21]. Digital image watermarking is considered a suitable solution for ownership authentication purposes since it is able to add a signal to an image that can seal or mark it [6, 9, 12]. According to different applications and requirements, digital image watermarking can be mainly classified into two types: invisible and visible. In invisible watermarking, a signal called a 'watermark' is embedded in the spatial or frequency domain of the image [5, 7, 22, 26, 38] in such a way that observers are incapable of distinguishing the difference between the original and watermarked images with the naked eye. The embedded watermark must be robust, i.e., must remain in the image after intentional or non-intentional attacks are performed. Thus, invisible watermarking methods can protect the copyright of images without affecting their visual quality. To retrieve the previously embedded watermark signal, an invisible watermarking algorithm requires an auxiliary extraction/detection stage be performed with the help of complex algorithms. Without this auxiliary stage, the watermark readability is almost impossible. On the other hand, in visible watermarking, the main objective is to demonstrate the copyright of images via the exhibition of a visual pattern directly on the image, and viewers can easily recognize the intellectual property with the naked eye [8, 29, 32]. One of the most important requirements is to embed the visual pattern on the image in an unobtrusive manner to avoid affecting the visual quality of the image. However, the overlap of a visible pattern inevitably affects the image visual quality, which can reduce its usability and/ or its commercial value.

Recently, in the literature, a new class of digital image watermarking schemes has been proposed to help copyright protection and ownership authentication issues. This technique is known as "unseen-visible watermarking" and was first introduced by [13] in 2007.

In general terms, unseen-visible watermarking involves embedding a visible watermark signal into an image that is not perceptible to the naked eye. The watermark signal becomes visible in the image whenever adequate image enhancement operations, which are usually fast and computationally non-complex, are performed. There are two main advantages to this approach: first, it allows ownership claiming of digital images in a practical way, i.e., without a complex detection/ extraction stage; second, the watermark imperceptibility is preserved. Although unseen-visible watermarking is a promissory research field that has several advantages over conventional visible and invisible watermarking approaches, it has some issues in imperceptibility and robustness that must be addressed for it to be considered a proper solution for copyright protection and ownership authentication issues. Table 1 summarizes the main differences in unseen-visible watermarking versus visible and invisible watermarking approaches.

In fact, the architecture of the proposed unseen-visible watermarking scheme is similar to conventional digital image watermarking, as shown in Fig. 1, either the visible or invisible modality.

To claim ownership authentication of color images, we propose in this paper a novel camouflaged unseen-visible watermarking based on luminance and texture properties in conjunction with an image enhancement criterion. The proposed algorithm has some advantages over invisible and visible watermarking in terms of readability (i.e., a complex auxiliary detection/extraction stage is not needed) and transparency (i.e., the watermark is not embedded in an obtrusive form in the image content), respectively. The experimental results demonstrate that the scheme is effective and applicable for digital color images with different content. The rest of the paper is organized as follows: Section 2 explains in detail the related work previously reported in the literature, Section 3 describes the algorithms for the embedding

Parameter	Invisible approach	Visible approach	Unseen-visible approach
Invisible watermark pattern	Yes	_	Yes
Visible watermark pattern	_	Yes	Yes
Identify ownership	Yes	Yes	Yes
Deterrence against theft	No	Yes	Yes
Prohibit unauthorized duplication	No	Yes	Yes
Transparency of image content	High	Low	High
Quality of watermarked image	High	Low	High
Need of explicit extractor/detector	High	_	Low
Robustness	High	Low	High
Computational complexity	Often Higher	Low	Low
Versatility of media content	Yes	Yes	Yes

Table 1 Main differences in unseen-visible watermarking versus visible and invisible watermarking approaches

and exposure processes, the experimental results, including the parameter settings, and a comparative analysis are presented in Section 4. Finally, Section 5 concludes this work.

2 Related works

To the best of our knowledge, only a few methods for unseen-visible image watermarking have been proposed in the scientific literature. In the follow paragraphs, we explain the representative proposals.

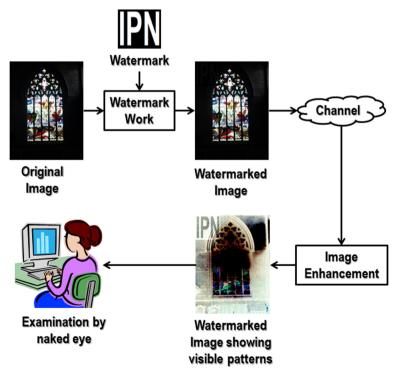


Fig. 1 Architecture of the proposed method

2.1 Unseen-visible watermarking based on gamma correction

In the literature, we found a scheme in [13, 19] that presented an algorithm that embeds a visible watermark into the spatial domain of a given color image. First, the algorithm selects the embedding region and the intensity level of the adjustment using the image enhancement criterion based on the gamma correction operation. Using these parameters, a visible watermark is embedded through a set of embedding rules that previously included an image denoising operation; i.e., viewers cannot notice the change under common viewing conditions, so the watermark is not perceptible to the naked eye. To solve this drawback and improve the image quality, the authors in [20] proposed a method that improved the proposal in [13, 19] using criteria based on the concepts of Just Noticeable Distortion (JND) and the Total Variation L^1 -Norm in the watermarking embedding process. To reveal the watermark in [13, 19, 20], a gamma correction function must be directly applied to the image or well by changing the viewing angles of the display devices. The main motivations of the proposals in [13, 19, 20] are that gamma correction operations can be easily integrated into most display devices to provide a watermark delivery scheme without any additional overhead deployment. The experimental results confirmed the relevance of the schemes in [13, 19, 20]; however, both require the existence of large smooth regions with dark hues within the host image, which is a prerequisite that constrains the practicability of the schemes and represents a serious drawback.

2.2 Unseen-visible watermarking based on histogram modification

The authors in [23] proposed a method based on the observation of the post-camera histogram operation to achieve a suitable color range that allows a visible watermark to be concealed in color images. In general terms, the method selects the largest homogenous region with the smallest variance in each RGB color model channel in the image. Then, based on the maximum and minimum mean value of the largest homogenous region of each RGB channel in conjunction with a threshold criterion, the watermark pattern is embedded into the color image. To reveal the watermark, a histogram modulation is performed into an interval, which requires the mean value and threshold criterion previously defined in the embedding stage. This method improves on the drawbacks presented in [13, 19] because it can be implemented using several color images with different visual content. In addition, it provides robustness against several signals processing and geometric distortions. However, the scheme has a couple of drawbacks. The first drawback is the dependence on the mean value and threshold criteria to reveal the watermark because the method may become informed watermarking. Both parameters will be required by authorized users to modulate the histogram; otherwise, the watermark is not revealed. The second drawback is the weak robustness of the method to reveal the watermark pattern when the watermarked image is compressed by JPEG lossy compression, which is currently a very common operation used in most digital image processing tasks.

2.3 Unseen-visible watermarking applied to 3D video content

Recently, unseen-visible watermarking has been extended to other applications, such as 3D video content. The authors in [24] proposed unseen-visible watermarking for color plus depth map 3D images based on depth image-based rendering. The embedded watermark is exposed by adjusting the rendering conditions. In general terms, the depth image-based rendering

produces virtual view images by warping the color images according to the per-pixel depth information, and the watermark is embedded into the 3D video signal by modifying the depth map with variations in the pixel values. However, in [24], the watermark pattern cannot always be adequately exposed when the variations in the pixel values are too small. Because the selection of variations in the pixel values is a critical issue in 3D unseen-visible watermarking schemes, the authors in [27, 28] proposed a method to solve the drawback in [24]. The method is based on a depth no-synthesis error model for defining the optimal pixel value of a watermark to create high-quality 3D video signals. Thus, the method in [24] only embeds the watermark in the farthest region of the depth map, but in [27, 28], the scheme can detect and find the region of the depth images that is suitable for watermark embedding. The schemes applied to 3D video content [24, 27, 28] show robustness against JPEG lossy compression and geometric scaling but show poor robustness against intentional attacks because simple common signal processing, such as noise corruption or image blurring, can remove the watermark information [28].

3 Proposed method

Thanks to the recent technological advances of the Internet, many people watch movies, TV series and documentaries on his/her personal computer or mobile device using online streaming video services. In 2016, the most important streaming media company extended their service to 130 new countries, and the number of subscribers has reached more than 87 million [2]. Moreover, almost all the digital images currently captured are uploaded to a social network on the Internet. This behavior has increased the need for developing efficient methods to address copyright protection and ownership authentication problems [3, 4, 14, 21].

Image enhancement operations are often applied to help exposing image information which was taken under constrained conditions, i.e. are used to reveal details or content not visible by naked eye, via the adequate adjusting of the contrast settings. In the context of unseen-visible image watermarking, if the unprotected picture is hypothetically regarded as a stego image hidden with some unseen information (details or content not visible by naked eye), the image enhancement operation inherently corresponds to the process of altering the viewing condition and revealing the hidden watermark [13], as illustrated in Fig. 1. Considering this situation, an unseen-visible watermarking technique must be adapted for this environment, i.e., where the enhancement function is not limited to the functions available for the display, such as the gamma function [19] or histogram modification [23].

Then, considering the limitations presented in the state of the art review [13, 19, 20, 23, 24, 27, 28], we introduce in this paper a camouflaged unseen-visible watermarking (CUVW) method for claiming the ownership of color images. Our proposed scheme adopts a watermark embedding strategy that involves luminance and texture properties to camouflage an unseen-visible watermark pattern. This feature allows the method to be effective on color images of a variety of topics, including natural, outdoor, indoor, landscape, people, objects and buildings scenes. The CUVW proposed method consists of embedding and exposure algorithms, which are explained in detail as follows. Figure 2 shows the general diagram of the CUVW proposed watermarking method. In general terms, to achieve a higher robustness without affecting the quality of the color image, our method embeds the watermark signal using the luminance information from the YCbCr color model and the texture properties obtained via a texture classification method based on discrete cosine transform (DCT) and a Just Noticeable Distortion (JND) criterion. As a consequence, the

proposed method is robust against aggressive geometric and signal processing distortions. The embedding process is accomplished in a post-processing form on the captured images and not at its acquisition moment. Our experiments revealed that the visual watermark can be observed after performing JPEG lossy compression with several quality factors, e.g., common signal processing distortions, such as noise corruption, geometric distortions and artistic image filtering, that are currently common operations performed by smartphones and other mobile devices. Meanwhile, the watermark exposure algorithm used to reveal the hidden information does not require auxiliary data and is a non-time-consuming process. The exposure can be accomplished via two methods: image enhancement composed of logarithmic and negative transformations and using any digital electronic device with a camera and varying the image enhancement parameters.

3.1 Definition of the color model

The literature in the research field contains different color models that have been used to represent several color components, which can be more or less independent. One of the major issues in color image processing is finding the appropriated color model for the problem being addressed. According to [6, 11], the RGB color model has the most correlated components, and the YCbCr color model components are the least correlated. The forward and backward transformations between both models are linear. Hence, if RGB is used into the design of a watermarking algorithm, the modification of one or more components independently to the others is not necessarily the best way, because the perceived colors are dependent of the three channels together, reason why is called a correlated model. However, the YCbCr model allows

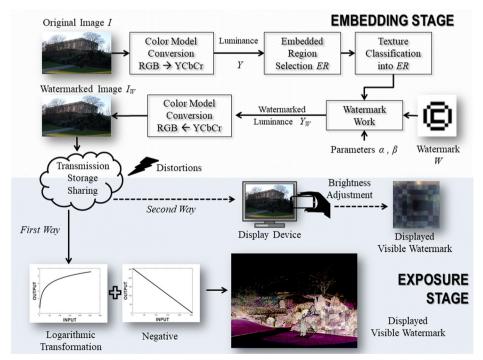


Fig. 2 General diagram of the CUVW proposed method

for uncorrelated components to be obtained and has the advantage of the luminance information being separate from the chrominance information [11]. Based on these facts, YCbCr was adopted as suitable color model for the proposed CUVW watermarking method.

3.2 Embedding algorithm

Embedding the watermark in the luminance information in the YCbCr color model gives the mark a certain number of robust properties with respect to JPEG lossy compression and other common signal processing. The embedding algorithm is described as follows:

Step 1. Convert the RGB color model of the original image, *I*, to the YCbCr color model and isolate the luminance, *Y*, from YCbCr. Figure 3 shows a sample result of step 1 of embedding algorithm.

Step 2. From the luminance information, *Y*, of size *MxN*, select the central pixel (\hat{x}, \hat{y}) of the embedded region, denoted *ER*, that satisfies the condition given by (1), where $n_1 x n_2$ are the dimensions of *ER* and the watermark, *W*. The variables (x,y) denote the spatial coordinates, and *wn* denotes a window for sliding all pixels of *Y* to find (\hat{x}, \hat{y}) . Figure 4 shows a set of sample results of step 2 of embedding algorithm.

$$(\hat{x}, \hat{y}) = \min_{(x,y)} \left(\frac{1}{n_1 \cdot n_2} \cdot \sum_{i,j \in \Omega} wn(i,j) \right), where \ \Omega = \begin{cases} i \in \left[x - \frac{n_1}{2}, x + \frac{n_1}{2} \right] \\ j \in \left[y - \frac{n_2}{2}, y + \frac{n_2}{2} \right] \end{cases}, x = 1, \dots, My = 1, \dots, N \quad . \tag{1}$$

Step 3. Once the embedding region, *ER*, is obtained, a texture classification process is performed to improve the imperceptibility requirement and obtain the camouflaged effect as follows, and the general diagram is shown in Fig. 5. The original *ER* is divided into non-overlapping blocks of 8×8 pixels denoted by b_k where $k = 1, 2, ..., (n_1 \cdot n_2)/(8 \times 8)$. The reason for the size 8×8 is to ensure compatibility with the JPEG lossy image

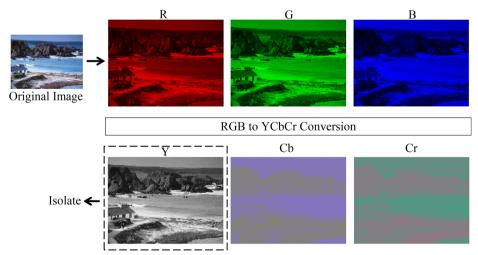


Fig. 3 Sample result of step 1 of embedding algorithm



Fig. 4 Several sample results of step 2 of embedding algorithm

compression standard. Then, DCT is applied to each block b_k , and we obtain the DCT coefficients, denoted F_k . In this way, inspired by [18], an estimation of the average brightness and texture complexity based on the DCT domain is performed to classify each block, b_k , inside the *ER* region into three classes: (*class 1*) dark and weak texture, (*class 3*) semi-dark and strong texture, and (*class 2*) the remaining blocks.

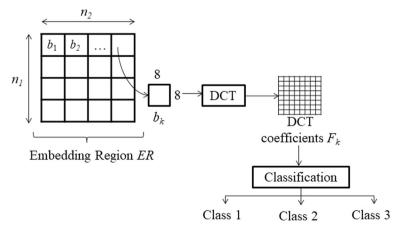


Fig. 5 General diagram of texture classification process

if
$$(NZ_k < T_1 \text{ and } F_k(1,1) < T_2)$$
 then $b_k = class 1$
else if $(NZ_k > T_1 \text{ and } F_k(1,1) < T_2)$ then $b_k = class 3$
else $b_k = class 2$

Fig. 6 Pseudocode of the classification of each block, b_k

According to the DCT properties, the DC term, F_k (1,1), represents the average brightness of each block, b_k . The texture complexity in each block, b_k , is estimated via a quantization of the DCT coefficients, F_k (u,v), where u,v=1,2,...,64 represents the frequency. The same algorithm used in the JPEG image compression is used to compute the amount of non-zero coefficients, denoted NZ_k , which is given by (2):

$$NZ_k = \sum \{ \lfloor (F_k(u, v)/Q(u, v)) \rfloor \neq 0 \} \quad , \tag{2}$$

where $\lfloor \cdot \rfloor$ denotes the integer part of the quotient, Q is a JPEG quantization matrix, and Q(u,v) denotes the quantization step at the frequency term (u,v). A large NZ_k value results in a stronger texture in b_k . Based on the F_k (1,1) and NZ_k values, the classification of each block, b_k , is computed, as shown Fig. 6.

In Fig. 6, T_1 and T_2 are predefined threshold values that are determined in Section 5. Figure 7 shows a sample result of step 3 of embedding algorithm.

Step 4. Once each block, b_k , is classified, W is divided in non-overlapping blocks of 8×8 pixels, denoted W_k , using the binary watermark pattern, W, of size $n_1 \times n_2$ and $\{0, 1\}$ values. Consequently, each W_k is embedded into each b_k according to the following scenarios: If b_k is classified as *class 1*, the pixel value, $b_k(x,y)$, in the spatial domain is modified by (3):

$$if \quad W_k(x,y) = 0$$

$$b'_k(x,y) = b_k(x,y) + \beta$$

$$else$$

$$b'_k(x,y) = b_k(x,y) - \beta ,$$
(3)

where (x,y) denotes the spatial coordinates, b'_k is the watermarked block, and β is a watermark strength factor.

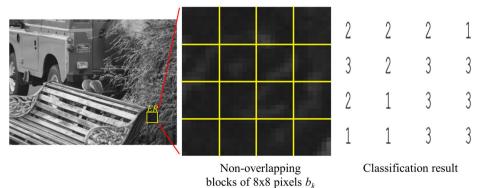


Fig. 7 Sample result of step 3 of embedding algorithm

Supposing b_k is classified as *class 2 or class 3*, the pixel value, $b_k(x,y)$, in the spatial domain is watermarked using (4):

$$if \quad W_k(x,y) = 0$$

$$b'_k(x,y) = b_k(x,y) + \frac{b_k(x,y)\cdot\alpha}{2}$$

$$else$$

$$b'_k(x,y) = b_k(x,y) - \frac{b_k(x,y)\cdot\alpha}{2} \quad ,$$
(4)

where (x,y) denotes the spatial coordinates, b'_k is the watermarked block, and α is a watermark strength factor. Figure 8 shows a sample result of step 4 of embedding algorithm.

Step 5. Finally, once *W* is embedded into *ER* in a camouflaged manner, the watermarked image, I_w , is constructed using the watermarked luminance component, Y_w , and the chrominance components, *Cb* and *Cr*, and converting the Y_wCbCr components back to the RGB color model representation. Figure 9 shows a sample result of step 5 of embedding algorithm.

3.3 Exposure algorithm

3.3.1 Image processing by a software solution

Given a watermarked image, $I_{\nu\nu}$, the ownership authentication may be proven by revealing the embedded watermark, W, via two non-complex methods.

Step 1. In the first method, I_w is processed using the logarithmic transformation given by (5):

$$I_{\log} = c \cdot \log(1 + I_w) \quad , \tag{5}$$

where c is a constant and $I_w \ge 0$. Figure 10 shows a sample result of step 1 of exposure algorithm using the image processing solution.

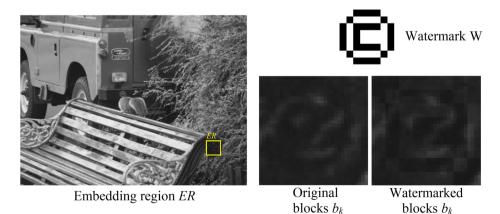


Fig. 8 Sample result of step 4 of embedding algorithm

🖉 Springer



Fig. 9 Sample result of step 5 of embedding algorithm. a Original image I. b Watermarked image I_w

Step 2. Subsequently, the output image, I_{log} , is processed by a negative function, given by (6):

$$I_r = T(I_{\log}) \quad , \tag{6}$$

where the transformation function, *T*, maps out the input range, [0-L-1] to $[L-1-I_{log}]$, *L* is the gray-scale resolution, and I_r shows the revealed watermark. Because not all display devices can manipulate the above transformations in a practical manner, the image processing given by (5) and (6) is provided in a software solution, which can be executed by any computing device. Figure 11 shows a sample result of step 2 of exposure algorithm using the image processing solution.

3.3.2 Image enhancement by a mobile device

To preserve the watermark exposure in practical scenarios, the watermark pattern can be revealed in our proposal via a second method by superimposing a digital electronic device, such as a smartphone or tablet with a camera, onto the display device in which the watermarked image is shown and only varying the image enhancement parameters, such as the brightness or contrast, of the camera until the watermark is exposed in the display.



Fig. 10 Sample result of step 1 of exposure algorithm using the image processing solution. **a** Watermarked image I_w , **b** Image I_w after logarithmic transformation

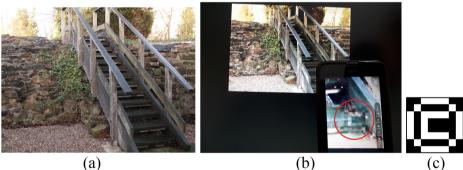


Fig. 11 Sample result of step 2 of exposure algorithm using the image processing solution. a Image with logarithmic transform, I_{log} . **b** Negative of (a) which shows the revealed watermark

Figure 12 shows a sample result of exposure algorithm using the image enhancement by a mobile device.

Both exposure procedures in the proposed method are complementary, and their performance ensures that the watermark is revealed in a correct manner.

The proposed method is inspired by real-world watermarks and keeps the advantages of both visible and invisible digital image watermarking methodologies, summarized into Table 1. In practice, the real-world watermarks are embedded into physical objects, e.g., in the bills or



(a)

(b)

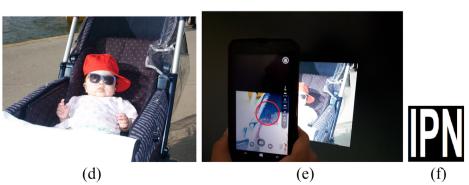


Fig. 12 Sample result of exposure algorithm using the image enhancement by a mobile device. a Watermarked image, I_w b Exposure demo using a mobile device. c Watermark. d Watermarked image, I_w e Exposure demo using a mobile device. (f) Watermark

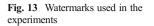
credentials, where such watermarks are invisible or at least unobvious under normal viewing conditions. However, if is necessary to prove the validity of the object, it is only required to change the viewing condition in certain way, e.g. by looking at the watermarked object against light sources, then the watermark information will become recognizable by naked eye [13].

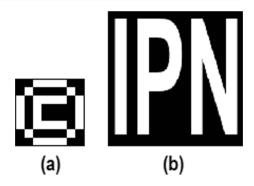
In a digital image context, an image processed by an unseen-visible watermarking method does not show visible patterns under normal viewing configurations [13], hence, the users can enjoy high-quality viewing experience of contents. Then, if the viewing conditions change, e.g. via an image enhancement operation such as gamma correction, histogram equalization, logarithmic function etc., the recognizable watermark pattern will revealed on the watermarked image and can be clearly recognized by naked eye. This technique is known as "unseen-visible watermarking" and was first introduced by [13] in 2007, which is basically a visible watermarking method. However, the visual quality obtained by the unseen-visible watermarking method is very close to invisible watermarking methods under normal viewing conditions. In fact, the architecture of the proposed unseen-visible watermarking scheme is similar to the real-world watermarking scheme and the conventional digital image watermarking, as shown in Fig. 1, either the visible or invisible modality.

4 Experimental results

In this section, the performance of the CUVW proposed algorithm was evaluated considering the watermark imperceptibility and robustness requirements using two datasets. The first dataset is the UCID dataset [33] that currently consists of 1338 uncompressed TIFF color images 512×384 in size with a color resolution of 24 bits per pixel. The second set is the RAISE-1k dataset [15] with high-resolution RAW images that are uncompressed and guaranteed to be camera-native in TIFF format and 4288×2848 in size with a color resolution of 24 bits per pixel. Our experiments were performed on a workstation running Microsoft Windows 10[°]C with an Intel[°]C Xeon[°]C 2.4 Ghz processor, 32" LED monitor and 16 GB of RAM, and the embedding procedure was implemented using Matlab© 9.1.0.441655 (R2016b). For the image enhancement exposure procedure, we used a Nokia Lumia 630[°]C mobile device with a 5 MP digital camera with autofocus and a 1/10.16 cm size sensor and a 4.5" LCD IPS display with a resolution of 854×480 pixels. The main reason for selecting this mobile device for the experiments was to establish a minimum requirement for our proposal, assuming that other robust devices will provide better results. A 2D binary pattern was used as the watermark, W, with a size $n_1 x n_2$. The watermarks used in the experiments are shown Fig. 13.

Figure 13a is 24×24 in size and was used in the UCID dataset. Figure 13b is 128×128 in size and was used in the RAISE dataset. The watermarked image quality was measured using the following known indices, the Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM). The difference in the color of the watermarked image was obtained using the Normalized Color Difference (NCD) measurement. The watermarked image robustness was tested using several geometric distortions, such as rotation, affine transformation, and aspect ratio changes; common signal processing, such as JPEG lossy compression, filtering, Gaussian and impulsive noise, and sharpening; and several artistic filters applied using the design software. Finally, our experimental results were compared with previously reported unseen-imperceptible visible watermarking research.





4.1 Parameter settings

In this section, we show the configuration of the main parameters used by the CUVW proposed method, which are the thresholds, T_1 and T_2 , that are used in the texture classification process, the watermark strength factors, α and β , that are used in the embedding algorithm, the constant value, c, that is used by the logarithmic transformation in the watermark exposure algorithm.

4.1.1 Threshold T₁

Considering the textures in the USC-SIPI image database [36] and the JPEG quantization matrix with a quality factor (QF) of 50, we obtained the average non-zero coefficients, NZ_k , using the procedure given by Eq. (2). For illustrative purposes and to show the behavior of NZ_k , in Fig. 14 we show the results obtained using a set of 4 textures that are 72 × 72 in size and classified as weak (Fig. 14, labels a and b) and strong (Fig. 14, labels c and d) textures, respectively. In this experiment, k = 1, 2... 9. In Fig. 14, we show that all the non-zero coefficients, NZ_k , of each b_k that belong to the weak textures (Fig. 14a–b) remain under a value of 10, i.e., $NZ_k < 10$. On the other hand, all the non-zero coefficients, NZ_k , of each b_k that belong to the strong textures (Fig. 14c–d) always exceed 10, i.e., $NZ_k > 10$. According to this behavior, $T_I = 10$ is considered a suitable value.

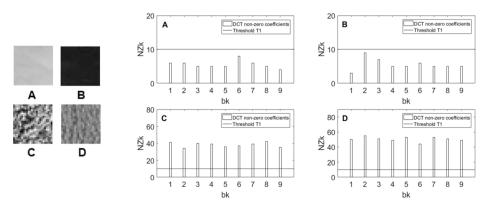


Fig. 14 Determination of the threshold T_1

4.1.2 Threshold T_2

To determine the threshold T_2 value, several aspects of the human visual system (HVS) were considered. The Human Visual System (HVS) is less sensitive to the lowest and highest intensity levels compared with the middle intensity level. The JND determines the intensity difference that the HVS cannot perceive, which is the difference between the intensity of the forward pattern and the intensity of the background, depending on the background intensity level. To determine the gray scale resolution, *gsr*, based on the background intensity level, we used the relationship provided by [40], which was formulated by (7). Based on the contrast sensitivity function of human vision after computation, the gray scale resolution of human eyes is shown in Fig. 15 [39, 40].

$$gsr = \begin{cases} -\frac{1}{8}p + 6, \quad p \in (0, 32) \\ -\frac{1}{32}p + 3, \quad p \in (33, 64) \quad p = 0, 1, 2, \dots 255 \\ \frac{1}{96}p + \frac{1}{3}, \quad p \in (65, 255) \end{cases}$$
(7)

Variable *p* in (7) is a pixel value. In Fig. 15 on the *x*-axis, we show the gray-scale range of an 8-bit depth resolution. In the lowest level (near the gray-scale 0 value), the human eye can distinguish six gray levels; i.e., the 0 and 6 Gy level values are perceived as the same by human eyes. At the gray scale value of 64, the gray level is stronger, and the human eye can distinguish one gray level. The same behavior occurs at gray level 255, and three gray levels can be perceived. According to this characteristic of HVS, to obtain a proper classification of each block, b_k , into *ER*, we considered the region where the human eye is not as sensitive, i.e., the gray value range from 0 to 31, and the threshold T_2 is set at $T_2 = 32$ for the gray scale value.

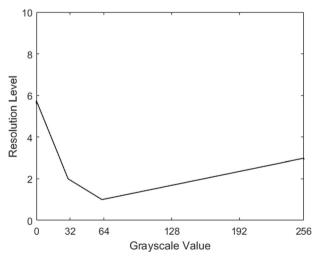


Fig. 15 The gray scale resolution of human vision [39, 40]

4.1.3 Watermark strength factors α and β

Considering the UCID and RAISE-1k datasets, the embedding algorithm was based on the spatial domain of the luminance information, *Y*, of the original color image, *I*, and the watermark strength factors, $\beta = [1, 3, 6, 9]$ and $\alpha = [0.1, 0.3, 0.6, 0.9]$. To determine the proper value of α and β , the PSNR metric was used in this experiment to measure the watermark imperceptibility, and it is given by (8):

$$PSNR(dB) = 10\log_{10}\left(\frac{MaxPixelValue^2}{(MSE_Y + MSE_{Cb} + MSE_{Cr})/3}\right) , \qquad (8)$$

where MSE is the Mean Square Error. Beginning with the average PSNR results obtained from the UCID dataset, we show three PSNR plots in Fig. 16 when: a) α is fixed and β is variable, b) α is variable and β is fixed, and c) α and β are simultaneously variable. Figure 16 shows that a large value of α or β increases the readability of the watermark, but the imperceptibility requirement decreases for large values of α or β . Hence, there is a trade-off between the readability and imperceptibility. Given the spatial resolution and content of the images from the UCID dataset, we show in Fig. 16 that the watermark strength factor α has a greater influence than β on the watermark imperceptibility. Figure 16 also shows that for $\alpha = 0.3$ and $\beta = 3$, the average PSNR is 61.89 dB, which indicates a good performance in terms of imperceptibility.

Considering the same conditions as the previous experiment and only replacing UCID with the RAISE-1k dataset, Figure 17 shows that a large β value increases the readability of the watermark, but the imperceptibility requirement decreases for large values of β . Again, there is a trade-off between the readability and imperceptibility. Given the high resolution and content of the images from the RAISE-1k dataset, Figure 17 shows that the watermark strength factor β has a greater influence than α on the watermark imperceptibility. Figure 17 also shows that for $\alpha = 0.3$ and $\beta = 3$, the average PSNR is 68.13 dB, which indicates a good performance in terms of imperceptibility. According to this behavior in the UCID and RAISE-1k datasets, $\alpha =$ 0.3 and $\beta = 3$ are suitable values for the embedding algorithm.

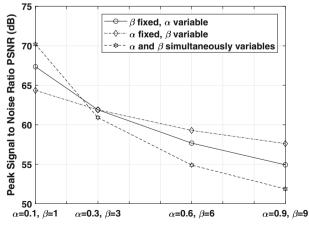


Fig. 16 Average PSNR obtained from the UCID dataset

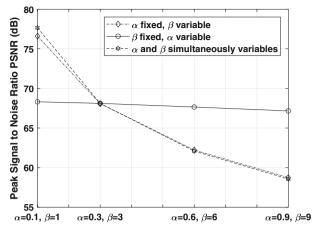


Fig. 17 Average PSNR obtained from RAISE-1k dataset

4.1.4 Constant value, c, for the logarithmic transformation

The constant value, c, of the logarithmic transformation used to reveal the watermark may be adaptive. Using the logarithmic transformation given by (5), Figure 18 shows the different curves obtained with values of c = 3, 5, 7 and 9.

Figure 18 shows that any curve can perform the expansion/compression of the gray scale values, and using a *c* value between 3 and 9 ensures the correct readability of the watermark in the proposed method. In summary, the main parameters used by the CUVW proposed method and the final values are shown in Table 2.

4.2 Watermark imperceptibility

As explained in the previous paragraphs, the proposed CUVW algorithm embeds a watermark logo in the luminance information of the YCbCr color model. Therefore, a careful watermark imperceptibility evaluation is compulsory. Using the values $\beta = 3$ and $\alpha = 0.3$, the watermark imperceptibility was evaluated in terms of the PSNR, SSIM [37] and NCD [10] image quality metrics defined by (8), (9) and (10), respectively.

$$SSIM(w,z) = \frac{(2\mu_w\mu_z + C_1)(2\sigma_{wz} + C_2)}{(\mu_w^2 + \mu_z^2 + C_1)(\sigma_w^2 + \sigma_z^2 + C_2)}.$$
(9)

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.

$$NCD = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} \left(\sqrt{(\Delta L(x,y))^{2} + (\Delta a(x,y))^{2} + (\Delta b(x,y))^{2}} \right)}{\sum_{x=1}^{M} \sum_{y=1}^{N} \left(\sqrt{(L(x,y))^{2} + (a(x,y))^{2} + (b(x,y))^{2}} \right)}$$
(10)

On the other hand, the normalized color difference, NCD [10], is based on the CIELAB color space, and it is applied to measure the difference in the color between two images. A

🖄 Springer

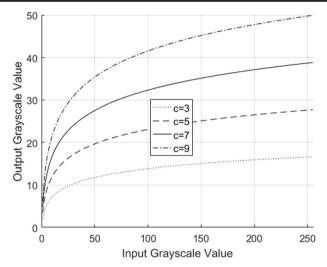


Fig. 18 Logarithmic transform with different constant value c

value closer to 0 represents a better quality with respect to the original image. A value of 0 indicates that the original and reference image are the same. Table 2 shows the average imperceptibility results obtained from the UCID dataset using different watermark sizes of 16×16 , 24×24 and 32×32 . Table 3 shows the average imperceptibility results obtained from the RAISE-1k dataset using different watermark sizes of 64×64 , 128×128 and 256×256 . Imperceptibility is measured in terms of the PSNR, SSIM and NCD metrics. As shown in Tables 3 and 4, a larger watermark value, *W*, with a size, $n_1 x n_2$, increases the readability of the watermark, but the watermark imperceptibility is diminished.

Again, there is a trade-off between the readability and imperceptibility. Globally, in all cases, the obtained PSNR values are greater than 58 dB for the UCID dataset and 68.13 dB for the RAISE-1k dataset. The SSIM values are closer to 1, and the NCD values are closer to 0. Although the idea to hide large logos in wide flat regions is attractive, this may not be the best choice in certain applications because flat regions may not exist in all images, and changes visible to the naked eye are directly proportional to the size of the logo. Hence, assuming that a small or large logo may protect the copyright or authenticate ownership in similar way, we considered the watermark sizes of 24×24 and 128×128 as suitable values to achieve the camouflaged effect of the proposed method and to preserve the trade-off between readability and imperceptibility based on our experiments, Tables 3 and 4 show that

Table 2 Summary of the parameters used in the proposed method	Parameter	Value
	Threshold T_I	10
	Threshold T_2	32
	Watermark strength factor α	0.3
	Watermark strength factor β	3
	Constant value c for logarithmic transform	3,5,7 or 9

	Average value		
Watermark size	PSNR (dB)	SSIM	NCD
16×16	66.1380	0.9992	0.0106
24×24	61.8903	0.9984	0.0107
32 × 32	58.7269	0.9975	0.0108

Table 3 Visual quality measured in terms of PSNR, SSIM and NCD for the UCID dataset

the CUVW proposed scheme provides fairly good fidelity of the watermarked image, and the difference in the colors between the watermarked and original images measured by the NCD metric is insignificant [31]. Figures 19, 20, 21, 22, and 23 show a set of original images, their watermarked versions and the revealed watermark.

4.3 Watermark robustness

To evaluate the watermark robustness of the proposed algorithm, several geometrical distortions, such as rotation by several angles, affine transformations, and translation with cropping, flipping, aspect ratio changes, and scaling; common signal processing, such as JPEG lossy compression using several quality factors, image corruption by Gaussian and impulsive noise, Gaussian and median filtering, sharpening, and histogram equalization; and several artistic filters supported by Adobe Photoshop© were performed. The experimental results are classified as geometric distortions, common signal processing and artistic filtering.

4.3.1 Geometric distortions

Figure 24 shows the robustness results of the CUVW proposed method in terms of watermark readability using the exposure procedure with image enhancement using the camera of a mobile device. The test image was obtained from the UCID dataset. According to the results in Fig. 24, we concluded that the CUVW proposed method has a good robustness against several geometric distortions, including aggressive rotation by 45° with auto-crop, translation with cropping, several affine transformations and scaling with a factor of 0.5, which all correctly revealed the watermark. In Fig. 24, the watermark readability obtained by the mobile device was sufficient to reveal the logo; however, this may be improved using another device with better hardware resources associated with the camera.

	Average value		
Watermark size	PSNR (dB)	SSIM	NCD
64 × 64	74.2357	0.9997	0.0106
128×128	68.1392	0.9993	0.0107
256 × 256	61.4401	0.9991	0.0109

Table 4 Visual quality measured in terms of PSNR, SSIM and NCD for the RAISE-1k dataset

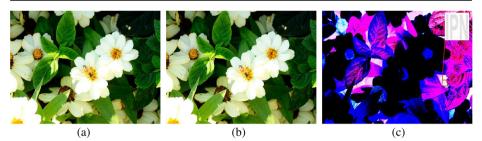


Fig. 19 a Original image. b Watermarked image. c Watermark readability with logarithmic-negative image processing. Test image 'natural' was obtained from RAISE-1k dataset

4.3.2 Common signal processing distortions

Figure 25 shows the robustness results of the CUVW proposed method in terms of the watermark readability using the exposure procedure with the logarithmic-negative image processing. The test image was obtained from the RAISE-1k dataset. Based on the obtained results, Figure 25 shows that the CUVW proposed method has a good robustness against several common signal processing distortions, including JPEG lossy compression with a quality factor of 70, 50 and 10, JPEG2000 lossy compression with a compression ratio from 1 to 100, image corruption by Gaussian noise with a tolerance $\mu = 0$, $\sigma 2 = 0.001$, and impulsive noise with a density of 0.05. Other signal processing applied to the watermarked images were median and Gaussian image filtering with window sizes of 5×5 and 7×7 , respectively. Likewise, the watermark readability of the proposed method was robust when the image was processed using image enhancement operations such as sharpening and histogram equalization.

4.3.3 Artistic filtering

Figure 26 shows the robustness of the results of the CUVW proposed method in terms of the watermark readability using the exposure procedure with the logarithmic-negative image processing. The test image was obtained from the RAISE-1k dataset. Figure 26 shows that the proposed method presents a high robustness against several artistic filters, which can be directly applied by the acquisition devices, e.g., smartphones or tablets, or using image edition software on a personal computer once the image is acquired. Because artistic filtering is a common practice that is growing with technology advances in mobile devices, our



Fig. 20 a Original image. b Watermarked image. c Watermark readability Watermark readability with logarithmic-negative image processing. Test image 'landscape' was obtained from RAISE-1k dataset



Fig. 21 a Original image. b Watermarked image. c Watermark readability with logarithmic-negative image processing. Test image 'people' was obtained from RAISE-1k dataset

experiments included a set of special distortions in the robustness test of unseen-visible watermarking algorithms.

4.4 Performance comparison

4.4.1 Computational complexity (speed): exposure of watermark via unseen-visible method versus extraction/detection of watermark via an invisible approach

The proposed algorithm based on unseen-visible watermarking has some advantages concerning invisible watermarking in terms of watermark readability, i.e., a complex auxiliary detection/extraction stage is not required. In general terms, the computational complexity (speed) is a factor related to the computation time for embedding and extracting the watermark in a digital watermarking system, which directly determines the computational complexity of each stage [25, 35]. In this way, the experiment in this section is focusing on the computational complexity comparative between extraction/detection stage of the invisible watermarking approaches reported in [1, 9, 12, 16, 17, 30, 34] versus watermark exposure of the proposed CUVW method. For all schemes, RGB color images 512 × 512 in size with a color resolution of 24 bits per pixel are considered. Our experiment was conducted on a workstation running Microsoft Windows 10[°]C with an Intel[°]C Xeon[°]C 2.4 Ghz processor with 16 GB of RAM, and the exposure and extraction/detection procedures were implemented using Matlab© 9.1.0.441655 (R2016b). Once the watermarked image was obtained by each method, it was distorted using an aggressive combined distortion composed by a rotation of 45° with autocropping, and then, the 'tic' and 'toc' functions of the Matlab© software were used to measure the elapsed time of each scheme for recover/detect and expose the watermark pattern,



Fig. 22 a Original image. b Watermarked image. c Watermark readability with logarithmic-negative image processing. Test image 'buildings' was obtained from RAISE-1k dataset



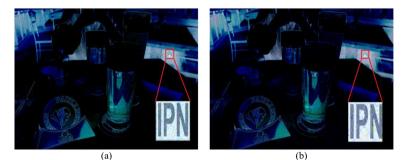
Fig. 23 a Original image. b Watermarked image. c Watermark readability with logarithmic-negative image processing. Test image 'outdoor' was obtained from UCID dataset



Fig. 24 Test image 'outdoor' was obtained from UCID dataset. **a** Without Distortion, (**b**) Rotation by 5° , (**c**) Rotation by 45° , (**d**) Affine Transformation [0.9,0.2,0;0.1,1.2,0;0,0,1], (**e**) Flip Horizontal, (**f**) Flip vertical, (**g**) Shearing *x*-direction [1 0 0; 0.5 1 0; 0 0 1], (**h**) Aspect Ratio Change [2,0,0;0,1.0,0;0,0,1], (**i**) Translation with Cropping x = 100, y = 100, (**j**) Scaling 0.5



Watermarked Image



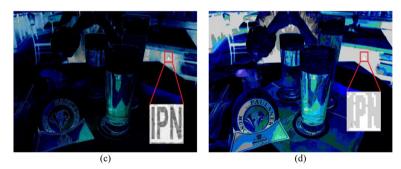


Fig. 25 Test image 'indoor' was obtained from RAISE-1k dataset. **a** Without Distortion, (**b**) JPEG Quality Factor = 70, (**c**) JPEG Quality Factor = 50, (**d**) JPEG Quality Factor = 10, (**e**) Gaussian noise, $\mu = 0$, $\sigma^2 = 0.001$, (**f**) Impulsive noise with density = 0.05, (**g**) Median filtering 5 × 5, (**h**) Gaussian filtering 7 × 7, (**i**) Sharpening, (**j**) Histogram equalization, (**k**) JPEG2000 Compression Ratio = 1, (**l**) JPEG2000 Compression Ratio = 100

respectively. To properly comparison, the reported time in Table 5 is the average of 150 run of each algorithm: [1, 9, 12, 16, 17, 30, 34] and the proposed one, respectively.

Table 5 shows the advantages of the proposed unseen-visible watermarking scheme related to invisible watermarking in terms of computation time of the exposure and the extraction/ detection procedures. In the literature, it is well known that geometric attacks desynchronize the embedding and extraction/detector stages of invisible watermarking algorithms. Thus, to be robust against geometric distortions, such as rotation with auto-cropping, invisible watermarking approaches need a complex auxiliary detection/extraction stage which is generally based on a frequency domain such as DFT, DCT, Contourlet or discrete wavelet transform DWT in conjunction with additional elements such as exhaustive search, hybrid domains, feature extraction, image normalization or neural networks, etc., in order to achieve



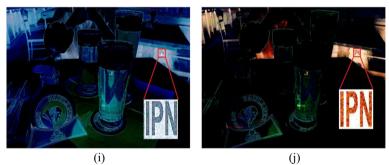






(g)

(h)





the correct watermark detection/extraction. It is clear that the more elements are included in the detection/extraction stage, the higher computational complexity is required. In this sense, invisible watermarking methods in [9, 17, 34] require an exhaustive search to extract/detect

Multimed Tools Appl

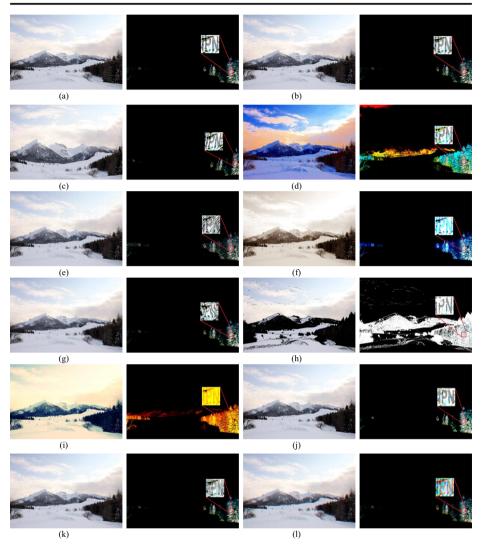


Fig. 26 Test image was obtained from RAISE-1k dataset. a Without Distortion, (b) Jitter, (c) Fisheye, (d) Color enhancement, (e) Texture added, (f) Sepia, (g) Wave, (h) Cartoon, (i) Cinema, (j) Oil painting, (k) Vertical tile, (l) Cellophane

correctly the watermark, obtaining average speeds of 44.63, 278.25 and 141.49 s, respectively, when the watermarked image was processed by the geometric distortion. On the other hand, method in [12] implements a hybrid watermarking technique composed by a chaotic mapping in the DCT domain in conjunction with a histogram modification procedure to extract/detect successfully the watermark, obtaining an average speed of 22.00s. There are other invisible watermarking methods that obtain average extraction/detection speeds under 10s, such as the case of approaches in [1, 16, 30], respectively. In this way, the method in [30] obtains a speed of 4.54 s, however, a drawback of the method in [30] is implementation of the Scale Invariant Feature Transform (SIFT) algorithm, which computational complexity is directly proportional of the image size, and that is a reason why it cannot be suitable to use with the high resolution

Table 5 Computation time comparative between unseen-visible method and invisible approach	comparative between u	inseen-visible met	hod and invisible	approach			
Unseen-visible approach: computation time (seconds)	Invisible approach: c	omputation time c	of the extraction/ of	Invisible approach: computation time of the extraction/ detection stages (seconds)			
Proposed method	Hybrid DFT-Contourlet domain [9]	0	DFT domain [34]	ontourlet DFT Hybrid DCT domain [17] domain [34] domain-histogram modification [12]	DCT domain-SIFT DCT domain-ims feature based [30] normalization [16]	DCT domain-SIFT DCT domain-image DWT domain-neural feature based [30] normalization network [1] [16]	DWT domain-neural network [1]
0.007 s	44.63 s	278.25 s	141.49 s	22.00 s	4.54 s	8.79 s	3.26 s

images, such as RAISE dataset. In the methods based on image normalization [16], the dimensions of the normalized original image and the normalized geometrically distorted image are different, as consequence the correct watermark extraction is difficult to be guaranteed and then additional correction procedures are needed, so it implies an increase of the computational complexity. For its part, the method in [1] has the dependence of a probabilistic neural network, which in conjunction with an embedding/extraction procedures based on the DWT domain, are designed to work only with a fixed image size that guarantees a low computational complexity. However, although the method in [1] obtains a relatively low speed of 3.26 s, it constraints in terms of image and feature vector sizes, limiting their application to high resolution images, such as RAISE dataset.

Finally, our proposed unseen-visible watermarking method requires only a combination of image enhancement operations composed by logarithmic and negative functions and has an exposure execution time of 0.007 s. Based on the obtained testing results, unseen-visible watermarking is clearly faster than invisible watermarking when the watermarked image was distorted by a geometric distortion. As shown in the experiments, there are two main advantages to unseen-visible watermarking method: first, it allows ownership claiming of digital images in a practical way, i.e., without a complex detection/extraction stage; second, the watermark imperceptibility is preserved.

4.4.2 Comparison with existing unseen-visible watermarking methods

Finally, a comparison performance in terms of the imperceptibility and robustness relative to that of the previously reported methods in [13, 19, 20, 23, 24, 27, 28] is show in Table 6. Table 6 presents the tolerance under distortions and designates the capacity to resist as either 'readable' or 'fail' when the tolerance is not given in detail by the other seven methods. A grid cell is marked with a dash, '-, 'for simulations not mentioned in the literature.

The comparison of the methods based on the gamma correction reveals that our proposed method outperforms the methods in [13, 19, 20] in terms of imperceptibility because our method obtains PSNR values <=68.13 dB. However, [13, 19, 20] obtained PSNR values under 50 dB. A serious drawback of the methods based on gamma correction is that both [13, 19, 20] require the existence of large smooth regions with dark hues within the host image, which is a prerequisite that constrains the practicality of the schemes. Our proposed method was tested using two datasets, the UCID dataset [33] and the RAISE-1k dataset [15], and the color images were of a variety of topics, including natural, outdoor, indoor, landscape, people, objects and building scenes. Moreover, the methods [13, 19, 20] show poor robustness against malicious removal attacks because simple image processing schemes, such as JPEG lossy, noise addition by Gaussian or impulsive noise, may destroy the watermark information [19].

The comparison with the method based on histogram modifications reveals that the method in [23] and our proposed method have a similar performance in terms of imperceptibility because both methods obtained PSNR values near 69 dB. The method in [23] and our proposed method have versatility in the media content because they can be applied to different images with different contents, and the embedding strategies are not limited to dark or flat areas with adequate sizes, which can constraint the practicality of the schemes. In terms of robustness, our method is outperformed by [23] in the tolerance against scaling, but our method outperforms the method in [23] against JPEG compression. The work in [23] only considers the JPEG2000 compression with a compression ratio from 10 to 100, and our method considers two JPEG compression modes. The first mode is JPEG2000 lossy with a

Table 6 Performance comparison	arison					
Comparison	Chuang et al. [13, 19]	Juarez-Sandoval et al. [20] Lin [23]	Lin [23]	Lin et al. [24]	Lin et al. [24] Pei et al. [27, 28] Proposed method	Proposed method
JPEG compression mode	1	JPEG lossy 50-100	JPEG2000 10-100	JPEG lossy 67–100	JPEG lossy 58–100	JPEG2000 lossy 1–100 JPEG lossy
Scaling	Ι	Until 0.5	Until 0.25	I	I	Until 0.5
Gaussian Noise	Fail	I	Readable	Fail	Fail	$\mu = 0, \sigma^2 = 0.001$
Impulsive noise	Fail	1	1	Fail	Fail	Density = 0.05
Versatility of media content Limited	Limited (dark, flat areas	Limited (dark, flat areas	Yes	Limited to	Limited to	Yes
Exposure procedure	with adequate size) Gamma correction	with adequate size) Gamma Correction	Histogram modification	depun map Adjustment the	depun map Adjustment the	Logarithmic and
				rendering conditions	rendering conditions	negative functions
Imperceptibility	PSNR <= 50.14 dB	PSNR<=50 dB	PSNR<=69 dB	I	PSNR<=63 dB	PSNR <= 68.13 dB
Artistic Filtering	1	1	1	1	I	Yes
Watermark size Image kind	From 32 × 32 until 128 × 128 2D color image and video	100×100 and 100×45 2D color image	From 64×64 until 256×256 2D color image	- 3D color image	3D color image	32 × 32 and 128x128 2D color image
»	b)	0))	»

compression ratio from 1 to 100, and the second one is the standard JPEG lossy with a quality factor from 10 to 100. In all cases, an adequate readability of the watermark pattern was obtained. Figure 25 shows the extreme tolerances with the assumption that the method reveals correctly the watermark for the rest of the tolerances. To conclude, in the comparison with [23], artistic filtering was not considered by the authors in [23], and the filtering is currently a common editing tool that should be included in the watermark robustness testing.

Finally, the comparison with the methods based on 3D images, [24, 27, 28], reveals that our proposed method is superior to them in terms of imperceptibility. For [24, 27, 28], the PSNR values are equals or less than to 63 dB, and our method obtains PSNR values near 69 dB. Against the JPEG lossy compression, the methods in [24, 27, 28] are weak and only obtain a tolerance near the quality factor 50, while our proposed method tolerates values from 10 to 100. The versatility of the media content in methods [24, 27, 28] is constrained to the use of a depth map of 3D images. The methods in this category show poor robustness against intentional attacks because simple common signal processing, such as noise corruption or image blurring, would remove the watermark information [28], while our proposed method shows robustness against several common signal processing distortions.

5 Conclusion

In this paper, we propose a novel camouflaged unseen-visible watermarking (CUVW) for use in color images for ownership authentication purposes. Our proposal preserves the strengths of the visible and invisible watermarking algorithms in terms of readability and imperceptibility, respectively. The proposed method maintains the "unseen" property of the visible watermark signal by hiding it in the spatial domain of the content image with a camouflage strategy based on the luminance and texture properties in conjunction with an image enhancement criterion. Also, our method improves the readability of the invisible watermarking modality and does not require the use of a complex detection stage to make the watermark pattern "visible." The pattern is rendered "visible" via two image enhancement processes that preserve the watermark exhibition ability against a practical scenario. The design of the proposed method allows small watermarks to be hidden in a camouflaged manner and preserves the visual quality of the watermarked images with average PSNR values between 58 dB and 68 dB, SSIM values close to 1 and NCD values close to 0. The experimental results show the robustness of the proposed method against a wide range of geometric attacks and common signal processing distortions, such as JPEG and JPEG2000 lossy modes, noise addition via Gaussian and impulsive noise, which severely affect the watermark readability of the unseenvisible watermarking schemes, and artistic filtering, and in all cases the watermark pattern was revealed. These last attacks and distortions were not previously considered in the literature [13, 19, 20, 23, 24, 27, 28]. Our proposed method was tested using two datasets, the UCID dataset [33] and RAISE-1k dataset [15], and the color images were classified by a variety of topics, including natural, outdoor, indoor, landscape, people, objects and building scenes.

Acknowledgments Authors thank the Instituto Politecnico Nacional (IPN) as well as the Consejo Nacional de Ciencia y Tecnologia de Mexico (CONACYT) by the support provided during the realization of this research.

References

- AL-Nabhani Y, Jalab HA, Wahid A, Md Noor R (2015) Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. J King Saud Univ Comput Inf Sci 27(4):393–401. https://doi.org/10.1016/j.jksuci.2015.02.002
- Barker C, Wiatrowski M (2017) The age of Netflix: critical essays on streaming media, digital delivery and instant access. McFarland, Incorporated Publishers, Jefferson
- Barni M, Bartolini F (2004) Applications. In: Watermarking systems engineering: enabling digital assets security and other applications. CRC Press, Boca Raton, pp 23–44
- 4. Barni M, Cox I, Kalker T, Kim HJ (2005) Digital watermarking. https://doi.org/10.1007/11551492
- Bas P, Furon T, Cayre F, Doërr G, Mathon B (2016) A quick tour of watermarking techniques. In: Watermarking Security Fundamentals, Secure Design and Attacks, SpringerBriefs in Electrical and Computer Engineering. Springer, Singapore, pp 13–31. doi:https://doi.org/10.1007/978-981-10-0506-0
- Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2014) Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification. SIViP 8(1):49–63. https://doi.org/10.1007/s11760-013-0459-9
- Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2015) Robust watermarking method in DFT domain for effective management of medical imaging. SIViP 9(5):1163–1178. https://doi. org/10.1007/s11760-013-0555-x
- Cedillo-Hernandez A, Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2016) A visible watermarking with automated location technique for copyright protection of portrait images. IEICE Trans Inf Syst E99.D(6):1541–1552. https://doi.org/10.1587/transinf.2015 EDP7412
- Cedillo-Hernandez M, Cedillo-Hernandez A, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2017) Digital color images ownership authentication via efficient and robust watermarking in a hybrid domain. Radioeng J 26(2):536–551. https://doi.org/10.13164/re.2017.0536
- Chang H, Chen HH (2007) Stochastic color interpolation for digital cameras. IEEE Trans Circ Syst Video Technol 17(8):964–973. https://doi.org/10.1109/TCSVT.2007.897471
- 11. Chareyron G, Da Rugna J, Trémeau A (2010) Color in image watermarking. In: Advanced techniques in multimedia watermarking: image, video and audio applications (Advances in Multimedia and Interactive Technologies), by Ali Mohammad Al-Haj, Information Science Reference; 1st edn. IGI Global, Hershey, pp 36–56
- Chrysochos E, Fotopoulos V, Xenos M, Skodras AN (2014) Hybrid watermarking based on chaos and histogram modification. SIViP 8(5):843–857. https://doi.org/10.1007/s11760-012-0307-3
- Chuang SC, Huang CH, Wu JL (2007) Unseen visible watermarking. IEEE international conference on image processing. San Antonio, Texas. pp 261–264. https://doi.org/10.1109/ICIP.2007.4379296
- Cox I, Miller M, Bloom J (2002) Applications and properties. In: Digital watermarking. The Morgan Kaufmann Series in Multimedia Information and Systems, 1st edn. Morgan Kaufmann Publishers, Burlington, pp 11–39
- Dang-Nguyen D-T, Pasquini C, Conotter V, Boato G (2015) RAISE a raw images dataset for digital image forensics. ACM Multimedia Systems, Portland, pp 219–224. https://doi.org/10.1145 /2713168.2713194
- Dong P, Brankov JG, Galatsanos NP, Yang Y, Davoine F (2005) Digital watermarking robust to geometric distortions. IEEE Trans Image Process 14(12):2140–2150. https://doi.org/10.1109 /TIP.2005.857263
- Garcia-Ugalde F, Cedillo-Hernandez M, Morales-Delgado E, Psenicka B (2012) Robust encoded spread spectrum image watermarking in contourlet domain. Signal Processing and Communication Systems (ICSPCS), 2012 6th International conference on, Gold Coast, QLD, Australia. https://doi.org/10.1109 /ICSPCS.2012.6508010
- Huang J, Shi YQ (1998) Adaptive image watermarking scheme based on visual masking. Electron Lett 34(8):748–750. https://doi.org/10.1049/el:19980545

- Huang CH, Chuang SC, Huang YL, Wu JL (2009) Unseen visible watermarking: a novel methodology for auxiliary information delivery via visual contents. IEEE Trans Inf For Secur 4(2):193–206. https://doi. org/10.1109/TIFS.2009.2020778
- Juarez-Sandoval O, Fragoso-Navarro E, Cedillo-Hernandez M, Nakano M, Perez-Meana H, Cedillo-Hernandez A (2017) Improved unseen-visible watermarking for copyright protection of digital image. 5th international workshop on biometrics and forensics, Coventry. pp 1–5. https://doi.org/10.1109 /IWBF.2017.7935084
- Langelaar GC, Setyawan I, Lagendijk RL (2000) Watermarking digital image and video data: a state-of-theart overview. IEEE Signal Process Mag 17(5):20–46. https://doi.org/10.1109/79.879337
- Lee ML, Ting PY, Wu TS (2016) Multimed Tools Appl 75:16173. https://doi.org/10.1007/s11042-015-2925-6
- Lin PY (2014) Imperceptible visible watermarking based on postcamera histogram operation. J Syst Softw 95:194–208. https://doi.org/10.1016/j.jss.2014.04.038
- Lin YH, Wu JL (2012) Unseen visible watermarking for color plus depth map 3D images. IEEE international conference on acoustics, speech and signal processing, Kyoto. pp 1801–1804. https://doi. org/10.1109/ICASSP.2012.6288250
- Mousavi SM, Naghsh A, Abu-Bakar SAR (2014) Watermarking techniques used in medical images: a survey. J Digit Imaging 27:714–729. https://doi.org/10.1007/s10278-014-9700-5
- Nematollahi MA, Vorakulpipat C, Rosales HG (2017) Image watermarking. In: Digital watermarking techniques and trends, (Springer Topics in Signal Processing). Springer, Singapore, pp 57–66. https://doi. org/10.1007/978-981-10-2095-7
- Pei SC, Wang YY (2014) A new 3D unseen visible watermarking and its applications to multimedia. IEEE 3rd global conference on consumer electronics, Tokyo, pp 140–143. https://doi.org/10.1109 /GCCE.2014.7031132
- Pei SC, Wang YY (2015) Auxiliary metadata delivery in view synthesis using depth no synthesis error model. IEEE Trans Multimed 17(1):128–133. https://doi.org/10.1109/TMM.2014.2368255
- Pei-Yu L, Yi-Hui C, Chin-Chen C, Jung-San L (2013) Contrast-Adaptive Removable Visible Watermarking (CARVW) mechanism. Image Vis Comput 31(4):311–321. https://doi.org/10.1016/j. imavis.2013.02.002
- Pham VQ, Miyaki T, Yamasaki T, Aizawa K (2008) Robust object-based watermarking using feature matching. IEICE Trans Inf Syst E91-D(7):2027–2034. https://doi.org/10.1093/ietisy/e91d.7.2027
- Sahoo A (2009) Fuzzy weighted adaptive linear filter for color image restoration using morphological detectors. Int J Comput Sci Eng 1(3):217–221 http://www.enggjournals.com/ijcse/doc/IJCSE09-01-03-18.pdf
- Santoyo-Garcia H, Fragoso-Navarro E, Reyes-Reyes R, Cruz-Ramos C, Nakano-Miyatake M (2017) Visible watermarking technique based on human visual system for single sensor digital cameras. Secur Commun Netw 2017(7903198):1–18. https://doi.org/10.1155/2017/7903198
- Schaefer G, Stich M (2004) UCID: an uncompressed color image database. Proc SPIE Int Soc Optical Eng 5307:472–480. https://doi.org/10.1117/12.525375
- Solachidis V, Pitas I (2001) Circularly symmetric watermark embedding in 2-D DFT domain. IEEE Trans Image Process 10(11):1741–1753. https://doi.org/10.1109/83.967401
- Tao H, Chongmin L, Zain JM, Abdalla AN (2014) Robust image watermarking theories and techniques: a review. J Appl Res Technol 12(1):122–138. https://doi.org/10.1016/S1665-6423(14)71612-8
- USC Viterbi School of Engineering (2017) USC-SIPI image database. http://sipi.usc.edu/database/database. php?volume=textures. Accessed 1 Aug 2017
- Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error measurement to structural similarity. IEEE Trans Image Process 13(4):600–612. https://doi.org/10.1109/TIP.2003.819861
- Xiaolin J, Yanli Q, Liping S, Xiaobo J (2011) An anti-geometric digital watermark algorithm based on histogram grouping and fault-tolerance channel. Intell Sci Intell Data Eng Lecture Notes Comput Sci 7202: 753–760. https://doi.org/10.1007/978-3-642-31919-8 96
- Yu T, Jing J (2008) New technology of infrared image contrast enhancement based on human visual properties. Infrared Laser Eng 6(37):951–954 http://en.cnki.com.cn/Article_en/CJFDTOTAL-HWYJ200806005.htm
- Yu P, Shang Y, Li C (2013) A new visible watermarking technique applied to CMOS image sensor. SPIE Proc 8917. https://doi.org/10.1117/12.2031136



Oswaldo Ulises Juarez-Sandoval was born in Mexico. He received the B.S. degree in Communication and Electronics Engineering, the M.S. degree in Microelectronics Engineering from the National Polytechnic Institute of Mexico (IPN) in the 2009 and 2013 respectively; He has experience in the satellital communication, IT management and security information; currently is student of the Communications and Electronic PhD program of the IPN were he is part time professor. His principal research interest is security information, image processing, hidden information, informatic forensic 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 National Polytechnic Institute of Mexico (IPN) in the years 2003, 2006 and 2011, respectively. He has 6 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.



Mariko Nakano-Miyatake was born in Japan. She received the M.E. degree in 1985, in Electrical Engineering from the University of Electro-Communications, Tokyo Japan, and the PhD degree 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.



Antonio Cedillo-Hernandez was born in Mexico. He received the B.S. degree in Computer Engineering, the M.S. degree in Microelectronic Engineering and his PhD in Communications and Electronic from the National Polytechnic Institute of Mexico in the years 2005, 2007 and 2013, respectively. He has about 7 years of professional practice in several strategic positions related to IT. Currently, he concluded a postdoctoral position at National Autonomous University of Mexico. His principal research interests are video and image processing, information security, watermarking and related fields



Hector Perez-Meana was born in Mexico. He received his M.S: Degree on Electrical Engineering from the Electro-Communications University of 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.