Hindawi
Security and Communication Networks
Volume 2017, Article ID 7903198, 18 pages
https://doi.org/10.1155/2017/7903198

Research Article

Visible Watermarking Technique Based on Human Visual System for Single Sensor Digital Cameras

Hector Santoyo-Garcia, Eduardo Fragoso-Navarro, Rogelio Reyes-Reyes, Clara Cruz-Ramos, and Mariko Nakano-Miyatake

Mechanical and Engineering School, Instituto Politecnico Nacional, Av. Santa Ana No. 1000, Col. San Francisco Culhuacan, Mexico City, Mexico

Correspondence should be addressed to Mariko Nakano-Miyatake; mnakano@ipn.mx

Received 5 August 2016; Accepted 15 December 2016; Published 12 January 2017

Academic Editor: Alessandro Cilardo

In this paper we propose a visible watermarking algorithm, in which a visible watermark is embedded into the Bayer Colour Filter Array (CFA) domain. The Bayer CFA is the most common raw image representation for images captured by single sensor digital cameras equipped in almost all mobile devices. In proposed scheme, the captured image is watermarked before it is compressed and stored in the storage system. Then this method enforces the rightful ownership of the watermarked image, since there is no other version of the image rather than the watermarked one. We also take into consideration the Human Visual System (HVS) so that the proposed technique provides desired characteristics of a visible watermarking scheme, such that the embedded watermark is sufficiently perceptible and at same time not obtrusive in colour and grey-scale images. Unlike other Bayer CFA domain visible watermarking algorithms, in which only binary watermark pattern is supported, proposed watermarking algorithm allows grey-scale and colour images as watermark patterns. It is suitable for advertisement purpose, such as digital library and e-commerce, besides copyright protection.

1. Introduction

Nowadays, a large amount of digital images in Internet has been captured by mobile devices, such as smartphones and tablets, owing to a great facility provided by these mobile devices to share and transmit digital images. However, since an adequate mechanism to protect rightful copyright of these images has not been established, copyright infringements become a serious problem. The digital watermarking technique has emerged as an alternative solution for this problem, embedding copyright information into the image in a visible or invisible manner.

Unlike invisible watermarking, visible watermarking consists in the overlaying of a logotype related to ownership into the original image in a perceptible manner, so visible watermarking can perform copyright protection in more direct and immediate manner than invisible watermarking. Generally, the embedded visible watermark may reduce the commercial value of the digital image, although it is translucent; therefore recently several removable visible watermarking techniques were proposed [1, 2]. However, there are many applications in which the permanent visible watermarking is more suitable. The digital library, e-commerce and digital press are the main applications of the permanent visible watermarking [3–5]. The digital library can offer users some digitalized documents, photograph, and arts with visible watermark pattern, and the users can read or look at them freely; however they cannot use these digital materials for other purpose, such as illegal sale, due to the visible watermark. In the case of e-commerce, an owner of some products, such as arts or professional photographs, can take pictures of his/her merchandise and put them on Internet for advertisement purpose. The images of merchandise can attract attention of possible customers; if these images contain translucent visible watermark, then an illegal use of these pictures can be avoided. In the case of the digital press, the protection of exclusive material is very important. A visible translucent

watermark indicates the originality of their materials and avoids its illegal use.

Concerning watermark robustness, the visible watermarking inherently provides robustness against a wide range of attacks, because the embedded visible watermark can be observed easily by the Human Visual System (HVS), although the watermarked image has received several attacks, such as geometrical attacks including scaling, rotation, transformation, and signal processing attacks consisting of compression, filtering, noise addition, and modification of brightness and contrast, among others [6, 7].

A visible watermarking algorithm should satisfy some requirements [8, 9], which are as follows:

(i) Embedded watermark should be perceptible in grey and colour host images.

(ii) Embedded watermark should be perceptible in any image regions with different characteristics: texture, plain, and edge.

(iii) Embedded watermark should not be too obtrusive, so details of host image may be perfectly recognizable.

(iv) Watermark embedding should not obscure or brighten considerably the host image, the watermarked area should be sufficiently perceptible by the HVS, and the degradation of nonwatermarked area is almost nullified.

(v) Embedded watermark should be robust against several common attacks.

(vi) Watermark embedding process should be automatic for all kinds of images.

In almost all watermarking algorithms, the watermark embedding is performed in a host image which is stored in a storage system, such as device memory, and after watermarked image is generated, the original unwatermarked host image remains in the storage system. Optionally the original image can be deleted by user. However, using some information forensic techniques, the deleted image can be recovered [10], so original unwatermarked image can coexist with its watermarked version. In [11], Craver et al. proved that the presence of an original unwatermarked image impedes performing rightful ownership protection in invisible watermarking case, and in the case of visible watermarking, the existing unwatermarked original image can be possessed by adversary, invalidating immediately the effect of visible watermark. Taking in account the situations related to an establishment of a rightful ownership, we consider that the watermark embedding process must operate before the storage of captured image, avoiding existence of unwatermarked host image.

Considering the above-mentioned visible watermarking requirements and rightful ownership protection issue, in this paper we propose a visible watermarking algorithm for mobile devices, in which the watermark embedding is performed at the right moment that a device's camera captures a picture, protecting the captured image before it is saved into the storage system. This implies that the watermark embedding is performed directly into the Colour Filter Array (CFA). Furthermore, for achieving the desired characteristics of a nonobtrusive visible watermark, the several characteristics of the HVS, related to luminance and spatial perception of the human eye, are considered in the embedding process. Sensibility of the HVS is higher in areas with medium luminance than in higher or lower luminance areas [12]; therefore proposed watermarking algorithm adjusts watermark energy using luminance information. In the plain and edge areas of the image, watermarking energy must be smaller to avoid watermark obtrusiveness, and textured areas, instead, must receive further treatment to enhance the visibility of the watermark. Proposed algorithm is compared with other Bayer CFA-based visible watermarking algorithms [13, 14] and numerical comparison results based on Mean Opinion Score (MOS) and Peak Signal to Noise Ratio (PSNR) show better performance of proposed algorithm satisfying all visible watermarking requirements mentioned above. It is worth noting that, in proposed visible watermarking scheme, the watermark pattern can be binary, grey-scale, and even a colour logotype, which is a desirable feature when the embedded watermark is used for also advertisement purpose besides copyright protection.

The rest of this paper is organized as follows. In Section 2, we briefly describe the process for a single sensor image capture in digital cameras and the required postprocessing to obtain a full colour picture. Section 3 presents current existing state of the art of visible watermarking and Section 4 describes the proposed method that performs watermarking in the Bayer CFA domain, considering the HVS for adaptive watermarking. Section 5 shows the experimental results obtained by the proposed method, comparing it with previously proposed Bayer CFA-based visible watermarking algorithms [13, 14]. Finally, conclusions are done in Section 6.

2. Single Sensor Camera Image Acquisition

A full colour image can be represented in three colour channels: red, green, and blue, which is known as the RGB colour model. A professional camera has three sensors, which allow fully capturing of the three RGB colour channels by using a different colour filter in each sensor to transform light into digital data. However, nonprofessional digital cameras, such as cameras equipped in mobile devices, use a single sensor to capture images in order to reduce the space occupied by the sensors of the cameras (Figure 1(a)). This single sensor has individual pixel colour filters which are arranged into a matrix known as the Colour Filter Array (CFA), being the Bayer CFA the most utilized CFA [15, 16], where only one of the three colour channels is stored per pixel as shown in Figure 1(b). Together with the CFA data, some metadata are generated in the capture process. All this data constitutes the so-called raw image or digital negative, referencing to a nonprocessed image representation obtained directly from the camera sensor.

Figure 1(c) shows an example of the CFA data, which seems a grey-scale image; however the value of each pixel presents one of three colour values, generating mosaic image (Figure 1(e)). To recover the original colour in each pixel of the CFA data, we need to estimate the values of other

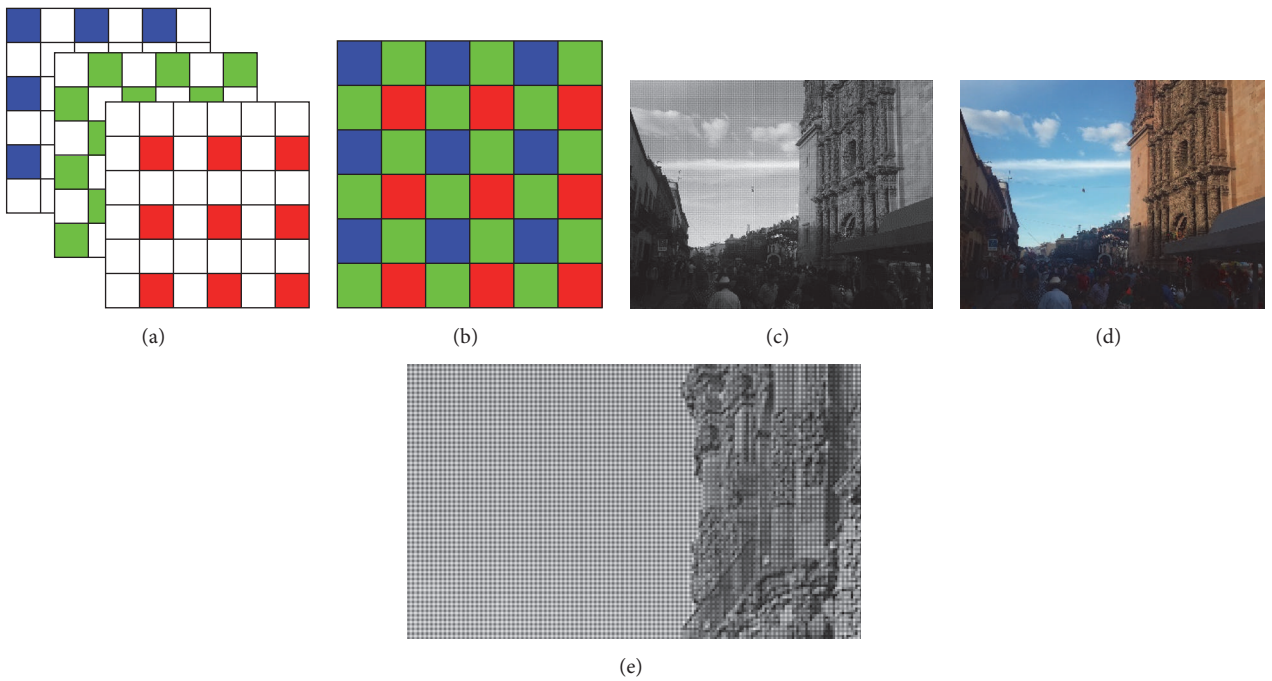


Figure 1: Single sensor image acquisition. (a) Image capture by single sensor of three filters, (b) Bayer CFA, (c) an example of CFA data, (d) recovered colour image after demosaicing operation, and (e) zoom in of the CFA data.

two missing colours. For example, a first pixel (top-left) of Figure 1(c) has only blue information as shown in Figure 1(b) and to obtain original colour of this pixel, two missing colour values (red and green) must be estimated. This estimation process is known as demosaicing or demosaicking, and many demosaicing algorithms are reported in the literature [15, 16]. The simplest one is based on the linear interpolation of the same colour of the neighbour pixels and more sophisticated algorithms try to reduce the interpolation artefacts, improving the quality of resulting colour image [15, 16]. Figure 1(d) shows colour image recovered from its CFA data given by Figure 1(c).

3. Visible Watermarking

Visible watermarking consists mainly in the embedding of a text or logotype as a seal that serves to validate directly the intellectual property of the image, so that the information related to copyright can be easily perceived by the bare eye. However, inevitably a visible watermark will cause a certain distortion to the host image [17–19].

There are currently many approaches that have developed visible watermarking algorithms [6]; however only few of them contemplate the use of the Human Visual System (HVS) model to perform this process. Using the HVS model it is possible to achieve the embedding of a less obtrusive visible watermark, while keeping its sufficient visibility. The HVS model indicates the sensibility of the human eye to regions of images with different luminance and frequency, which may allow an efficient design of visible watermarking schemes [17]. Kankanhalli et al. in [9] proposed the use of scaling and embedding factors, α and β, which are computed using the HVS model. Each pixel of the watermarked image is determined as weighted linear combination between the host pixel value weighted by the scaling factor α and the watermark pixel value weighted by the embedding factor β. This visible watermarking formula is given by

$$C'_{ij} = \alpha_{ij} C_{ij} + \beta_{ij} W_{ij}, \quad 1 \le i \le M;\ 1 \le j \le N, \tag{1}$$

where C_{ij} and W_{ij} represent a pixel value located at the (i, j) position of a host image C and a watermark image W, respectively, C'_{ij} is the (i, j)th pixel value of the watermarked image, and $M \times N$ is the size of the host and watermark images. This operation is performed in Discrete Cosine Transform (DCT) domain computing scaling factor α and embedding factor β based on the DC and the AC coefficients [9].

Mohanty et al. also presented a visible watermarking algorithm in the DCT domain by applying the equation (1) to each 8×8 DCT block [19]. The scaling and embedding factors α and β are determined from the average luminance and variance value of each DCT block. This algorithm provides a better performance compared with [9]. Hu and Kwong also proposed the use of scaling and embedding factors determined by the luminance masking in the Discrete Wavelet Transform (DWT) [20]. Huang and Tang used the Contrast-Sensitive Function (CSF) based on the HVS to vary the intensity of the watermark in different regions of image by generating a CSF mask in the Discrete Wavelet Transform (DWT) and the DWT blocks of both the image and the watermark are classified using their entropy [21]. Another approach that utilizes the CSF is proposed by Tsai et al., which

is based on the Content and Contrast Aware (COCOA) watermarking algorithm [22] and visible watermark embedding is performed in the multilevel decomposition of the DWT. In these algorithms, the watermark pattern can be grey-scale and colour images.

Nevertheless, these algorithms operate in some time-consuming transform domains, such as DCT [9, 19] and DWT [20–22]. Although the advance of mobile device technology is considerably fast, the processing power and memory capacity of mobile devices are still limited compared with conventional computers. So implementation of frequency domain algorithms [9, 19–22] in any mobile devices is still not practical. Additionally, according to Craver's demonstration [11], a rightful ownership cannot be established correctly in these schemes [9, 19–22], because these algorithms embed visible watermark into an image stored in storage system, and although the original unwatermarked image has been deleted from the memory after watermarking process, it can be recovered using some forensic techniques [10].

In the CFA domain visible watermarking, the watermark is embedded directly into the Bayer CFA domain and the watermarked Bayer CFA is transferred to a watermarked image using demosaicing operation before its storage in device memory. In this process, visible watermarking must not perform any time-consuming frequency transform, keeping the consuming time for watermarking minimum to hold an adequate usability of mobile devices. Considering the above, the CFA domain watermarking can be considered as the most adequate scheme to establish rightful ownership over the images captured by mobile devices.

Until now a few CFA domain visible watermarking schemes are proposed [13, 14]. Lukac et al. proposed a scheme where an embedding factor β, given by (1), is assigned to each image pixel which coincides with a pixel of a binary watermark [13]. In this scheme, the embedding factor β is a user-setting constant value without consideration of any characteristics of the HVS [13]. Yu et al. added a lineal piecewise function that modifies the embedding factor β by taking into account the perceptibility of human eyes to certain luminosity [14]. In this scheme, since the texture feature is not considered to determine watermark embedding strength, an embedded watermark pattern in the texture area provides very low perceptibility, failing the second requirement of visible watermarking. It is worth noting that in both algorithms [13, 14] the scaling factor α in (1) is constant value 1, which means that the watermarking formula given by (1) becomes $C'_{ij} = C_{ij} + \beta_{ij} W_{ij}$.

4. Proposed Method

Proposed visible watermarking scheme performs directly in the Bayer CFA domain to protect images captured by mobile devices, such as smartphones and tablets. In the proposed scheme, since the watermarking is carried out before the captured image is stored in the storage system; any unwatermarked original image does not exist, establishing a rightful ownership over the image as indicated by [11].

To satisfy the conflicting requirements of the visible watermarking mentioned above [8, 9], in which a watermark should not be too obtrusive and at same time it must be sufficiently visible in any area of the image, the characteristics of the HVS must be explored. In visible watermarking, the sensibility of the HVS to luminance is analysed, and relatively higher sensibility of the HVS in middle luminance range compared with other ranges is taken into consideration to moderate the watermark embedding strength [9]. Also we take advantage of the low sensibility of the HVS for detecting changes in textured areas to embed a stronger watermark pattern [9, 19]. In the proposed scheme, we compute edge densities to classify the input Bayer CFA into plain, textured, and edge areas to obtain an adequate watermarking strength for each area. Also luminance information of each area is considered to adjust the watermark embedding strength.

In proposed algorithm, we use the generic visible watermarking algorithm given by (1), in which the scaling factor α_{ij} and embedding factor β_{ij} of the (i, j)th pixel are determined using the edge density and the luminance information of host image. The sensibility of the HVS related to luminance mentioned above can be expressed by the exponential function $f(x) = \exp(-(x - \mu')^2)$ which provides adequate values of embedding energy respect to luminance value x, where μ' is the middle luminance value of the host image.

The block diagram of proposed scheme is shown by Figure 2. Firstly, each pixel $C(i, j)$ of the Bayer CFA C captured by mobile device is classified into plain, edge, and texture according to the relationship between the pixel $C(i, j)$ and its neighbourhood of size $K \times K$ pixels. The Bayer CFA is represented as a mosaic structure as shown by Figure 1(e), which presents fine texture feature in all regions; therefore, to avoid detecting erroneously the whole Bayer CFA as texture area, we selected the Canny operator proposed by [23] as an edge detector. In the Canny operator, first a Gaussian filter is applied to the Bayer CFA, smoothing the Bayer CFA and reducing the mosaic effect to allow a proper detection of edge and texture areas.

Once binary edge map of the Bayer CFA is obtained by the Canny operator, we obtain the edge density of each pixel $C(i, j)$, which is calculated by

$$\rho_{i,j} = \frac{1}{K^2} \sum_{\substack{i-\lfloor K/2 \rfloor \le p \le i+\lfloor K/2 \rfloor \\ j-\lfloor K/2 \rfloor \le q \le j+\lfloor K/2 \rfloor}} \text{edge}(p, q), \tag{2}$$

where $\rho_{i,j}$ is the edge density of $C(i, j)$ in the Bayer CFA C and $\text{edge}(p, q)$ is the binary value in edge map in neighbour pixel $C(p, q)$ obtained by the Canny operator, K is the width and height of the neighbourhood, and $\lfloor \cdot \rfloor$ is the round toward zero operator. Then, according to the value of the edge density $\rho_{i,j}$ obtained by (2), the type of each element of the Bayer CFA is determined as plain, edge, and texture by

$$\text{Pixel Type} = \begin{cases} \text{Plain} & \rho_{i,j} \le 0.1 \\ \text{Edge} & 0.1 \le \rho_{i,j} \le 0.2 \\ \text{Texture} & 0.2 < \rho_{i,j}. \end{cases} \tag{3}$$

In a plain area, no edge is found, so the edge density $\rho_{i,j}$ in the plain area must be small, while in a textured area, many

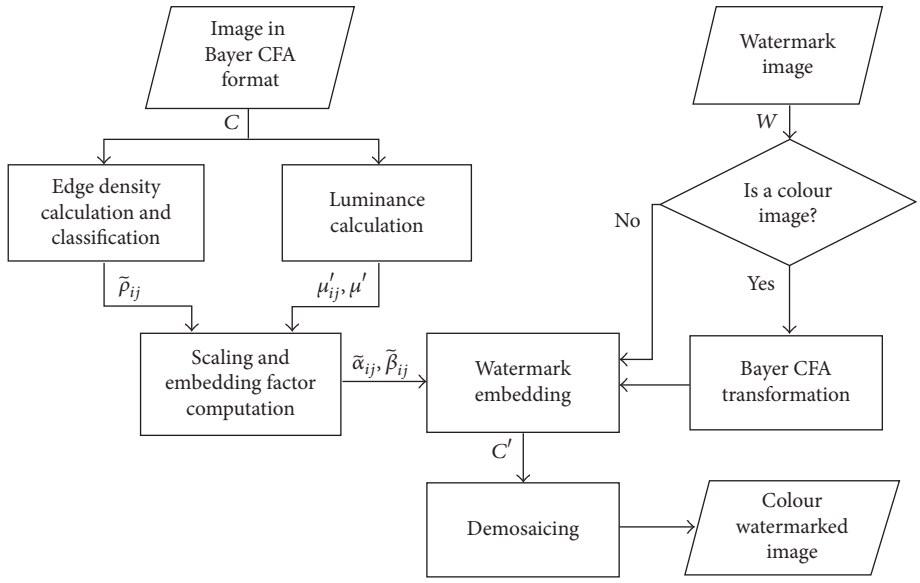


Figure 2: Block diagram of proposed scheme.

edges appear, which makes the edge density large. In the case of edge area, a few determined edge lines appear, taking an intermediate value of edge density. The threshold values, 0.1 and 0.2, used to determine pixel type of Bayer CFA are empirically obtained according to [24].

An example of the pixel classification mentioned above is shown in Figure 3. Figure 3(a) shows Bayer CFA captured by mobile device, Figure 3(c) shows result of pixel classification, in which black, white, and grey pixels represent plain, edge, and texture areas, respectively, and Figures 3(b) and 3(d) are zoomed parts of Figures 3(a) and 3(c), respectively. From these figures, we can observe that the mosaic effect of the Bayer CFA has disappeared correctly by the smoothing Gaussian filter used as preprocessing of the Canny operator, and the pixels are classified correctly into plain, edge, and texture.

The HVS is less sensible to the textured area; therefore, the watermark embedding energy must be large for this area to obtain watermark visibility, while in the plain area where any change of pixel value is noticeable by the HVS, the watermark must be embedded in minimum energy. Also in the edge area, where the host image provides important visual information, the embedding energy is also minimized. The edge density $\rho_{i,j}$ of Bayer CFA obtained by (2) indicates the level of texture of each pixel and using this value, we calculate $\tilde{\rho}_{i,j} \in [0, 1]$ taking into account above consideration related to the sensibility of the HVS.

$$\tilde{\rho}_{i,j} = \begin{cases} 0 & \text{Plain and Edge pixels} \\ \dfrac{\left(\rho_{i,j} - 0.2\right)}{0.8} & \text{Texture pixels.} \end{cases} \tag{4}$$

In the Bayer CFA, the intensities of three basic colours (R, G, and B) are interposed among them generating a mosaic pattern as shown by Figure 1(e), so the Bayer CFA keeps the luminance variation of its input image. Considering this, we can obtain the luminance value of each pixel, which is a mean intensity value of its neighbourhood of size $K \times K$ as given by

$$\mu_{ij} = \frac{1}{K^2} \sum_{\substack{i-\lfloor K/2 \rfloor \le p \le i+\lfloor K/2 \rfloor \\ j-\lfloor K/2 \rfloor \le q \le j+\lfloor K/2 \rfloor}} C(p, q), \tag{5}$$

where μ_{ij} is the luminance value of the (i, j)th pixel and $C(p, q)$ is the intensity of the (p, q)th pixel of the Bayer CFA. The luminance value μ_{ij} is normalized using (6), dividing it by the dynamic range 2^b, where b is number of bits of each pixel and $b = 8$ is the typical value in almost all cameras in mobile devices.

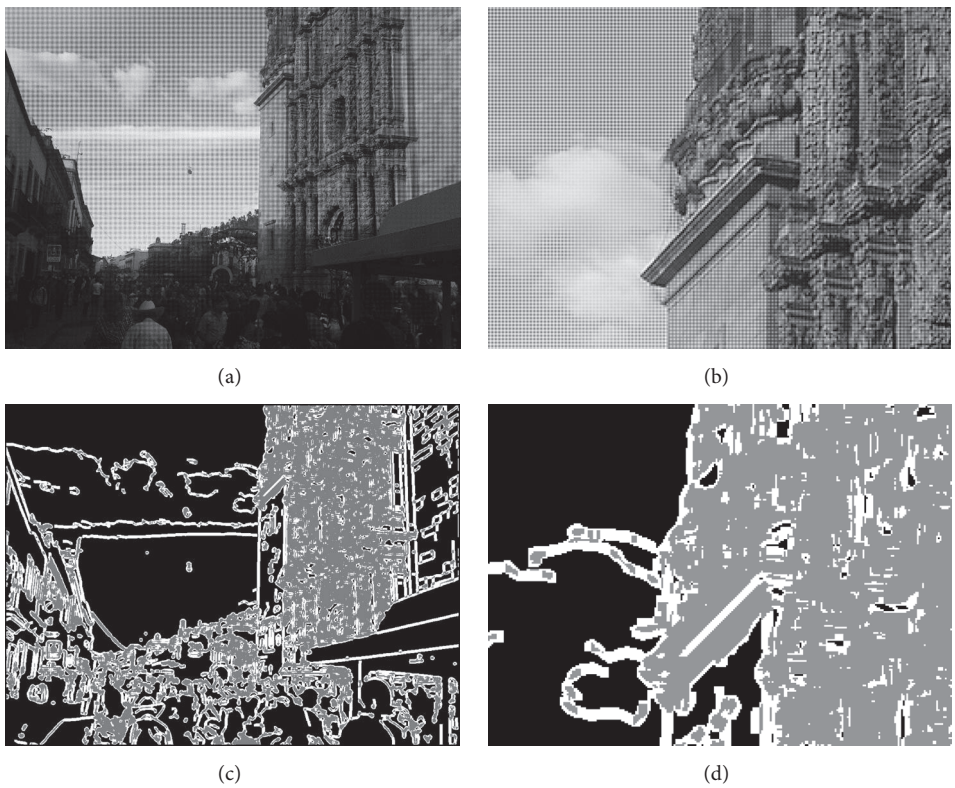
$$\mu'_{ij} = \frac{\mu_{ij}}{2^b}. \tag{6}$$

The normalized mean value is calculated by

$$\mu' = \left(\frac{1}{NM}\right) \sum \mu'_{ij}, \tag{7}$$

where N and M are dimensions of the Bayer CFA.

In the generic visible watermarking formula given by (1), the scaling factor α_{ij} determines the contribution of (i, j)th host pixel, while the embedding factor β_{ij} determines the contribution of (i, j)th watermark pixel. To satisfy the conflictive requirements of the visible watermarking mentioned above, for the image area where the sensibility of the HVS is high, in other words plain or edge area with middle luminance, a large scaling factor α_{ij} and a small embedding factor β_{ij} are required. In the meanwhile for the image area where the sensibility of the HVS is low, in other words textured area with lower or higher luminance, small α_{ij} and large β_{ij} are required. Considering that the exponential function $f(x) = \exp(-(x - \mu')^2)$ mentioned before can be considered as an expression of the HVS sensibility to the



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

Figure 3: An example of pixel classification. (a) Bayer CFA data, (b) zoomed part of (a), (c) pixel classification result, and (d) zoomed part of (c).

luminance, we formulate both the scaling factor α_{ij} and the embedding factor β_{ij} as

$$\alpha_{ij} = \left(1 - \widetilde{\rho}_{ij}\right) \exp\left(-\left(\mu'_{ij} - \mu'\right)^2\right), \tag{8}$$

$$\beta_{ij} = \widetilde{\rho}_{ij} \left(1 - \exp\left(-\left(\mu'_{ij} - \mu'\right)^2\right)\right). \tag{9}$$

It is worth noting that (9) is the inverse form of (8), which indicates that the contribution of the host image given by α_{ij} is large in the area where the HVS has high sensibility, and the contribution of watermark given by β_{ij} is small. Figure 4 shows the behaviours of the scaling and the embedding factors α_{ij} and β_{ij}, varying luminance μ'_{ij}, and edge density $\widetilde{\rho}_{ij}$ of each pixel of the Bayer CFA. From this figure, we can observe the visible watermarking energy in different luminance and spatial characteristics.

Once α_{ij} and β_{ij} are obtained, these values are scaled within the ranges $[\alpha_{\min}, \alpha_{\max}]$ and $[\beta_{\min}, \beta_{\max}]$. The typical values are $[0.95, 0.99]$ and $[0.01, 0.15]$, respectively, which are empirically determined [9]. Using both scaled factors, $\widetilde{\alpha}_{ij}$ and $\widetilde{\beta}_{ij}$, the visible watermarked Bayer CFA image is generated by (1). In the proposed scheme, the watermark pattern can be binary, grey-scale, and also colour image. When the watermark is a colour image, the CFA domain transform must be applied to the colour watermark image to convert it into the Bayer CFA before its embedding. Once the watermarked Bayer CFA image is generated, the demosaicing operation is applied to the watermarked Bayer CFA image to generate watermarked colour image.

5. Experimental Results

The proposed visible watermarking algorithm has been implemented and evaluated by using colour images captured by different mobile devices available nowadays and some images generated artificially. Both types of images present texture, plain, edge areas and luminance variation. Figure 5 shows some examples of colour images (Figures 5(a)–5(d)) and some monochrome, grey-scale, and full colour watermark patterns (Figures 5(e)–5(h)).

5.1. Watermark Visibility and Unobtrusiveness. The proposed algorithm is evaluated from watermark visibility and unobtrusiveness points of view, which are two conflictive requirements for visible watermarking. The performance of proposed scheme is compared with Bayer CFA-based visible watermarking algorithms proposed by [13, 14]. For comparison purposes, some artificially generated host images shown by Figures 5(a) and 5(b), which present texture and plain areas, and a binary watermark given by Figures 5(e) and 5(f) are used, because in the schemes of [13, 14], only binary watermark can be embedded. The neighbourhood size K used in (2) and (5) depends on the size of the host image. Empirically, the best classification results were given by setting $K = 15$ for host images with 1024×768 dimensions.

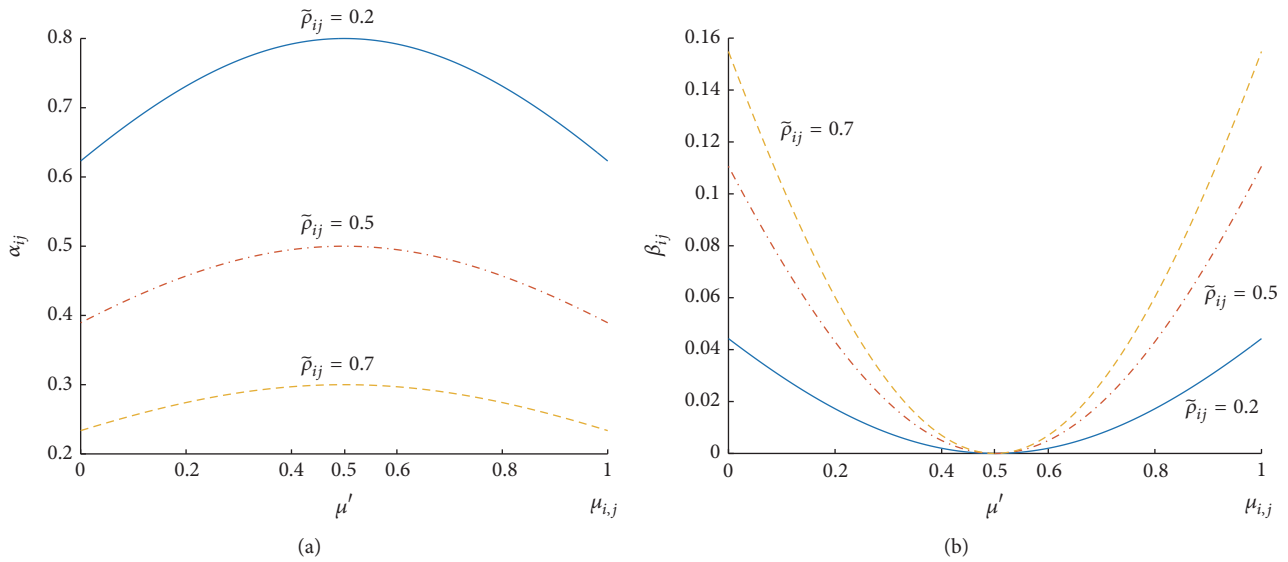


FIGURE 4: Behaviours of the scaling and embedding factors with different luminance and edge density. (a) Behaviour of the scaling factor α_{ij} with different luminance $\mu_{i,j}$ and edge density $\widetilde{\rho}_{ij}$, (b) behavior of the embedding factor β_{ij} with different luminance $\mu_{i,j}$, and edge density $\widetilde{\rho}_{ij}$.

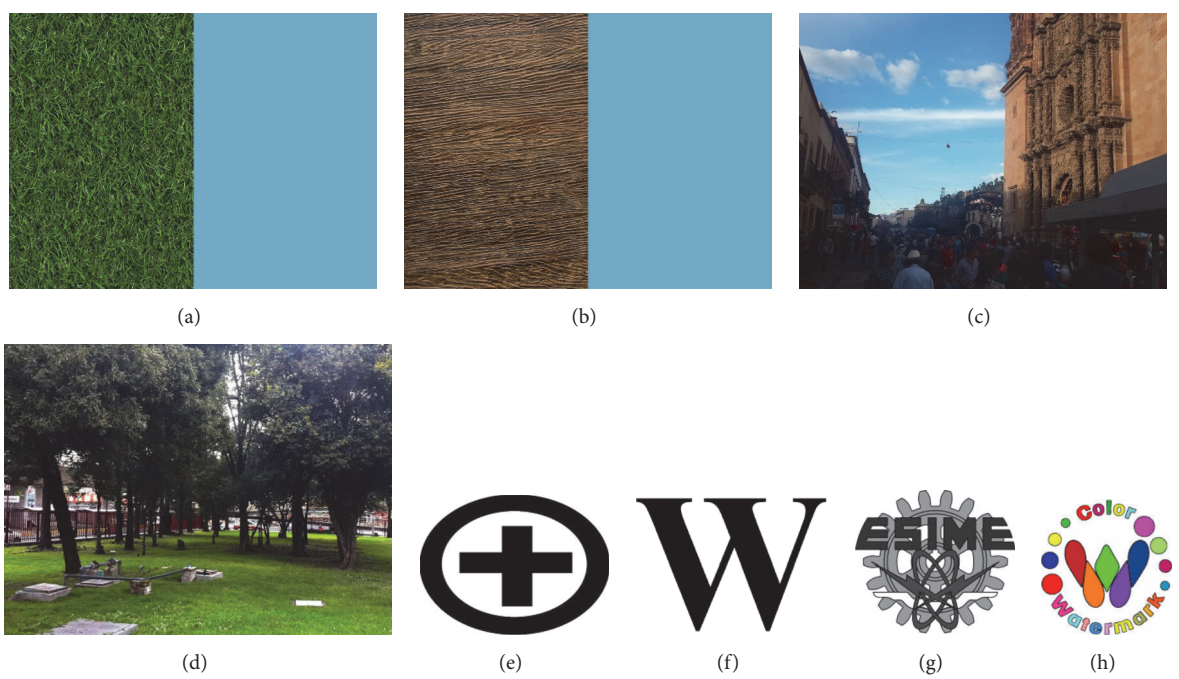
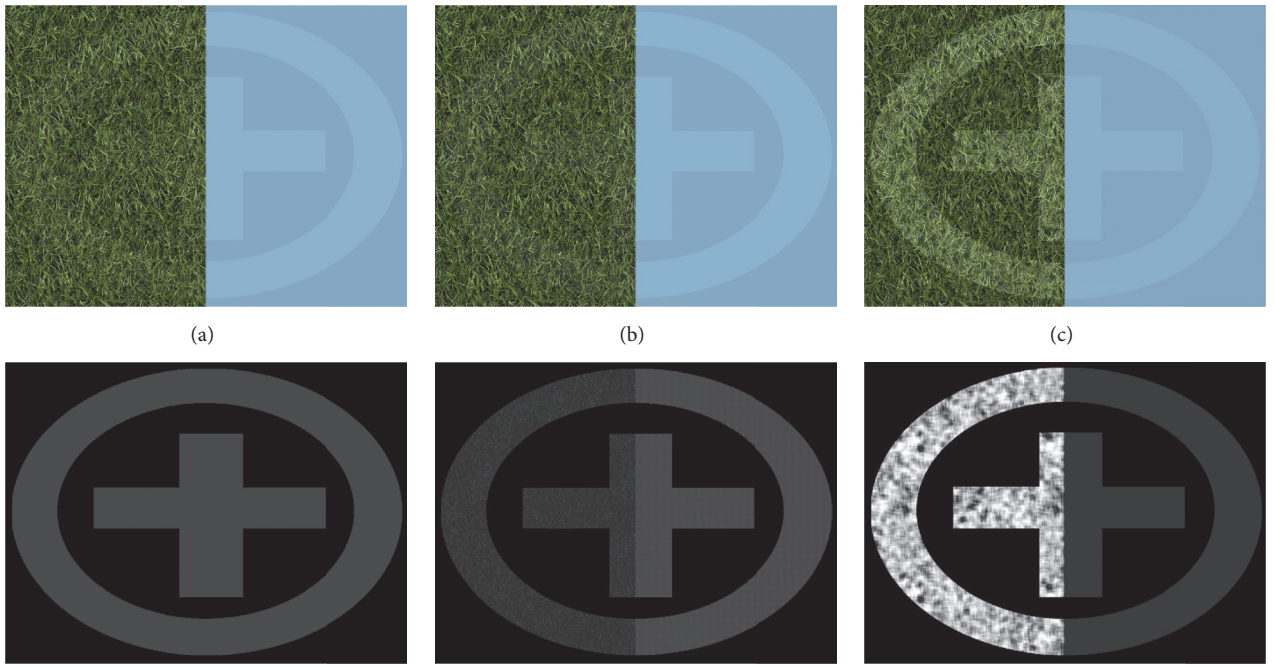


FIGURE 5: Host images and watermark patterns used in the evaluation. ((a)–(d)) Colour host images, (e), (f) binary watermark patterns, (g) grey-scale watermark pattern, and (h) colour watermark pattern.

The comparison results are shown in Figures 6 and 7, in which (a), (b), and (c) show the watermarked images generated by schemes of [13, 14] and the proposed one, and the corresponding watermark strengths of each watermarking scheme are shown by (d), (e), and (f), respectively. From these two figures, we can observe that the proposed scheme provides the watermark visibility in the texture area, allowing clear observation of the watermark pattern, while watermark strength in plain area is smaller than that provided by other two methods [13, 14] to avoid watermark obtrusiveness.

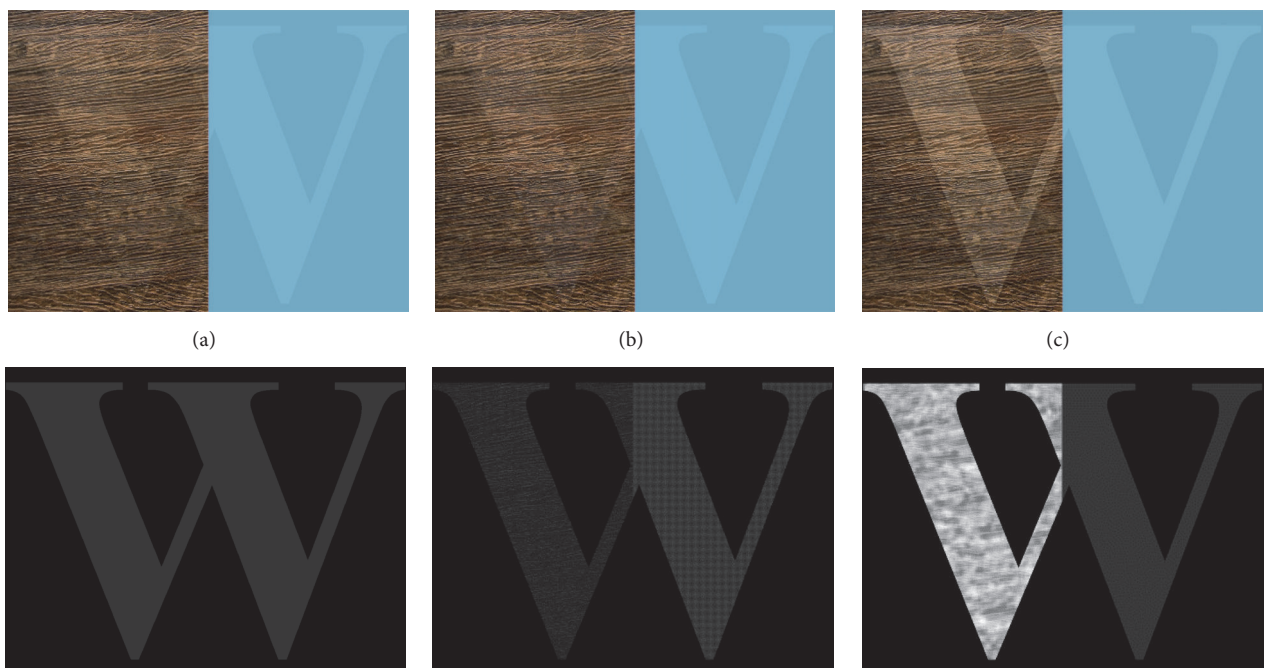
Figures 8 and 9 show the watermarked images generated by schemes proposed by [13, 14] and the proposed scheme, in which images are natural images captured by smartphone. It is worth noting that these images present large variation of luminance and spatial characteristics. Again in Figures 8 and 9, (a), (b), and (c) show the watermarked images generated by schemes of [13, 14] and the proposed one, and the corresponding watermark strengths of each watermarking scheme are shown by (d), (e), and (f), respectively. From these figures, we can observe that the proposed scheme



(a) (b) (c)

(d) (e) (f)

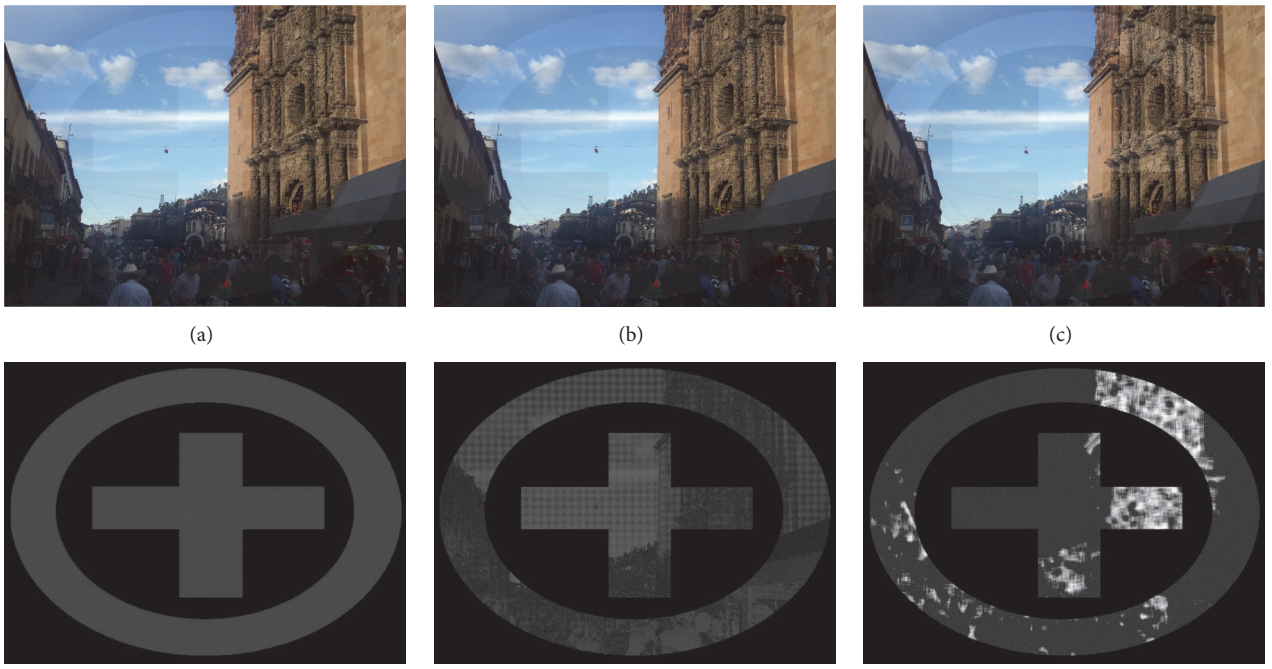
Figure 6: Comparison results using artificial colour image (Figure 5(a)). (a) Watermarked image by the scheme [13]. (b) Watermarked image by the scheme [14]. (c) Watermarked image generated by the proposed scheme. ((d), (e), and (f)) Watermark embedding strengths by the three schemes, respectively.



(a) (b) (c)

(d) (e) (f)

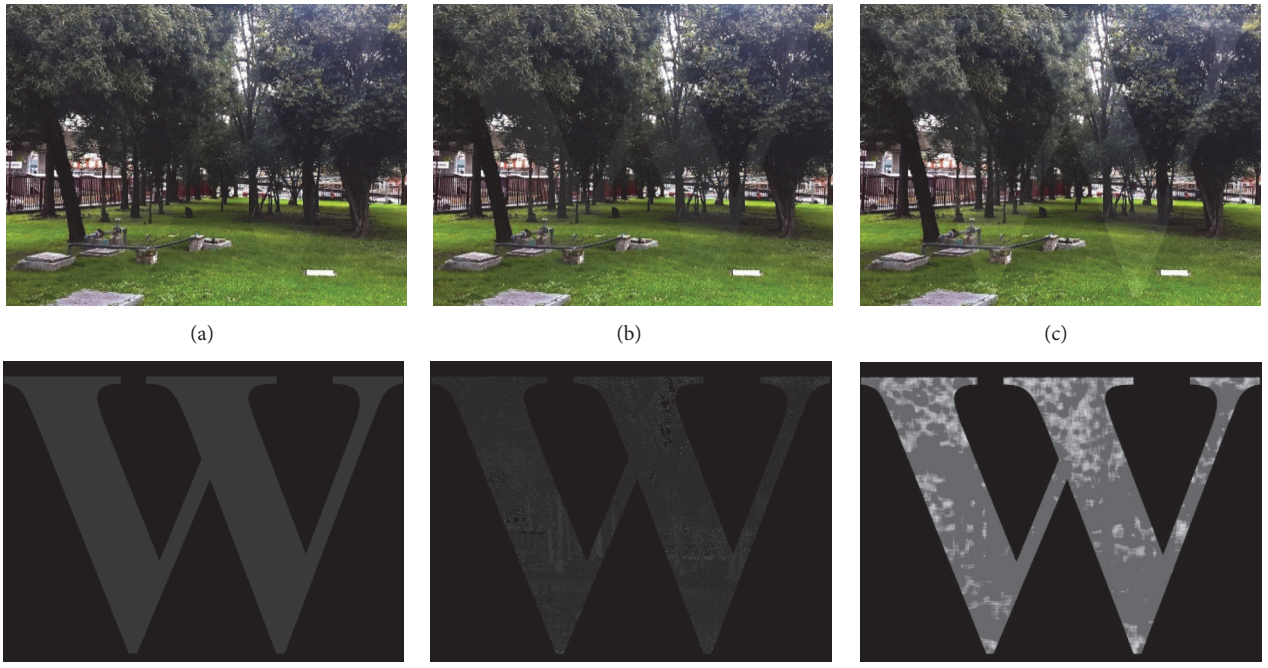
Figure 7: Comparison results using artificial colour image (Figure 5(b)). (a) Watermarked image by the scheme [13]. (b) Watermarked image by the scheme [14]. (c) Watermarked image generated by the proposed scheme. ((d), (e), and (f)) Watermark embedding strengths by the three schemes, respectively.



(a) (b) (c)

(d) (e) (f)

Figure 8: Comparison results using natural colour image (Figure 5(c)). (a) Watermarked image by the scheme [13]. (b) Watermarked image by the scheme [14]. (c) Watermarked image generated by the proposed scheme. ((d), (e), and (f)) Watermark embedding strengths by the three schemes, respectively.



(a) (b) (c)

(d) (e) (f)

Figure 9: Comparison results using natural colour image (Figure 5(d)). (a) Watermarked image by the scheme [13]. (b) Watermarked image by the scheme [14]. (c) Watermarked image generated by the proposed scheme. ((d), (e), and (f)) Watermark embedding strengths by the three schemes, respectively.

Table 1: Watermark visibility evaluation.

MOS	Description
5	Excellent. No effort required to recognize completely the watermark pattern
4	Good. No appreciable effort required to recognize completely the watermark pattern
3	Fair. Moderate effort required to recognize completely the watermark pattern (small part of watermark is not visible)
2	Poor. Considerable effort require to recognize completely the watermark pattern (some part of the watermark is not perceptible)
1	Unacceptable. The watermark is not perceptible

Table 2: Watermark unobtrusiveness evaluation.

MOS	Description
5	Excellent. High quality image. The detail of host image can be observed completely
4	Good. Visual degradation is minimum. The detail of host image can be observed with minimum effort
3	Fair. Visual degradation is acceptable. Some area of host image can be observed with some effort
2	Poor. Visual degradation is high. Some areas of host image are not observed due to obtrusive watermark
1	Unacceptable. Visual degradation is unacceptable. Major part of the host image is not observed due to very obtrusive watermark

provides a larger watermark embedding strength in texture area and a smaller embedding strength in plain area, allowing watermark visibility and unobtrusiveness at same time.

In the visible watermarking, any objective assessment for watermark visibility and unobtrusiveness is not established, because both issues are directly related to the HVS which is totally subjective, and then the assessment of these performances is carried out using the subjective measure based on Mean Score Opinion (MOS). The MOS evaluation is applied to 80 persons with different ages, genders, and occupations. Tables 1 and 2 show the evaluation criteria applied to evaluate watermark visibility and watermark unobtrusiveness, respectively. Table 3 shows the MOS-based comparison results related to the watermark visibility and unobtrusiveness among the proposed scheme and two previous schemes [13, 14]. The MOS data of the table are average values of 80 observers' scores using two artificial images shown by Figures 5(a) and 5(b) with two watermark patterns and two natural images shown by Figures 5(c) and 5(d) with two watermark patterns. From this table, we can observe that the proposed algorithm provides a better performance than two algorithms [13, 14] from both watermark visibility and unobtrusiveness points of view. In proposed algorithm, we can get visibility MOS values 4.59 and 4.13 for artificial and natural images, respectively, which are more than "good" score, while the watermark unobtrusiveness scores are 4.39 and 4.10 for both images, which are also more than "good" score.

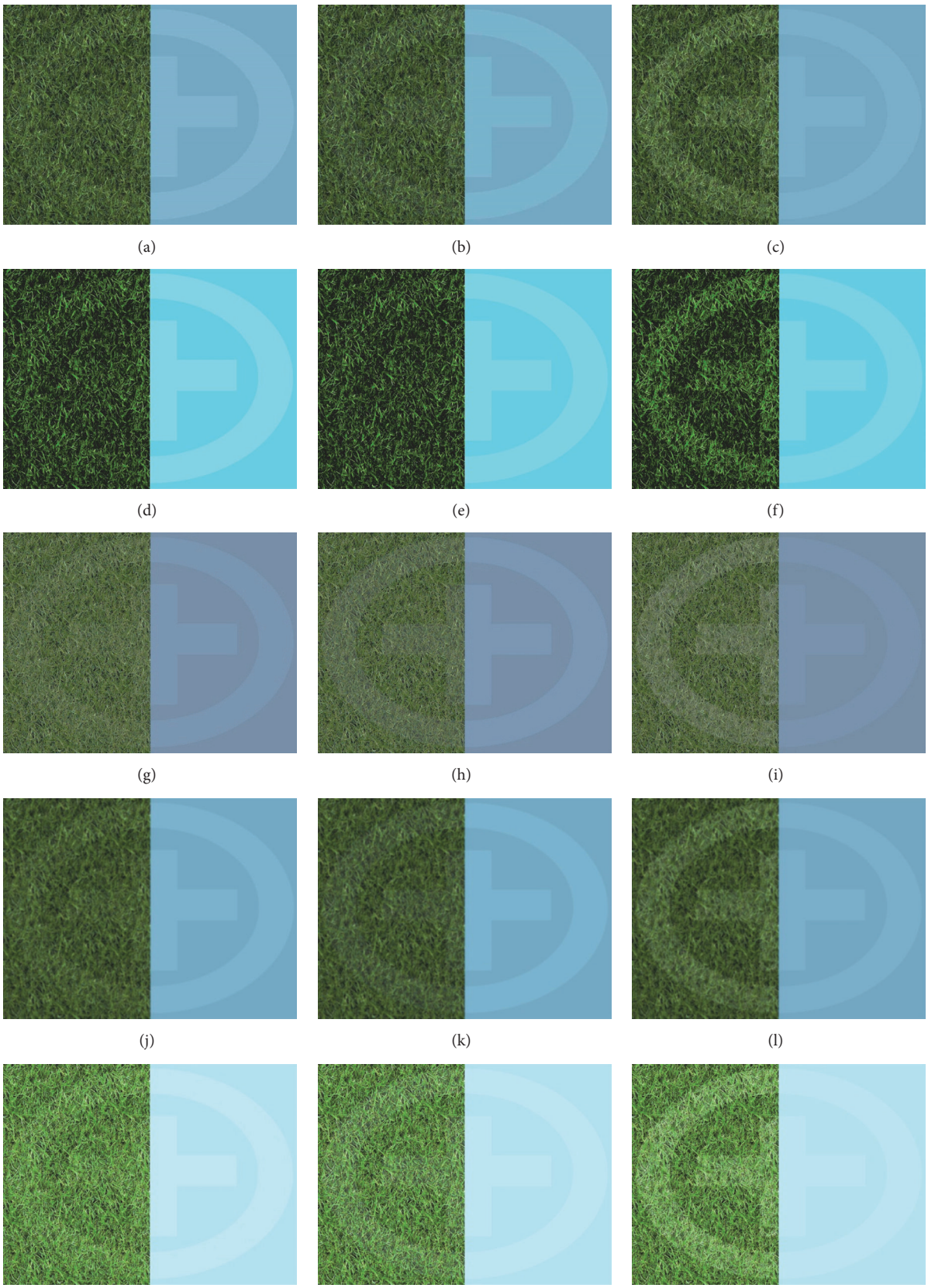
Although any objective assessment for the visibility and unobtrusiveness of the embedded visible watermark is not established, we try to assess the watermark visibility computing the PSNR between the translucent visible watermarked images and the opaque watermark superimposed image. Table 4 shows the watermark visibility comparison among two previously proposed algorithms [13, 14] and proposed one. In this experiment, we used two natural images given by Figures 5(c) and 5(d).

Considering that the watermark unobtrusiveness indicates that the details of the host image are clearly observable through a sufficiently translucent watermark pattern, we consider that this assessment is highly related to the HVS; therefore any objective assessment cannot be pertinent.

5.2. Watermark Robustness. In the visible watermarking, the watermark visibility and unobtrusiveness must be maintained after several common attacks to the watermarked image, such as JPEG compression, contrast change, luminance change, blurring, and Gaussian noise contamination. Tables 5 and 6 show the MOS values for proposed algorithm and two previous algorithms [13, 14] under several attacks, using artificial images given by Figures 5(a) and 5(b) and natural images given by Figures 5(c) and 5(d), respectively. The attacks were carried out using Adobe Photoshop CC 2015; the parameters used for each attack are noted in the tables. All MOS values in the tables are average of scores for two images marked by 80 observers. Figure 10 shows watermarked artificial images generated by [13, 14] and proposed algorithm, which suffered several attacks mentioned above, while Figure 11 shows watermarked and attacked natural images generated by [13, 14] and proposed algorithm. In both figures, the images in first, second, and third column correspond to watermarked images generated by [13, 14] and proposed one, respectively. From the tables and figures, we can conclude that proposed algorithm performs better under all attacks applied to the watermarked image. All images used for the evaluation are available in http://hectorsantoyo.com.mx/research/mos/images_pack.zip.

It is worth noting that the MOS evaluation of robustness to geometrical attacks was not carried out, because geometrical attacks do not cause any change of pixel values and the embedded visible watermark can be recognized perfectly by the HVS.

5.3. Watermarking with Grey-Scale and Colour Watermark Pattern. As mentioned before, in the proposed visible watermarking scheme, we can embed also grey-scale and colour watermark patterns into the input colour image. If the watermark image is a colour one, it is firstly transformed in Bayer CFA format before its embedding, as shown in Figure 2. Figures 12–14 show watermarked images generated by the proposed scheme using grey-scale and colour watermark patterns given by Figures 5(g) and 5(h). In Figure 12, the watermark patterns are embedded into the colour image generated artificially, while in Figures 13 and 14, we used colour images captured by a smartphone. From these figures, we can see that the proposed visible watermarking scheme embeds adequately both types of watermark patterns, providing



(a) (b) (c)

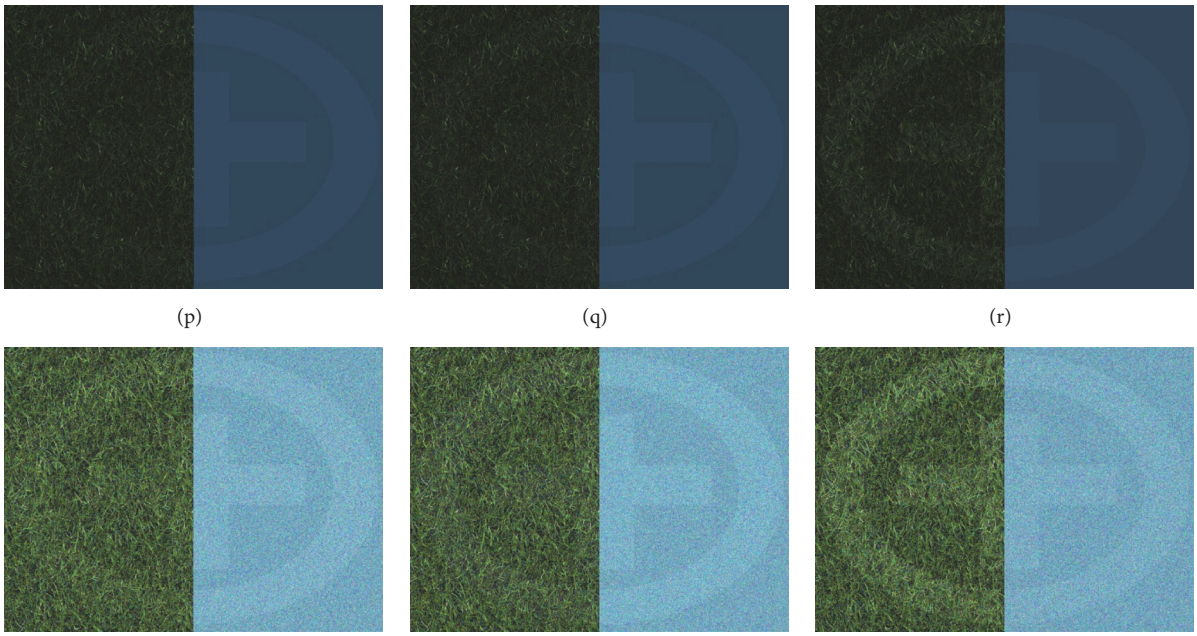
(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

(m) (n) (o)

Figure 10: Continued.



(p) (q) (r)

(s) (t) (u)

Figure 10: Attacked visible watermarked artificial images (Figure 5(a)), generated by [13, 14] and proposed algorithm. ((a)–(c)) Compressed watermarked images by JPEG standard, ((d)–(f)) high contrast, ((g)–(i)) low contrast, ((j)–(l)) Gaussian low-pass filter, ((m)–(o)) high illumination, ((p)–(r)) low illumination, and ((s)–(u)) Gaussian noise contamination.

Table 3: Comparison of MOS among two previously proposed algorithms [13, 14] and proposed algorithm.

	Artificial images (Figures 5(a) and 5(b))		Natural images (Figures 5(c) and 5(d))	
	Visibility	Unobtrusiveness	Visibility	Unobtrusiveness
Lukac's method [13]	3.18	4.01	2.22	3.84
Yu's method [14]	3.19	3.89	3.02	3.83
Proposed method	4.59	4.39	4.13	4.10

Table 4: Comparison of watermark visibility using objective assessment based on PSNR.

Natural images	PSNR (dB)		
	Lukac's method [13]	Yu's method [14]	Proposed method
Figure 5(c)	15.07	15.08	15.96
Figure 5(d)	11.49	11.72	12.40

watermark unobtrusiveness and sufficient visibility. The use of grey-scale and colour watermark patterns provides also advertisement effects for the watermarked images, which is another advantage of our proposed scheme.

5.4. Computational Complexity. In this subsection we analyze the computational complexity of the proposed algorithm compared with other visible watermarking schemes operated in the frequency domains, such as the DCT domain [19] and the DWT domain [21], and the CFA domain algorithms [13, 14]. The proposed algorithm operates directly in CFA domain, in which any transform is not required; however we use the Canny operator to detect edges, which requires relatively high computational cost. The number of multiplications required for the Canny operator for an image with $N \times N$ pixels is $48N^2$ [23]. The number of multiplications to calculate scaling and embedding factors is $7N^2$, being total number of multiplications $55N^2$.

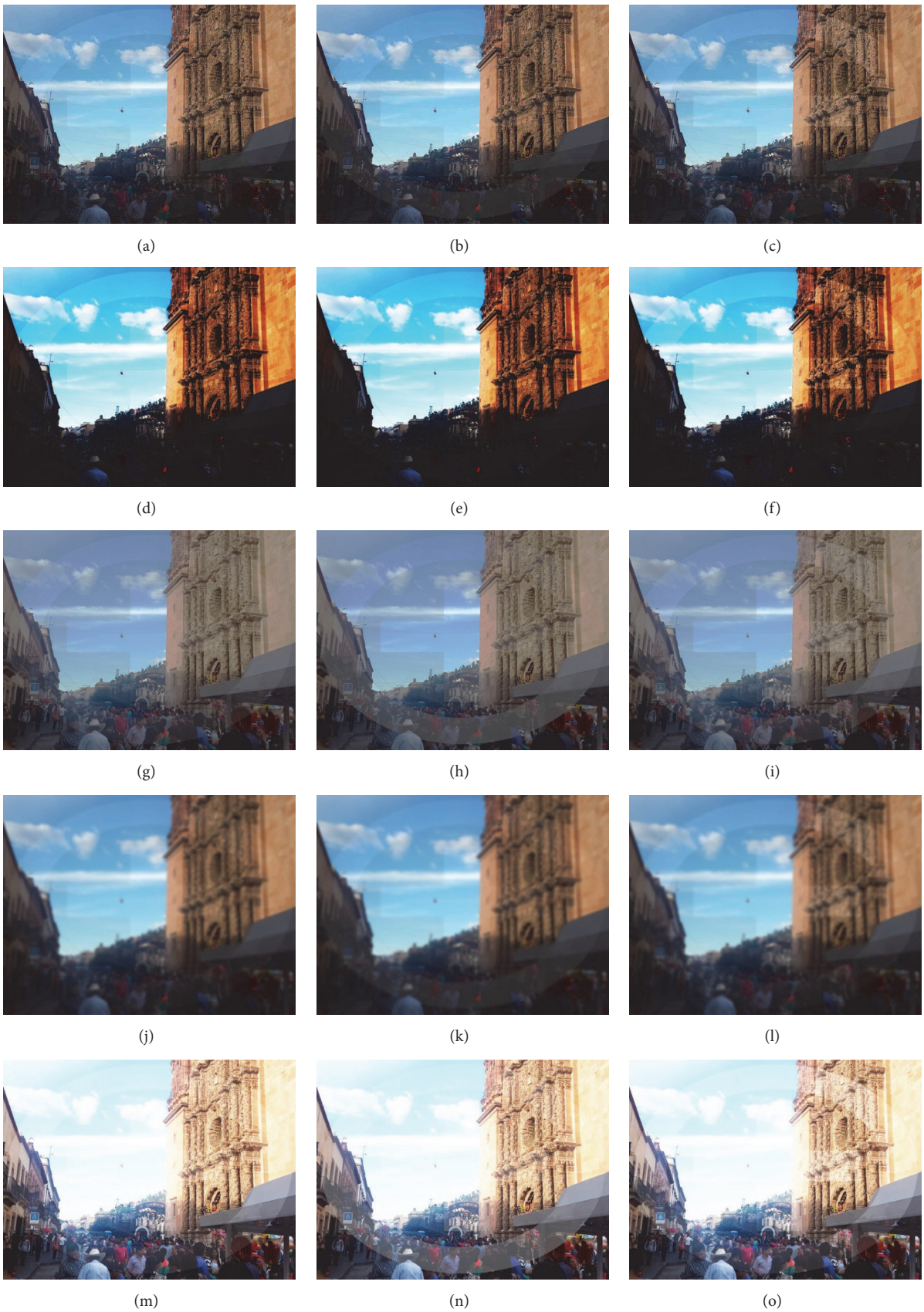
In the frequency domain visible watermarking algorithms, first the host image is transformed to the frequency domain, and then the visible watermark pattern is embedded into the frequency coefficients. Finally, the inverse transform is applied to the watermarked coefficients to obtain the watermarked image. Considering that the number of multiplications required by the 2D DCT for each block of 8×8 pixels is 4096 [25], the total number of the multiplications required for an image of $N \times N$ pixels is $64N^2$, because the image of $N \times N$ pixels contains $N^2/64$ nonoverlapped blocks, while the number of multiplications required for the 2D DWT varies depending on the number of the order of

Table 5: Comparison of the MOS using two artificial images (Figures 5(a) and 5(b)), among two previously proposed algorithms [13, 14] and proposed algorithm under several attacks. "V" and "UO" mean watermark visibility and unobtrusiveness, respectively.

Algorithms	JPEG compression (quality factor: 30%)		High contrast (+200)		Low contrast (−200)		Gaussian blur (8 × 8 filter)		High luminance (+100)		Low luminance (−100)		Gaussian noise (variance 0.01)	
	V	UO	V	UO	V	UO	V	UO	V	UO	V	UO	V	UO
[13]	3.13	3.92	2.66	3.68	3.13	3.45	2.86	3.23	2.86	3.47	2.35	3.17	2.39	3.20
[14]	3.04	3.77	2.45	3.50	3.57	3.48	2.97	3.25	2.94	3.47	2.37	3.11	2.40	3.15
Proposed	4.56	4.32	4.49	4.19	4.36	3.83	4.24	3.69	4.17	3.87	3.98	3.71	4.00	3.75

Table 6: Comparison of the MOS using two natural images (Figures 5(c) and 5(d)), among two previously proposed algorithms [13, 14] and proposed algorithm under several attacks. "V" and "UO" mean watermark visibility and unobtrusiveness, respectively.

Algorithms	JPEG compression (quality factor: 30%)		High contrast (+200)		Low contrast (−200)		Gaussian blur (8 × 8 filter)		High luminance (+100)		Low luminance (−100)		Gaussian noise (variance 0.01)	
	V	UO	V	UO	V	UO	V	UO	V	UO	V	UO	V	UO
[13]	2.42	3.71	1.76	3.18	3.07	3.85	1.97	2.85	2.24	3.61	2.09	3.24	1.70	3.03
[14]	3.07	3.68	1.90	3.15	3.66	3.52	2.76	2.94	2.86	3.48	2.52	3.27	2.29	3.12
Proposed	4.17	4.08	3.03	3.46	4.30	3.98	3.61	3.26	3.65	3.77	3.40	3.47	3.35	3.41



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

(m) (n) (o)

Figure 11: Continued.

(p) (q) (r)

(s) (t) (u)

Figure 11: Attacked visible watermarked natural images (Figure 5(c)), generated by [13, 14] and proposed algorithm. ((a)–(c)) Compressed watermarked images by JPEG standard, ((d)–(f)) high contrast, ((g)–(i)) low contrast, ((j)–(l)) Gaussian low-pass filter, ((m)–(o)) high illumination, ((p)–(r)) low illumination, and ((s)–(u)) Gaussian noise contamination.

the wavelets (T) and the decomposition levels (L) required by the visible watermarking algorithm. For an image of $N \times N$ pixels, the number of multiplications required for 2D DWT is $(16/3)TN^2(1 - 1/4^L)$. For example, in the DWT-based visible watermarking [21], where the 9/7 biorthogonal wavelets with $T = 9$ and decomposition levels $L = 5$ are used, the number of multiplications is approximately $48N^2$. Generally, the inverse transform requires the same number of operations as that required for its transform. Table 7 shows the number of multiplications required for the DCT-based algorithm [19], the DWT-based algorithm [21], and proposed algorithm.

In the CFA domain algorithm [13], the embedding factor is a user-setting constant value; therefore the number of multiplications is N^2 for an image of $N \times N$ pixels while in [14] the embedding factor is obtained according to luminance value of each pixel, so $2N^2$ multiplications are required. Comparing the conventional CFA domain algorithms [13, 14], proposed algorithm requires a larger number of operations. However, considering normal computer power of any available mobile device, which is approximately 5GFLOPS–15GFLOPS [26], the proposed visible watermarking algorithm for an image with 2000×2000 pixels can operate within 0.2 seconds. In this case we considered the number of multiplications, additions, comparisons, and some overhead caused by memory access. Considering the above we can conclude that proposed visible watermarking algorithm can operate in real-time.

6. Conclusions

We proposed Bayer CFA domain visible watermarking scheme for images captured by mobile devices, in which watermark embedding is performed directly in the Bayer CFA before the captured image is stored in a storage system. The proposed watermarking scheme allows establishing rightful ownership according to the proof provided by [11], because original unwatermarked image does not exist anywhere, avoiding its possession of any adversaries. In order to provide a proper operation in mobile devices, which presents still limited computational resources, the computational complexity for watermarking must be reduced. Unlike almost all visible watermarking algorithms, the proposed scheme operates in Bayer CFA domain without any time-consuming frequency transforms. Therefore, we consider that the proposed scheme is suitable to protect images captured by mobile devices.

Until now, few watermarking algorithms have been developed for Bayer CFA domain, in which the HVS is not explored sufficiently. As consequence of this situation, visible watermarking requirements were not satisfied completely. The proposed approach takes advantage of the two most important characteristics of the HVS: luminance and texture sensibility of human's eye, allowing the proposed scheme to meet desirable characteristics of visible watermarking. The experimental results show the better performance of proposed algorithm compared with two Bayer CFA-based algorithms [13, 14], from watermark visibility and unobtrusiveness points of view. Also the robustness of visible watermark provided by proposed algorithm under several attacks is evaluated and compared with two previous Bayer CFA-based algorithms [13, 14]. From the experimental results, we conclude that proposed algorithm provides a better performance compared with two algorithms [13, 14] in all

(a) (b)

Figure 12: Watermarked image generated by proposed scheme, using grey-scale (a) and colour images (b) as watermark patterns.

(a) (b) (c)

Figure 13: Watermarked image generated by proposed scheme. (a) Original colour image and (b) and (c) watermarked images by grey-scale and colour watermarks, respectively.

(a) (b) (c)

Figure 14: Watermarked image generated by proposed scheme. (a) Original colour image and (b) and (c) watermarked images by grey-scale and colour watermarks, respectively.

Table 7: Number of multiplications required by the DCT-based visible watermarking algorithm [19], the DWT-based visible watermarking algorithm [21], and proposed algorithm.

Visible watermarking	Transform/inverse transform	Watermarking	Total
DCT-based algorithm [19]	$64N^2$	$N^2/8$	$\approx 128N^2$
DWT-based algorithm [21]	$48N^2$	$5N^2$	$101N^2$
Proposed algorithm	0	$55N^2$	$55N^2$

attack cases. It is worth noting that the main assessments are obtained using the MOS evaluations, because we consider that the sensibility of the HVS is highly subjective issue. However, we provide an objective evaluation based on the PSNR for the watermark visibility, which provides also better performance of the proposed scheme compared with the previous methods [13, 14].

The computational complexity of the proposed algorithm is analyzed and compared with other visible watermarking algorithms performed in different domains, and we conclude that the proposed visible watermarking algorithm can operate in real-time on the mobile devices.

Unlike previous Bayer CFA domain visible watermarking, in which only binary watermark pattern is accepted, the proposed watermarking scheme allows embedding any types of watermark images, including grey-scale and colour images. The grey-scale and colour watermark pattern are desirable if the visible watermarking is additionally used for advertisement purpose.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

Authors thank the National Council of Science and Technology (CONACyT) of Mexico for the financial support during the realization of this research.

References

[1] P.-Y. Lin, Y.-H. Chen, C.-C. Chang, and J.-S. Lee, "Contrast-adaptive removable visible watermarking (CARVW) mechanism," *Image and Vision Computing*, vol. 31, no. 4, pp. 311–321, 2013.

[2] Y. Hu, S. Kwong, and J. Huang, "An algorithm for removable visible watermarking," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 1, pp. 129–133, 2006.

[3] S.-C. Shie and S. D. Lin, "Improving robustness of visible image watermarks," *Imaging Science Journal*, vol. 56, no. 1, pp. 23–28, 2008.

[4] F. C. Mintzer, L. E. Boyle, A. N. Cazes et al., "Toward on-line, worldwide access to Vatican Library materials," *IBM Journal of Research and Development*, vol. 40, no. 2, pp. 139–160, 1996.

[5] H. M. Gladney, F. Mintzer, and F. Schiattarella, "Safeguarding digital library contents and users: digital images of treasured antiquities," *D-Lib Magazine*, 1997.

[6] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, 2000.

[7] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: classification, estimation-based attacks, and benchmarks," *IEEE Communications Magazine*, vol. 39, no. 8, pp. 118–125, 2001.

[8] C.-H. Huang and J.-L. Wu, "Attacking visible watermarking schemes," *IEEE Transactions on Multimedia*, vol. 6, no. 1, pp. 16–30, 2004.

[9] M. S. Kankanhalli, Rajmohan, and K. R. Ramakrishnan, "Adaptive visible watermarking of images," in *Proceedings of the 6th IEEE International Conference on Multimedia Computing and Systems (ICMCS '99)*, pp. 568–573, Florence, Italy, June 1999.

[10] R. Poisel and S. Tjoa, "Forensics investigations of multimedia data: a review of the state-of-the-art," in *Proceedings of the 6th International Conference on IT Security Incident Management and IT Forensics (IMF '11)*, May 2011.

[11] S. Craver, N. Memon, B.-L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 573–586, 1998.

[12] H. Qi, D. Zheng, and J. Zhao, "Human visual system based adaptive digital image watermarking," *Signal Processing*, vol. 88, no. 1, pp. 174–188, 2008.

[13] R. Lukac and K. N. Plataniotis, "Camera image watermark transfer by demosaicking," in *Proceesdings of the 48th International Symposium Focused on Multimedia Signal Processing and Communications (ELMAR '06)*, pp. 9–12, Zadar, Croatia, June 2006.

[14] P. Yu, Y. Shang, and C. Li, "A new visible watermarking technique applied to CMOS image sensor," in *Proceedings of the 8th Symposium on Multispectral Image Processing and Pattern Recognition (MIPPR '13)*, vol. 8917, Wuhan, China, October 2013.

[15] B. K. Gunturk, J. Glotzbach, Y. Altunbasak, R. W. Schafer, and R. M. Mersereau, "Demosaicking: color filter array interpolation," *IEEE Signal Processing Magazine*, vol. 22, no. 1, pp. 44–54, 2005.

[16] D. Menon, S. Andriani, and G. Calvagno, "Demosaicing with directional filtering and a posteriori decision," *IEEE Transactions on Image Processing*, vol. 16, no. 1, pp. 132–141, 2007.

[17] A. Kejariwal, "Watermarking," *IEEE Potentials*, vol. 22, no. 4, pp. 37–40, 2003.

[18] D. J. Granrath, "The role of human visual models in image processing," *Proceedings of the IEEE*, vol. 69, no. 5, pp. 552–561, 1981.

[19] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '00)*, pp. 1029–1032, New York, NY, USA, July-August 2000.

[20] Y. Hu and S. Kwong, "Wavelet domain adaptive visible watermarking," *Electronics Letters*, vol. 37, no. 20, pp. 1219–1220, 2001.

[21] B.-B. Huang and S.-X. Tang, "A contrast-sensitive visible watermarking scheme," *IEEE Multimedia*, vol. 13, no. 2, pp. 60–66, 2006.

[22] M.-J. Tsai, "A visible watermarking algorithm based on the content and contrast aware (COCOA) technique," *Journal of Visual Communication and Image Representation*, vol. 20, no. 5, pp. 323–338, 2009.

[23] J. Canny, "A computational approach to edge detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 8, no. 6, pp. 679–698, 1986.

[24] Z. Wei and K. N. Ngan, "Spatio-temporal just noticeable distortion profile for grey scale image/video in DCT domain," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 3, pp. 337–346, 2009.

[25] L. Agostini, I. Silva, and S. Bampi, "Pipelined fast 2D DCT architecture for JPEG image compression," in *Proceedings of the 14th Symposium on Integrated Circuits and Systems Design*, pp. 226–231, Pirenopolis, Brazil, September 2001.

[26] "ARM Cortex Processors," https://www.arm.com/products/processors.