IET Biometrics

Special Issue: Selected Papers from the International Workshop on Biometrics and Forensics (IWBF2017)

The Institution of Engineering and Technology Journals

Improved imperceptible visible watermarking algorithm for auxiliary information delivery

ISSN 2047-4938
Received on 2nd August 2017
Revised 10th December 2017
Accepted on 20th December 2017
E-First on 28th February 2018
doi: 10.1049/iet-bmt.2017.0145
www.ietdl.org

Oswaldo Juarez-Sandoval[1], Eduardo Fragoso-Navarro[1], Manuel Cedillo-Hernandez[1], Antonio Cedillo-Hernandez[2], Mariko Nakano[1] ✉, Hector Perez-Meana[1]

[1]SEPI ESIME Culhuacan, Instituto Politecnico Nacional, Mexico City, Mexico
[2]Universidad Nacional Autonoma de Mexico, Mexico City, Mexico
✉ *E-mail: mnakano@ipn.mx*

Abstract: An imperceptible visible watermarking (IVW) algorithm is proposed to deliver auxiliary information about the visual contents, including ownership information. The proposed algorithm overcomes several inconveniences presented in previously reported IVW algorithms using the just noticeable difference (JND) criterion, invisible watermarking and binarisation function. The proposed algorithm consists of the visible watermark embedding and the exhibition stages. The JND criterion is used to embed visible watermark pattern in an imperceptible manner by the human visual system, while invisible watermarking based on the discrete cosine transform is used to share crucial parameters between both stages, which makes possible the watermark visualisation without any side information. In the watermark exhibition stage, the imperceptibly embedded visible watermark pattern is exhibited by the binarisation function. The proposed algorithm can be applied to any class of images with different characteristics and several visible watermark patterns can be embedded into an input image. Evaluation results show that performance of the proposed algorithm is better compared with previously reported algorithms from several practical points of view.

1 Introduction

Nowadays, thanks to the recent technological advances of the Internet, many consumers seek the desired visual information on their computers or mobile phones. At the same time, these advances provide new opportunities for the developers to create their visual contents in a digital manner and deliver them through Internet. Naturally, the contents developers desire to transmit some important information, such as ownership information, contact details, and usage right, together with their digital contents. Usually, the information related to the digital contents is added as metadata into the digital file; however, many file transformation tools remove the metadata to reduce the file size. Also, in many cases, detailed information about the visual contents is provided using 2D bar codes or quick response (QR) codes; however, these 2D codes occupy important space in the digital visual contents.

Digital watermarking technologies emerged as a reliable mechanism for copyright protection of the digital contents [1–4], whose use has been extended to provide good solutions in many applications related to the digital contents, such as tamper detection [5, 6], broadcast monitoring system [7] and so on. Also, the ownership information, including contact detail, usage right etc., can be successfully delivered using the watermarking technique, providing an alternative solution for the above mentioned problems of metadata and QR codes. Huang *et al.* proposed a novel unseen visible watermarking (UVW) algorithm for auxiliary information delivery [8], in which a visible watermark pattern is embedded in an imperceptible manner into the host image. If the viewer requires some auxiliary information about the image, then he/she applies the gamma correction equipped in the TV monitor to visualise the embedded visible watermark, which contains the auxiliary information. In this scheme, any watermark exhibition algorithm is not required, which is the principal advantage of this scheme. However, the watermark pattern must be embedded into the darkest plain region in order to obtain the proper effect of the gamma correction for watermark visualisation. Considering the fact that relatively few images contain a darkest plain region, its use may be limited.

Taking into account the limitation of [8], Lin proposed the imperceptible visible watermarking (IVW) algorithm, in which a visible watermark pattern is embedded into a plain region of the most appropriate colour channel [9]. To reveal the watermark pattern, the histogram range of the watermarked image is modified using the mean value of the selected region of the appropriate colour channel. Lin's algorithm can be applied to almost all images with different characteristics; however, the mean value and colour channel used in the embedding stage are required to visualise the watermark pattern in the watermark exhibition stage. In many cases, without this information, the visible watermark pattern cannot be visualised. The author suggested that all possible combinations of three colours and 256 intensities by each colour channel are used to visualise the watermark pattern. However, it may reduce the practical use of this scheme. Additionally, in this scheme, the exhibited watermark pattern is a colour pattern, which is not convenient if a QR code is used as the watermark pattern because almost all QR code decoders cannot decode the colour QR code. If the QR code is used as the watermark pattern, a binarisation must be performed on the selected colour channel as a post-processing after visualisation of the watermark pattern.

Juarez *et al.* [10] proposed an improved version of the UVW algorithm [8] in order to increase applicability to a wide range of images that contain neither the plain region nor the darkest region, introducing the total variation algorithm with L1-norm (TV-L^1) [11] and a shifted gamma function. In this algorithm, the visible watermark embedding and exhibition are carried out in the luminance channel of the colour image. The TV-L^1 decomposes the input image into a cartoon image and a texture image. Since the cartoon image usually contains a large plain region, the watermark pattern is embedded into this image. The watermark embedding formula used in this algorithm is the same as [8], but the embedding energy is calculated adaptively to the human visual system (HVS) using the just noticeable difference (JND) criterion. In the watermark exhibition stage, the shifted gamma function is used to reveal the visible watermark pattern. However, the shift value obtained and used in the embedding stage is required to reveal the watermark pattern, so this value must be transmitted to the watermark exhibition stage as side information. Moreover, the TV-L^1 algorithm is not suitable for all types of images, actually more than half of images used in the experiment presented some difficulties. Besides this situation, the high computational complexity of this algorithm reduces its practical use.

Recently, many people watch movies, TV series and documentaries on his/her PC or mobile devices using the online video service. In 2016, the most important stream media company extended their service to 160 countries and the number of subscribers has reached more than 87 million [12]. Considering this actual situation, watermarking techniques for auxiliary information delivery can be adapted in this environment, where enhancement function used for watermark visualisation does not have to be limited to the functions available in monitor or display. The enhancement function can be any function generated by a computer algorithm and applied in the watermark exhibition stage. Considering the limitation presented in the previous schemes [8–10], in this study, we present an improved IVW, which is based on our previous work [10] but overcomes several inconveniences presented in it [10].

In the proposed algorithm, the JND criterion is used to calculate an appropriate embedding energy to guarantee watermark imperceptibility by the HVS. To reveal the watermark pattern, a binarisation function is applied to the watermarked image. Since the crucial parameters to operate binarisation function cannot be preserved after watermarking, these parameters must be shared between the watermark embedding and the exhibition stages. Thus in the proposed algorithm, the crucial parameters are embedded into randomly selected blocks of the host image using an invisible quantisation index modulation (QIM) watermarking algorithm under dither modulation (DM) modality (QIM-DM) in the discrete cosine transform (DCT) domain. The experimental results show the desirable properties of the proposed algorithm as an auxiliary information delivery system. The robustness of the proposed algorithm against compression and noise contamination is compared with the previously presented methods [9, 10]. The robustness against malicious attacks, such as geometric distortions, including cropping, rotation, translation, and scaling, were not considered because the objective of the proposed scheme is content information delivery. In this application, a consideration of the malicious attacks becomes meaningless.

The rest of this paper is organised as follows: in Section 2, we provide the brief descriptions of two pioneering algorithms, UVW [8] and IVW [9]. The proposed IVW scheme is described in Section 3 and in Section 4 the experimental results of a proposed method including a comparison with the previous algorithms [8–10] are shown. Finally, we conclude this paper in Section 5.

2 Related works

In this section, two pioneer works related to the IVW algorithms [8, 9] are described briefly.

2.1 UVW based on gamma function [8]

Huang *et al.* [8] proposed a novel visible watermarking scheme called UVW for auxiliary information delivery, in which the embedded watermark pattern is invisible to naked eye under normal viewing conditions; while applying gamma correction, which is off-the-shelf function of TV monitor, the watermark pattern becomes visible without any watermark extraction algorithm. In the 8 bits resolution, the gamma correction is formulated by $q = 255^{(1-\gamma)} \times p^{\gamma}$, where p and q are the input and output intensities of the image, and $\gamma < 1$ is constant. The intensity value $i^* = 0$ presents a maximum gradient of the gamma correction function and, because this function is the means of watermark exhibition, this algorithm must embed the watermark pattern in the plain darkest region.

Once an adequate intensity value i^* is determined, the best region to embed a binary watermark pattern W is determined by applying the following equation:

$$(x^*, y^*) = \arg\min_{(x, y)} \sum_{x = x_0}^{x_0 + w - 1} \sum_{y = y_0}^{y_0 + h - 1} |I(x, y) - i^*|, \tag{1}$$

where (x^*, y^*) is the upper-left position of most appropriate region R, w and h are width and height of the watermark pattern W and the region R, I is the input image of size $M \times N$ and (x_0, y_0) is the position in I, which satisfies $1 \le x_0 \le M - w + 1$, $1 \le y_0 \le N - h + 1$. Once the most appropriate region R is determined, the de-noising operation is applied iteratively to the region, which makes the revealed watermark pattern clearer. This de-noising operation is controlled by a threshold value $T_d \in [0, 1]$. If $T_d = 1$, the de-noising operation is repeated until all pixel values within the region R become to i^*, while $T_d = 0.5$ means that the iterative de-noising operation stops if the half of the pixels of the region have intensity value i^* [8].

After the de-noising operation, a binary watermark pattern W is embedded into the region R as follows:

$$R_{\rm w}(x, y) = \begin{cases} R(x, y) + \Delta_a, & \text{if } W(x, y) = 1, \\ R(x, y), & \text{otherwise}, \end{cases} \tag{2}$$

where R is the original region after the de-noising operation, $R_{\rm w}$ is the watermarked region and Δ_a is the watermark embedding strength.

As mentioned above, the input image must contain a darkest plain region for watermark embedding; however, almost all images do not satisfy this condition. Although authors suggest some alternative methods, such as histogram equalisation and the combination of shift function and gamma function [8], the effectiveness of these functions strongly depends on the characteristics of the image. For example, the histogram equalisation is effective only in low contrast images and the combination of the shift function and the gamma function requires the shift value to reveal the unseen watermark pattern; however, this value depends on the input image.

2.2 IVW based on histogram modification [9]

Lin proposed an IVW based on histogram operation [9], in which the range of the histogram is narrowed within three bins to reveal the embedded visible watermark pattern. The minimum or maximum bin value of the modified histogram is determined by the mean value m of the region where the imperceptible visible watermark pattern is embedded.

In the imperceptible visible watermark embedding of [9], first a region of size $w \times h$ with a minimum variance of the colour image is selected by (3), where $w \times h$ is the size of the watermark pattern

$$sr^* = \arg\min_{k} \sum_{C \in \{R, G, B\}} \sum_{k = 1}^{w \times h} (e_C(p_k) - \bar{e}_C)^2, \tag{3}$$

where $C \in \{R, G, B\}$ is one of three colour channels, $e_C(p_k)$ is the colour intensity of a kth pixel in colour channel C, $\bar{e}_C$ is the mean value and sr^* is the upper-left position of the selected region. To keep the modified bin range of the histogram is within [0, 255], the mean value m is selected in an appropriate manner, applying the following equation:

$$m = \begin{cases} \min(\bar{e}_{\rm R}, \bar{e}_{\rm G}, \bar{e}_{\rm B}), & \text{if } \min(\bar{e}_{\rm R}, \bar{e}_{\rm G}, \bar{e}_{\rm B}) \ge T_h, \\ \max(\bar{e}_{\rm R}, \bar{e}_{\rm G}, \bar{e}_{\rm B}), & \text{otherwise}, \end{cases} \tag{4}$$

where $T_h$is the threshold value, which is set to 2 [9]. Once the mean value m is determined, the pixel value of the selected region will take one of the two values. If the pixel value corresponds to a white pixel of the watermark, then this pixel value is equal to the mean value m, otherwise, the pixel value is set to $m - T_h$. In this manner, the binary watermark pattern is embedded imperceptibly. Unlike [8], this method can embed an imperceptible visible watermark in a region with any intensity.

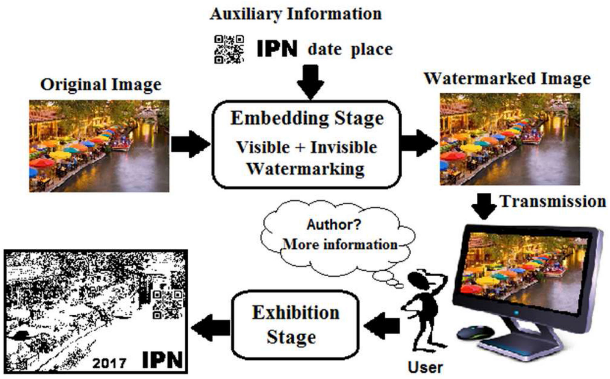

Fig. 1 *Brief diagram of proposed scheme*

The principal disadvantage of this scheme is that the mean value *m* is required in the watermark exhibition stage to properly reveal the watermark pattern because, in almost all images, the most appropriate region with minimum variance given by (3) is changed after watermark embedding. Without the knowledge of the mean value *m* used in the embedding stage, the visible watermark pattern cannot be revealed. In [9], the author suggests that all possible histogram modifications are applied to the watermarked image to reveal the visible watermark pattern. However, the trial number reaches about 3×256 times, so it is not feasible in the practical applications.

Another disadvantage of this scheme is that it is not robust to the JPEG compression. Considering the fact that the JPEG compression is an essential operation in digital image and video on the Internet, its practical use may be also limited.

3 Proposed algorithm

The proposed algorithm consists of two stages: the watermark embedding stage and the visible watermark exhibition stage. Fig. 1 shows the principal application of the proposed scheme, in which a user observes an image or a frame of video on his/her computer and if he/she desires more information about the digital content then visible watermarks, such as owner's logotype and QR code, are visualised clicking a mouse button. The quality of the watermarked image that the user observes is almost the same as the quality of the original image. In the proposed scheme, multiple watermark patterns, such as owner's logotype, QR code, and other additional information, e.g. date and place, can be embedded.

In the watermark embedding stage, visible watermark, and invisible watermark, which consist of crucial parameters to reveal the visible watermark pattern, are embedded in an imperceptible manner. In the visible watermark exhibition stage, firstly the crucial parameters are extracted from the image and using these parameters, the binarisation operation is applied to the image to reveal visible watermark patterns.

3.1 Watermark embedding stage

In the proposed scheme, the owner of the digital content can determine the number of imperceptible visible watermarks that are embedded into the image. We denote this number as *K*. The watermark embedding stage of the proposed IVW scheme takes the following steps:

1. Select the region where the invisible watermark is embedded. Using contents owner's secret key, *BN* blocks of 8×8 pixels are selected randomly from the host image. The number of selected blocks *BN* depends on the number of the visible watermark patterns *K* which is determined by the owner depending on his/her need. The relationship between *BN* and *K* will be explained later. We denote the regions occupied by the selected *BN* blocks as R_{IV} for further explanation.
2. Select the *K* most proper regions with the size $S_{h_k} \times S_{w_k}$, $1 \le k \le K$ from the three colour channels of the host image, where S_{h_k} and S_{w_k} are the height and width of the *k*th visible watermark pattern. To this end, we define candidate regions R_k of size $S_{h_k} \times S_{w_k}$ for the *k*th region, which must satisfy $R_k \in I - (R_{IV} + R_l^*)$, where R_{IV} are the selected blocks of the image *I* for invisible watermarking and R_l^* is the most proper region for *l*th visible watermark pattern, which has already been embedded, $1 \le l < k \le K$. This condition for the candidate regions guarantees that the watermarked regions, both visible and invisible, are not overlapped among them. To determine the most proper region for the *k*th visible watermark, we select a region with the lowest variance from all candidate regions R_k.

$$R_k^* = \arg\min_{R_k} \left(\frac{1}{S_{h_k} \times S_{w_k} - 1} \sum_{(i,j,c) \in R_k} \left(p_{i,j,c} - \mu_{R_k} \right)^2 \right), \quad (5)$$

where $p_{i,j,c}$ is the (i,j)th pixel value of the *c*th colour channel, μ_{R_k} is the mean value of a candidate region and R_k^* is the most proper region for *k*th visible watermark pattern. From (5) R_k^* can be considered as the smoothest region within the candidate regions R_k in terms of variance.
3. Obtain the mean values and colour channels of the *K* selected regions. Once the *K* most proper regions $R_k^*, k = 1, 2, \ldots, K$ are selected, obtain their corresponding mean values μ_k^* and the colour channels c_k^*, where $c_k^* \in \{\text{red}, \text{green}, \text{blue}\}$. Finally, *K* pairs of data $\{(\mu_1^*, c_1^*), (\mu_2^*, c_2^*), \ldots, (\mu_K^*, c_K^*)\}$ are obtained.
4. Embedding imperceptible visible watermark. The *K* visible watermark patterns are embedded into the *K* most proper regions R_k^* of the host image as shown by using the following equation:

$$\hat{R}_k^*(i,j) = \begin{cases} \max\left(0, \mu_k^* - \left[\dfrac{T_{\text{JND}}}{2}\right]\right), & \text{if } W(i,j) = 0, \\ \min\left(\mu_k^* + \left[\dfrac{T_{\text{JND}}}{2}\right], 255\right), & \text{if } W(i,j) = 1, \end{cases} \quad (6)$$

where $\hat{R}_k^*(i,j)$ is the *k*th visible watermarked region, T_{JND} is the embedding strength of the visible watermark, which is determined using the JND criterion [13]. The value μ_k^* is the mean intensity of the colour channel c_k^* of the *k*th selected region R_k^* in step 2, *W* is the binary watermark pattern and $[x]$ provides the nearest integer value of *x*.
5. Compute the watermarking strength T_{JND}. The strength of the visible watermarking must depend on the mean intensity value of the region to keep good imperceptibility. The HVS is less sensible to the lowest and the highest intensity level compared with the middle intensity level, and the JND determines the intensity difference between the intensity of the forward pattern and the intensity of the background that the HVS cannot perceive, depending on the background intensity level. To determine the JND depending on the background intensity level, we used relationship provided by [14], which is formulated by

$$T_{\text{JND}} = \begin{cases} -\dfrac{1}{8}p + 6, & p \in (0, 32), \\ -\dfrac{1}{32}p + 3, & p \in (33, 64), \\ \dfrac{1}{96}p + \dfrac{1}{3}, & p \in (65, 255), \end{cases} \quad (7)$$

where *p* is the intensity value. Fig. 2 shows the JND values of each background intensity value according to (7). We can

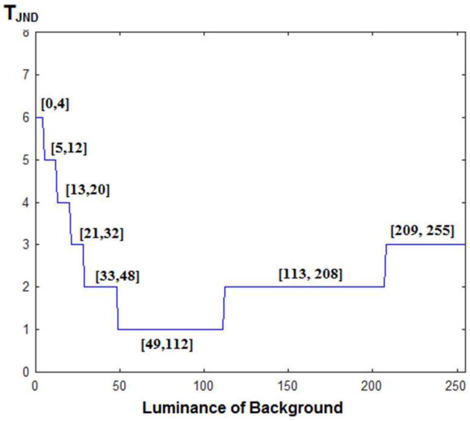

Fig. 2 *JND value of each background luminance [14]*

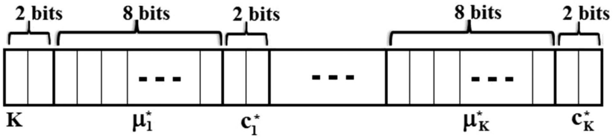

Fig. 3 *BS composed of the crucial parameters*

observe from Fig. 2 that if the background intensity is within [49, 112], the visible watermark pattern must be embedded with the smallest strength to keep its imperceptible property.

6. Embedding crucial parameters using the invisible watermarking technique. The crucial parameters are composed by the pair of a mean intensity value and colour channel of K selected region $\{(\mu_1^*, c_1^*), (\mu_2^*, c_2^*), \dots, (\mu_K^*, c_K^*)\}$, which are embedded into the BN selected blocks of the visible watermarked image using an invisible watermarking technique based on the QIM-DM watermarking [15] in the 2D DCT domain. Firstly, the crucial parameters are converted into the bits sequences (BS) as shown by Fig. 3. Considering that the mean intensity μ_k^* is within the range [0,255], which can be represented by 8 bits, while c_k^* takes one of the three values, red = 1, green = 2 and blue = 3, it can be represented by 2 bits.

The maximum number of embeddable visible watermarks K must be determined taking into account the practical situations. Considering that a uniform resource locator (URL) can be easily encoded in a QR code, and a user interested in obtaining more information about the visual content can decode the URL to obtain all available information, we decided that $K = 3$ is sufficient. Since one visible watermark pattern may be logotype of the owner, other watermarks can be a QR code and the captured date, etc. Therefore, the number of actually embedded visible watermark patterns K can be represented by 2 bits. It is worth noting that the value of K can be changeable according to the application without modifying the proposed algorithm.

Once the watermark bits sequence is generated, which is embedded into the selected BN blocks in step 1 of the visible watermarked image. We divide the bits sequence into the sub-sequence of four bits and each selected BN block is transformed by 2D DCT. Then each sub-sequence composed of 4 bits is embedded into the four alternating current (AC) coefficients with lowest frequencies of each selected block in the 2D DCT domain. The number of the selected blocks BN can be expressed by

$$BN = (2 + 10K)/4, \tag{8}$$

where K is the number of visible watermark patterns and x is the ceiling function.

The watermark embedding is carried out using QIM-DM algorithm [15], which is given by

$$B_{\mathrm{w}} = Q(B + d(z, BS_z), \Delta) - d(z, BS_z), \qquad z = 1, 2, 3, 4 \tag{9}$$

where B and B_{w} are original and watermarked DCT blocks, respectively, BS_z is the segmented bit sequence with 4 bits of the BS shown in Fig. 3. The quantification operation $Q(x, \Delta)$ is given by

$$Q(x, \Delta) = \left[\frac{x}{\Delta} \right] \times \Delta \tag{10}$$

and $d(z, 0)$ is a pseudo-random signal chosen with uniform distribution and $d(z, 1)$ is expressed by

$$d(z, 1) = \begin{cases} d(z, 0) + \dfrac{\Delta}{2}, & \text{if } d(z, 0) < 0, \\ d(z, 0) - \dfrac{\Delta}{2}, & \text{otherwise,} \end{cases} \tag{11}$$

where Δ is the step-size of quantification operation, which defines invisible watermarking strength.

Once all bits sequence is embedded into the DCT coefficients, the watermarked DCT coefficients are converted into the spatial domain applying the inverse 2D DCT.

3.2 Visible watermark exhibition stage

The visible watermark exhibition stage consists of the following steps:

1. Extraction of crucial parameters. First of all, the crucial parameters must be extracted from the watermarked image. To this end, the BN blocks are selected by the owner's secret key from the watermarked image, and then the bits sequence composed by the crucial parameters is extracted from the BN selected blocks using the QIM-DM extraction algorithm [15]. Each selected block is transformed into the DCT domain by the 2D DCT. From the four AC coefficients with lowest frequencies of each block, four bits sequence is extracted by

$$\widetilde{BS}_z = \underset{l \in \{0, 1\}}{\arg\min}\, (c_z - Ds(z, l))^2, \qquad z = 1, 2, 3, 4 \tag{12}$$

where $\widetilde{BS}_z$ is the zth extracted watermark bit, c_z is the zth watermarked DCT coefficient, and $Ds(z, l)$ is a dither signal given by

$$Ds(z, 0) = Q(c_z + d(z, 0), \Delta) - d(z, 0) \tag{13}$$

and

$$Ds(z, 1) = Q(c_z + d(z, 1), \Delta) - d(z, 1), \tag{14}$$

where $d(z, 1), l = 0, 1$ is given by (11) and the quantification operation $Q(x, \Delta)$ is given by (10). The step-size Δ must be the same value used in watermark embedding stage.

Once the bits sequence $\widetilde{\mathrm{BS}}_z$ is extracted, the crucial parameters $\{(\mu_1^*, c_1^*), (\mu_2^*, c_2^*), \dots, (\mu_K^*, c_K^*)\}$ are recovered.

2. Imperceptible visible watermark exhibition. Using the extracted crucial parameters $\{(\mu_1^*, c_1^*), (\mu_2^*, c_2^*), \dots, (\mu_K^*, c_K^*)\}$, the binarisation operation is applied to reveal the kth visible watermark pattern, which is given by

$$\hat{I}_{c_k^*} = \begin{cases} 1, & \text{if } \tilde{I}_{c_k^*} \geq \mu_k^*, \\ 0, & \text{otherwise,} \end{cases} \qquad c_k^* \in \{\text{red}, \text{green}, \text{blue}\}, \tag{15}$$

where $\tilde{I}_{c_k^*}$ and $\hat{I}_{c_k^*}$ are the kth selected colour channel of the watermarked image and the image with the revealed watermark pattern.

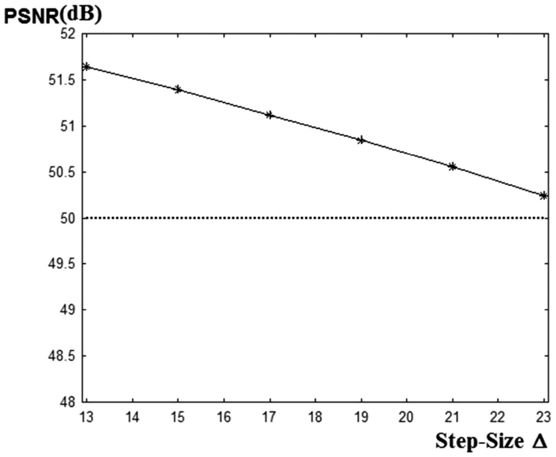

Fig. 4 *Relationship between step-size Δ and PSNR (dB)*

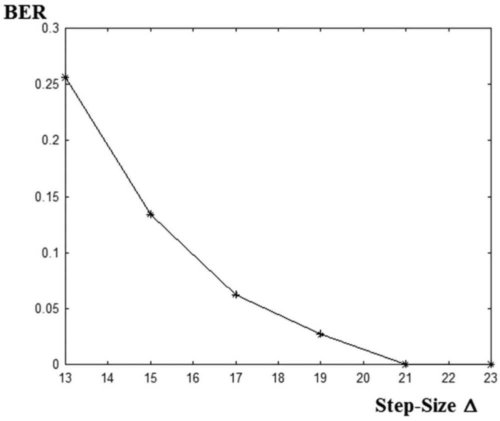

Fig. 5 *Relationship between step-size Δ and BER under JPEG compression with QF = 50*

Table 1 Quality degradation caused by the invisible watermarking

K	*BN*	PSNR, dB
1	3	51.37
2	6	51.03
3	8	50.82

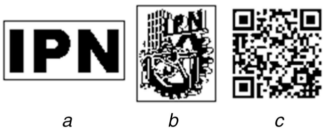

Fig. 6 *Binary watermark patterns*
(a)–(c) Patterns used for evaluation

4 Experimental results

In this section, we evaluate the proposed algorithm from different points of view. First, we show that the proposed algorithm is suitable for any class of images: plain images and detailed images. Also, the watermark imperceptibility and robustness against non-malicious common attacks, such as compression and noise contamination are shown. The performance of the proposed scheme in a real application, shown in Fig. 1, is also provided. Finally, we provide a comparison table, in which the global performance of the proposed algorithm is compared with three previously reported algorithms [8–10]. As an image dataset, we used the uncompressed colour image dataset (UCID) [16], which contains 1338 colour images with size 512 × 384 pixels or 384 × 512 pixels.

In the proposed algorithm, two types of watermarks, the imperceptible visible watermark patterns, and the invisible watermark sequence, are embedded into the host image. The embedding strength of the visible watermark is defined using the JND criterion given by (6) and the embedding strength of the invisible watermarking is defined by step-size Δ used by (9), which is directly related to the quality of the watermarked image and the robustness of the embedded watermark sequence. Therefore, we analyse the step-size Δ from the watermark imperceptibility and robustness points of view to determine an adequate value of the step-size Δ. Here we used eight blocks of 8 × 8 pixels ($BN = 8$) to embed three visible watermark patterns ($K = 3$).

Fig. 4 shows the relationship between the step-size Δ and the watermarked image quality by means of peak signal to noise ratio (PSNR), while Fig. 5 shows the relationship between the step-size Δ and the bit error rate (BER) of the extracted invisible watermark sequence after the watermarked images are compressed by JPEG compression with quality factor (QF) = 50. From Figs. 4 and 5, we can set the value of the step-size Δ equal to 21, because this value guarantees that the PSNR is higher than 50 dB and the BER is equal to 0 under the JPEG compression with the QF = 50.

The image quality degradation caused by the invisible watermarking depends on the number of blocks (*BN*) of 8 × 8 pixels, which is determined by the number of visible watermark patterns (*K*), as given by (8), and the host image size. Table 1 shows the average quality degradation caused by the invisible watermarking of the different number of visible watermark patterns using all images of the dataset [16].

4.1 Suitability for any class of images

Unlike the UVW scheme proposed by Huang *et al.* [8], in which the unseen visible watermark can be embedded only into images that contain a darkest plain region, in the proposed algorithm any class of images can be used for watermark embedding and exhibition. As the watermark pattern, we used a binary pattern composed of letters ‘IPN’ with 46 × 96 pixels, a binary logotype with 72 × 60 and a QR code with 80 × 80 pixels which contains a URL as shown by Fig. 6.

Fig. 7 shows some examples of the watermarked image together with the visible watermark revelation version. Figs. 7*a* and *c* are watermarked images with one watermark pattern (Fig. 6*a*) and Figs. 7*b* and *d* are visible watermark revelation applying the binarisation operation given by (15). As we can observe, Fig. 7*a* contains a plain region, while Fig. 7*c* does not contain any plain region. In both cases, the visible watermark patterns are imperceptible by the naked eye and the revealed watermark patterns, shown in Figs. 7*b* and *d*, are very clear.

4.2 Watermark imperceptibility

In this section, we evaluate the quality degradation of the watermarked image with respect to the original one by means of the PSNR (dB). Table 2 shows the average PSNR values obtained when the watermarked images contain different numbers of visible watermark patterns using all images in the UCID dataset [16]. It is worth noting that in all cases, the PSNR values are >47 dB, which guarantees that the visible watermark and the invisible watermark are imperceptible by the HVS.

4.3 Watermark robustness

In this section, we evaluate the embedded visible watermark robustness against the most common non-malicious attacks, compression and noise contamination using the UCID colour image database [16]. Fig. 8 shows the BER of the extracted watermark under the JPEG compression attack with different QF, and Fig. 9 shows the relationship between the BER and the JPEG2000 compression rate (bpp). In both figures, letters ‘H’,’Q’,’M’ and ‘L’ mean four error correction levels in the common QR code. From both figures, we can observe that the proposed scheme provides higher robustness to both compression attacks than previously proposed algorithms [9, 10], and the revealed QR code can be decoded from the compressed image.

Table 3 shows the visible watermark robustness against noise contamination by impulsive noise.

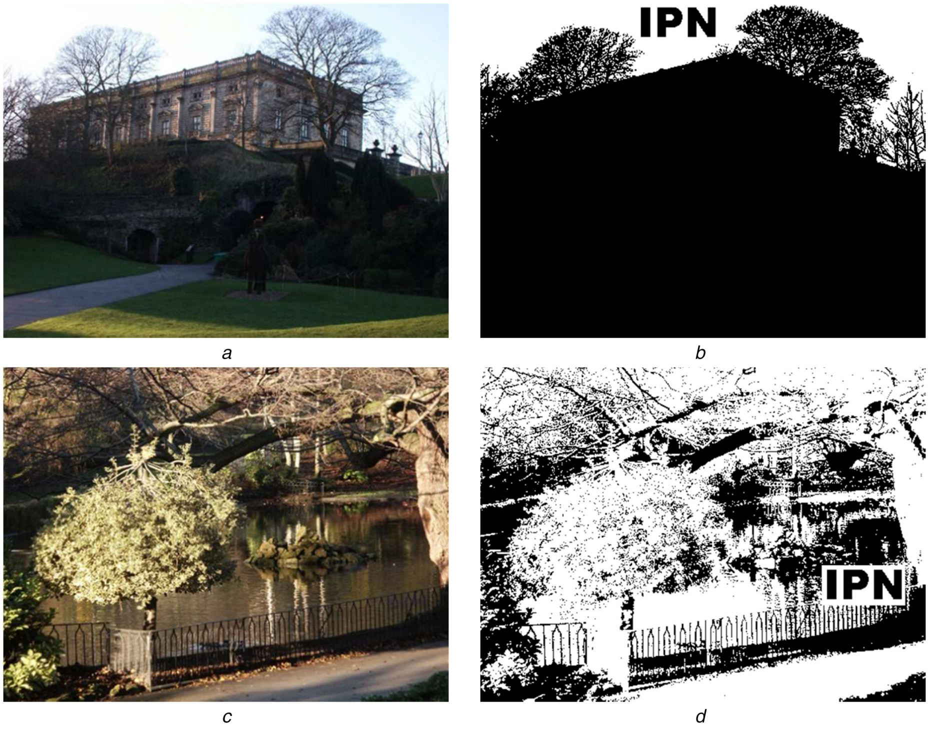

Fig. 7 *Suitability of the proposed algorithm for any class of images*
(a), ***(c)*** Watermarked image with PSNR 49.92 dB and 49.38 dB, respectively, ***(b)***, ***(d)*** Visible watermark revelation version

Table 2 Average watermarked image quality respect to its original one

K	PSNR, dB
1	49.47
2	48.72
3	47.97

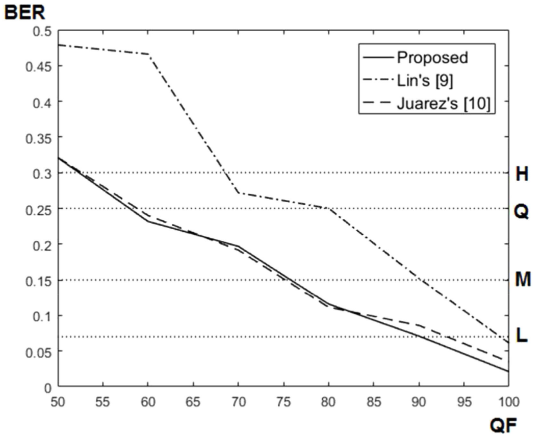

Fig. 8 *Relationship between the QF of JPEG compression and the BER of the extracted visible watermark pattern*

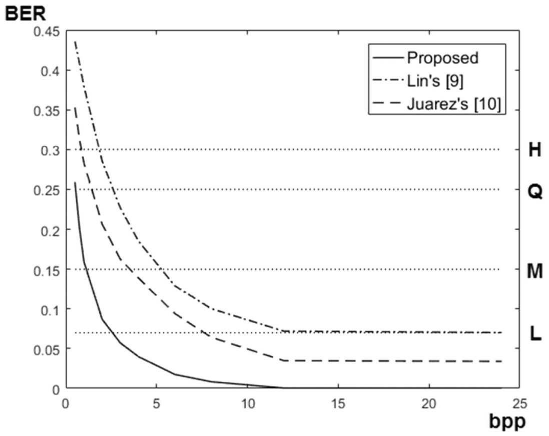

Fig. 9 *Relationship between the compression rate (bpp) of JPEG2000 compression and the BER of the extracted visible watermark pattern*

Table 3 BER (%) of the extracted visible watermark under impulsive noise contamination

Noise density (%)	BER, %		
	Proposed	[9]	[10]
1	0.49	0.48	2.39
3	1.51	1.55	4.10
5	2.53	2.49	7.26
7	3.57	3.57	10.01
9	4.56	4.50	13.02

From this table, we can observe that both, proposed and Lin's scheme [9] provide the same robustness to the noise contamination and higher robustness than [10]. It is worth noting that the comparison results of [8] are not included because very few images (<1%) in the dataset [16] are suitable for [8]. In all experiments, we used side information from [9, 10] to obtain the binary watermark pattern to obtain the BER.

Fig. 10 shows some examples of the visible watermark revelation version from the attacked watermarked images. Fig. 10*a* is the watermarked image compressed by using the JPEG compressor whose QF is equal to 70, while Fig. 10*b* is its revelation version. Fig. 10*c* is the noisy watermarked image with 10% impulsive noise, and Fig. 10*d* shows the watermark revelation version. From all cases, we can observe that the revealed visible watermark pattern is sufficiently clear after the watermarked image received the attacks mentioned above.

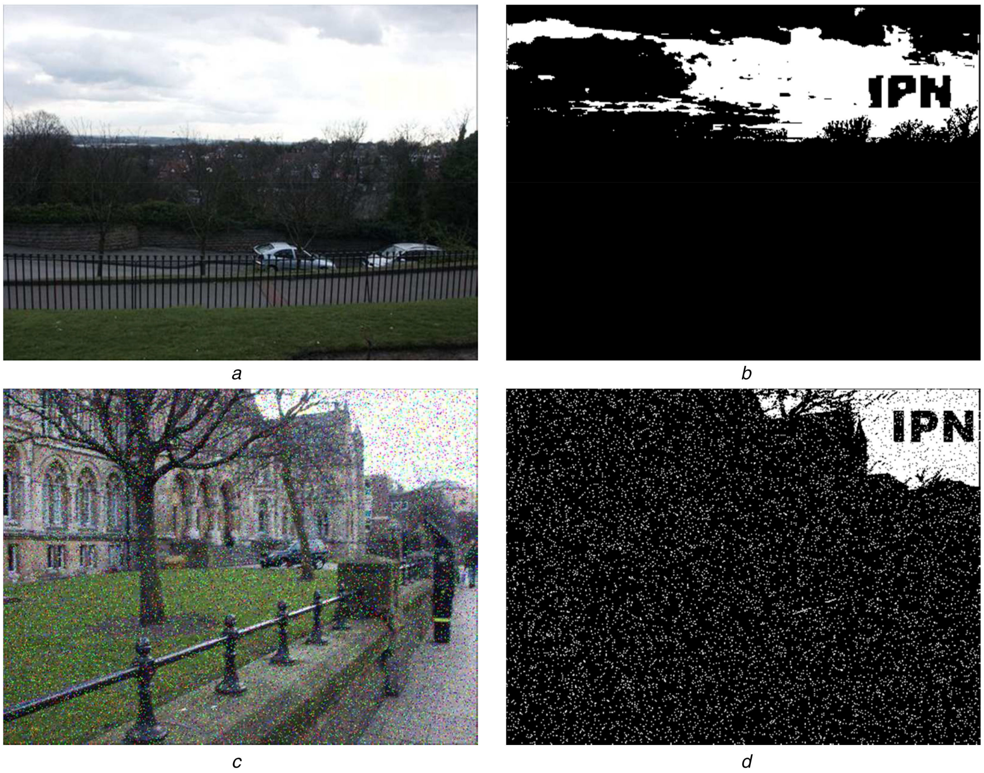

Fig. 10 *Watermark robustness*
(a) Watermarked and JPEG compressed image with QF 70, ***(c)*** Watermarked and impulsive noise contamination image with 10% of density, ***(b)***, ***(d)*** Watermark revelation versions of (a) and (c), respectively.

4.4 Performance in real application

In this section, we evaluate the performance of the proposed algorithm as an auxiliary information delivery system. For this purpose, we embed three visible watermark patterns given by Fig. 6 into all images of the dataset [16]. One of them is a QR code that provides URL and other two visible watermark patterns are letters and owner's logotype. For viewers who have interest in some auxiliary information about the visual contents, they can reveal the information clicking mouse button or touching screen, and for other viewers who do not have interest in any auxiliary information, the visible watermarks are totally imperceptible for them. Fig. 11 shows an example of this real application, being Fig. 11*a* the watermarked image with three visible watermark patterns. Figs. 11*b–d* are watermark revelation versions of Fig. 11*a*. In all cases, the revealed visible watermark pattern is very clear which allows obtaining the auxiliary information including its ownership information.

Fig. 12 shows the revealed QR codes from the watermarked image using two previous IVW algorithms [9, 10]. We can observe from this figure that the scheme [9] reveals a colour watermark pattern, while in the algorithm [10]; a grey-scale watermark pattern is exhibited. Since a common QR code reader cannot decode colour and grey-scale QR codes, the users cannot obtain auxiliary information from these QR codes. Therefore, in the previous algorithms [9, 10] some post-processing with crucial data, such as the mean value and the colour channel, are required to decode the revealed QR code.

Table 4 shows the global comparison among previously reported three algorithms and proposed one, considering several aspects in their practical use as the auxiliary information delivery system. In this table, the percentage of the first row means percentages of images suitable in all 1338 images in the dataset [16]. We can observe from this table that the proposed scheme is more suitable for this real application compared with previously proposed schemes [8–10].

5 Conclusion

This study presented an extended version of [10], in which we proposed an improved IVW algorithm based on the JND criterion, the invisible watermarking technique, and the binarisation operation. Unlike [8], in the proposed algorithm, the visible watermark pattern can be embedded imperceptibly into any class of images, such as plain images and textured images with any intensity level as shown in Fig. 7. In all cases, the revealed visible watermark is very clear. The proposed algorithm can embed multiple visible watermark patterns and reveal each watermark one by one as shown in Fig. 11. This capability of the proposed algorithm takes advantage of the application that provides auxiliary information, including ownership information, because the content owner can provide several types of auxiliary information depending on his/her interest.

In [9, 10], the crucial parameters, such as the mean value and the colour channel, are not shared among the watermark embedding and exhibition stages. It causes that in the watermark exhibition stage, the user must prove all possible parameters to reveal the visible watermark pattern, reducing its usability. Unlike [9, 10], in the proposed algorithm these crucial parameters are shared among the watermark embedding and exhibition stages through invisible watermark embedded randomly by the owner's secret key. Then in the proposed scheme, the user clicks only mouse button to obtain auxiliary information, revealing the visible watermark patterns.

The proposed algorithm provides higher robustness to the image compression, such as JPEG and JPEG2000 than [9, 10], as shown Figs. 8 and 9. It is important capability because almost all images and video are compressed based on one of these image compressors.

6 Acknowledgments

This work is supported by the National Science and Technology Council (CONACyT) of Mexico with the grant number CB-2014-20237925.

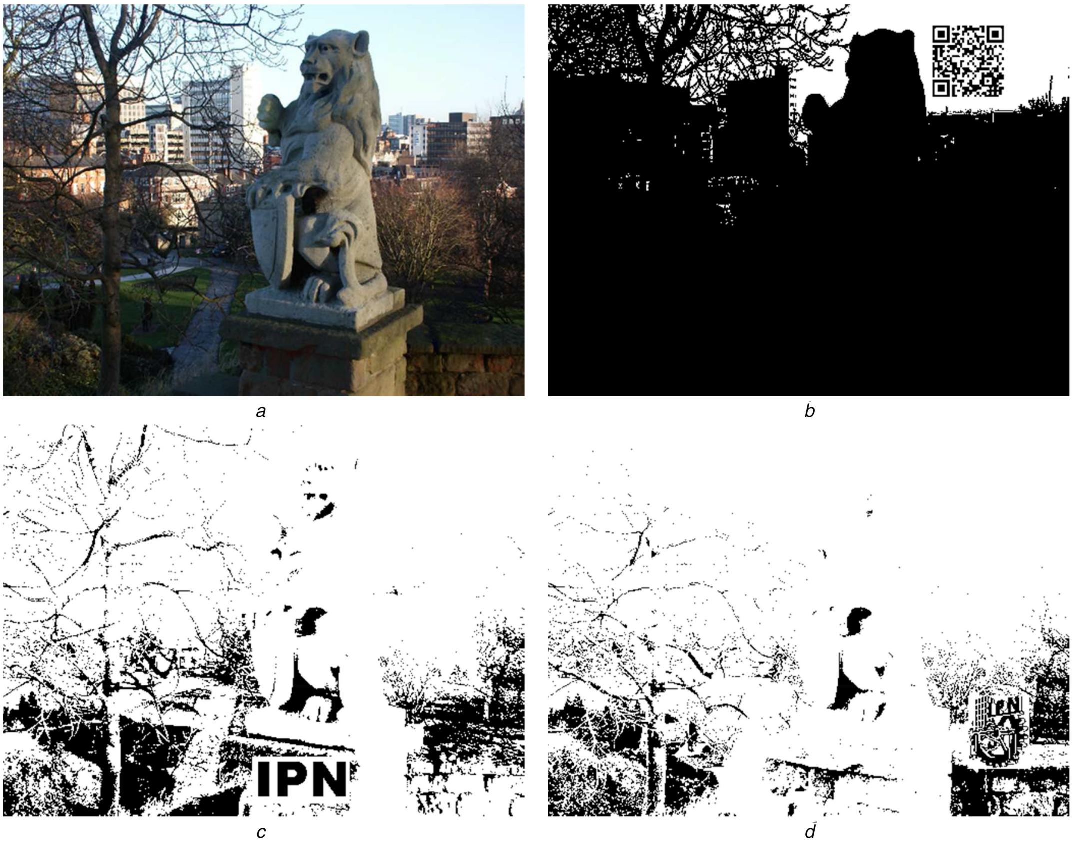

Fig. 11 *Examples of three visible watermarks, given by Fig. 6, embedded into the image*
(a) Watermarked image, ***(b)–(d)*** Watermark revelation version of (a)

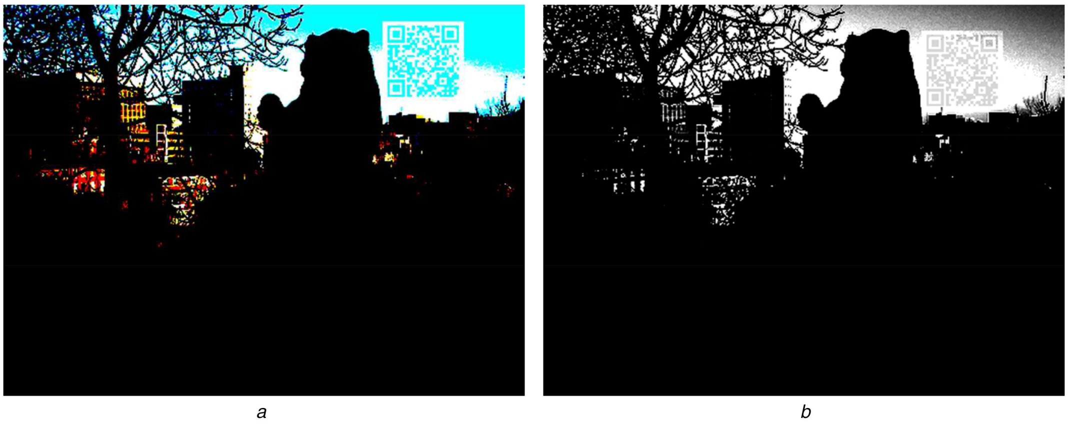

Fig. 12 *Visible watermark exhibition using*
(a) Lin's algorithm [9], ***(b)*** Juarez's algorithm [10], when the visible watermark pattern is the QR code

Table 4 Global comparison among previously proposed algorithms and proposed algorithm

	[8]	[10]	[9]	Proposed
universality	noonly images with a darkest plain region	noonly images with a plain region	yes	yes
	0.75%	44.6%	100%	100%
required side information for exhibition stage	no required	shift value	mean value colour channel	no required
revealed watermark	grey-scale	grey-scale	colour	binary
suitability for QR code	depend on contrast	depend on contrast	no	yes

7 References

[1] Langelaar, G., Setyawan, I., Lagendijk, R.: 'Watermarking digital image and video data. A state-of-the-art overview', *IEEE Signal Process. Mag.*, 2000, **17**, (5), pp. 20–46

[2] Cox, I., Kilian, J, Leighton, F., *et al.*: 'Secure spread spectrum watermarking for multimedia', *IEEE Trans. Image Process.*, 1997, **6**, (12), pp. 1673–1687

[3] Cedillo, M., García, F., Nakano, M., *et al.*: 'Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification', *J. Signal Image Video Process.*, 2015, **8**, (1), pp. 49–63

[4] Barni, M., Bartolini, F., Piva, A.: 'Improved wavelet-based watermarking through pixel-wise masking', *IEEE Trans. Image Process.*, 2001, **10**, (5), pp. 783–791

[5] Rosales, L., Cedillo, M., Nakano, M., *et al.*: 'Watermarking-based image authentication with recovery capability using halftoning technique', *Signal Process., Image Commun.*, 2013, **28**, pp. 69–83

[6] Arab, F., Abdullah, S.M., Hashim, S.M., *et al.*: 'A robust video watermarking technique for the tamper detection of surveillance systems', *Multimedia Tools Appl.*, 2016, **75**, (18), pp. 10855–10885

[7] Yaslan, Y., Gunsel, B.: 'An integrated on-line audio watermark decoding scheme for broadcast monitoring', *Multimedia Tools Appl.*, 2008, **40**, (1), pp. 1–21

[8] Huang, C.-H., Chuang, S.-C., Huang, Y.-L., *et al.*: 'Unseen visible watermarking: a novel methodology for auxiliary information delivery via visual contents', *IEEE Trans. Inf. Forensics Sec.*, 2009, **4**, (2), pp. 193–206

[9] Lin, P.-Y.: 'Imperceptible visible watermarking based on post camera histogram operation', *J. Syst. Softw.*, 2014, **95**, pp. 194–208

[10] Juarez, O., Fragoso, E., Cedillo, M., *et al.*: 'Improved unseen-visible watermarking for copyright protection of digital image'. Proc. Int. Workshop on Biometrics and Forensics, Coventry, UK, April 2017.

[11] Liu, A., Lin, W., Paul, M., *et al.*: 'Just Noticeable Difference for image with decomposition model for separating edge and textured regions', *IEEE Trans. Circuits Syst. Video Technol.*, 2010, **20**, (11), pp. 1648–1652

[12] Barker, C., Wiatrowski, M.: '*The age of Netflix: critical essays on streaming media, digital delivery and instant access*' (Mcfarland & Co., Inc. Pub., North Carolina, USA, 2017, 1st edn.)

[13] Podilchuk, C., Zeng, W.: 'Image-adaptive watermarking using visual model', *IEEE J. Sel. Areas Commun.*, 1998, **16**, (4), pp. 525–539

[14] Yu, P., Shang, Y., Li, C.: 'A new visible watermarking technique applied to CMOS image sensor'. Proc. SPIE Multispectral Image Acquisition, Processing and Analysis, Wuhan, China, October 2013, p. 8917

[15] Chen, B., Wornell, G.W.: 'Quantization index modulation: a class of provably good method for digital watermarking and information embedding', *IEEE Trans. Inf. Theor.*, 2001, **47**, (4), pp. 1423–1443

[16] Schaefer, G., Stich, M.: 'UCID – an uncompressed colour image database'. available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.8709&rep=rep1&type=pdf, accessed 1st July 2017.