


## Adaptive removable visible watermarking technique using dual watermarking for digital color images

Kevin Rangel-Espinoza<sup>1</sup> · Eduardo Fragoso-Navarro<sup>1</sup> ·  
Clara Cruz-Ramos<sup>1</sup> · Rogelio Reyes-Reyes<sup>1</sup>  ·  
Mariko Nakano-Miyatake<sup>1</sup> · Héctor M. Pérez-Meana<sup>1</sup>

Received: 8 November 2016 / Revised: 13 April 2017 / Accepted: 6 June 2017 /  
Published online: 19 June 2017  
© Springer Science+Business Media, LLC 2017

**Abstract** This paper proposes a removable visible watermarking system based on a dual watermark technique and blind removal. A visible watermark pattern is embedded in the cosine discrete transform (DCT) domain, taking into consideration the texture and luminance features of the watermark and host images to create a visible watermarked image. To prevent illegal visible watermark removal, the original watermark is embedded in an invisible manner in the visible watermarked image by employing the Quantization Index Modulation-Dither Modulation (QIM-DM) technique, thus ensuring that the original watermark cannot be obtained by malicious attacks. The visible watermark removal process is carried out using only the correct user's keys, without the need for additional information, such as the original watermark or the original host image, which allows a high-quality image to be obtained; however, if the user's keys used in the removal process are wrong, the visible watermarked image suffers higher distortion in its content, even in non-visible watermarked regions. The experimental results show that the proposed system outperforms previous related works in terms of blind removal, preservation of the quality of the unmarked recovered image, and higher visual degradation of the content in the recovered image if an illegal removal attempt is performed.

**Keywords** Removable visible watermarking · Copyright protection · Adaptive visible watermarking · Dual watermarking · Blind extraction · Image restoration

---

✉ Rogelio Reyes-Reyes  
rreyesre@ipn.mx

<sup>1</sup> Instituto Politécnico Nacional Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacan, Av. Santa Ana No. 1000, Col. San Francisco Culhuacan, Ciudad de México, Mexico

## 1 Introduction

There are a wide range of information transmitted through the Internet that requires special protection against unauthorized access and use. Some special cases such as medical data, databases [4], military content, e-government documents [5] among others, require appropriate protection. Among them, digital images are digital contents that receive frequently alteration by any user employing various software tools for photo editing, such as GIMP and Photoshop, which allows unauthorized users to appropriate digital content. Due to this problem, various visible watermark techniques have been used for copyright protection in digital images and videos; the main advantage of these techniques lies in the immediate identification of the digital content owner at first glance, which in turn represents its main disadvantage because the visible watermark obstructs the original content, degrading the quality of the host image [13]. However, in various applications, such as the distribution and sale of multimedia content and military, medical and satellite images, it is important to provide protected digital content; once the customer is convinced to purchase the unprotected content, the visible watermark can be removed at any time by an authorized user, and the multimedia content is restored to its original form.

Taking into consideration these problems, some removable visible watermarking systems have been proposed. However, they have two main limitations: the visible watermark transparency and visibility, and the quality of recovered image after the visible watermark is removed. They must maintain a balance among the perception of the content of the host image, the watermark visibility, and the robustness of the visible watermark to removal attempts, which are determined mainly by the embedded strength of the watermark. The embedding strength should be estimated by taking into consideration the characteristics of the host image and the watermark pattern based on the Human Visual System (HVS) [15].

Therefore, removable visible watermarking systems must satisfy the following features: a) restoration, i.e., an authorized user can remove the visible watermark without degrading the quality of the protected image, allowing the value of the digital content to be preserved; b) transparency, i.e., the embedded watermark should not seriously obscure or obstruct the original content of the host image; c) global protection, i.e., a visible watermark should protect the largest possible area of the host image; d) protection against illegal removal, i.e., if an unauthorized user tries to remove the visible watermark using incorrect keys, the protected image must suffer severe visual degradation throughout the image, keeping the visible watermark visually recognizable; e) multi-authorization, i.e., it is possible to generate different versions of the watermarked images using different user's keys even though the same watermark pattern and host image are used; and f) blind removal, i.e., the visible watermark should be removed only using the correct user's keys, without any additional information [17]. Considering the above-mentioned removable visible watermarking requirements, we propose in this paper a removable visible watermarking scheme based on a dual watermarking technique in which the watermark pattern is adaptively embedded in a visible manner in the host image considering the texture and luminance features of both images. Then, the original watermark is embedded in an invisible manner into the visible watermarked image using two user's keys, which prevents unauthorized users from obtaining it and thus attempting to remove the visible watermark.

The rest of this paper is organized as follows: in Section 2, prior works regarding visible watermark removal techniques will be introduced; the proposed removable visible watermarking system is presented in Section 3; the experimental results and discussion are shown in Section 4; and, finally, the conclusions are described in Section 5.

## 2 Prior works

In this section, previously reported removable visible watermarking algorithms are classified into two categories. The first category contains non-blind removal techniques, which require the original watermark or other additional information together with the user's keys to carry out the process of visible watermark removal [6, 9, 18, 19]; the second category contains blind removal techniques, which only require the user's keys to carry out the visible watermark removal because the original watermark was previously embedded invisibly in the marked content [3, 16]. In the following subsections, the two categories are analyzed.

### 2.1 Removable visible watermarking algorithms based on non-blind removal

Hu et al. proposed a removable visible watermarking algorithm in the DWT domain in which the user-key-controlled visible watermarked images are generated using different scaling and embedding factors in both the low-frequency sub-band and the high-frequency sub-band of the DWT decomposed host image. The different versions of the visible watermarked images are visually similar but numerically different [6]. Yang et al. proposed a removable visible watermarking algorithm in the DCT domain in which the embedding factors are estimated for each non-overlapped  $8 \times 8$  DCT block. To generate a user-key-controlled visible watermarked image, several versions of the watermark pattern are generated by employing a chaotic logistic map in which the user's key is used as a seed [19].

Lin et al. proposed a removable visible watermarking algorithm in the DWT domain in which the embedding strength of the watermark is computed according to the contrast of the host image and the watermark for each of the 4 sub-images is generated from the sub-sampling technique. The user's key that controls the visible watermark removal is generated from the pairs of sub-images employed in the watermark embedding that control the watermark strength [9]. Yang and Yin proposed a removable visible watermarking algorithm operating in Block Truncation Coding (BTC) compressed images. First, the original host image is compressed by the BTC technique, and then, the visible watermark pattern is embedded into the compressed image considering the two quantization levels of BTC. To prevent the illegal recovery of the host image, the original watermark is encrypted using chaotic maps, and the resulting image is later embedded in an invisible manner in the watermarked image [18].

The main disadvantage of the algorithms that belong to this category is the necessity of having the original watermark [6, 9, 19] or extra information [18]. Therefore, extra storage and additional bandwidth are required to save or transmit the original watermark or any additional information derived therefrom when an authorized user wants to remove the visible watermark. These processes involve associated risks, e.g., a malicious user could obtain the original watermark by accessing the storage medium, or it could be recovered through computer forensics techniques even if it has already been deleted from the storage device [12]. In section 4.4.1, we show that these algorithms [6, 9, 18, 19] allow a malicious user obtaining an illegally recovered image with minimal distortion using the illegally obtained original watermark and any user's keys.

### 2.2 Removable visible watermarking algorithms based on blind removal

Removable visible watermarking algorithms based on blind removal [3, 16] propose that the original watermark should be inserted invisibly within the visible watermarked image,

preventing unauthorized users from illegally obtaining the original watermark. Therefore, these algorithms only need the user's keys to perform the process of visible watermark removal, avoiding the need for extra storage and additional bandwidth.

Tsai and Chang proposed a reversible visible watermarking algorithm operating in the spatial domain. To recover the original host image, the watermark pattern is compressed by JBIG and embedded using a reversible watermarking technique. Because the amount of embedded data must be reduced due to the constraint of the reversible watermarking, this scheme can protect only part of the host image. To avoid illegal recovery of the host image, a noise pattern generated by the user's key is introduced to the visible watermark pattern [16].

Chen et al. proposed reversible visible watermarking scheme, in which reversible invisible watermark is embedded into the visible watermarked image using difference-expansion reversible embedding algorithm [3]. First, the invisible watermark is extracted from the visible watermarked image and is used to remove the visible watermark. Although the difference-expansion based reversible watermarking method provides total reversibility, the application of this method to any image causes under and over flow of pixel values range [0, 255], and as consequence, the total reversibility cannot be obtained. Additionally, since invisible watermarking is performed in spatial domain, this scheme is not robust to JPEG compression.

In section 4.4.2, the proposed system is compared with two removable visible watermarking systems based on blind removal [3, 16], and the numerical comparison results demonstrate the superior performance of the proposed system.

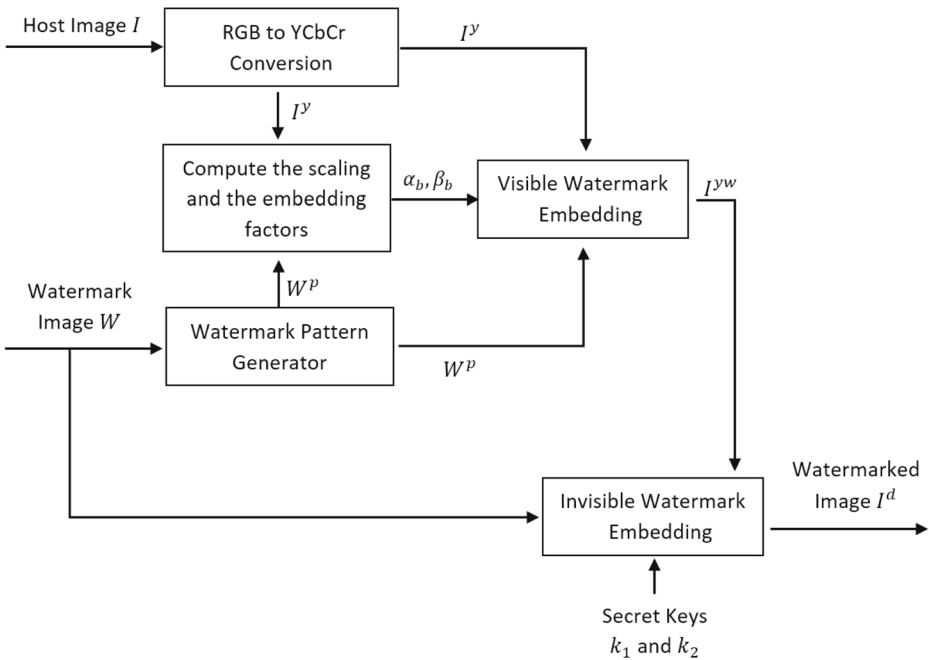
### 3 Proposed removable visible watermarking system

The proposed removable visible watermarking system consists of two stages: (I) the dual watermark embedding stage shown in Fig. 1 and (II) the visible watermark removal stage shown in Fig. 2.

#### Nomenclature

$I$	the host color image
$P^p$	the luminance component of the converted host image to YCbCr format
$W$	the binary watermark image
$W^p$	the binary watermark pattern generated from the binary watermark image
$P^{pw}$	the visible watermarked luminance component
$I^d$	the dual (visible and invisible) watermarked image
$I^{dy}$	the luminance component of the converted dual watermarked image to YCbCr format
$I^r$	the recovered unwatermarked image
$\alpha_b, \beta_b$	the scaling and embedding factors of the $b$ -th block, used for the adaptive visible watermarking
$f_i(I_b^y, W_b^p)$	the HVS sensibility function to the luminance between the host image and the watermark pattern of the $b$ -th block
$f_t(I_b^y, W_b^p)$	the HVS sensibility function to the texture between the host image and the watermark pattern of the $b$ -th block
$S$	the size of the original binary watermark $W$
$v^s$	the conversion into a 24 bit-sequence of $S$ , where the numbers of rows and columns are represented with the first and last 12 bits, respectively

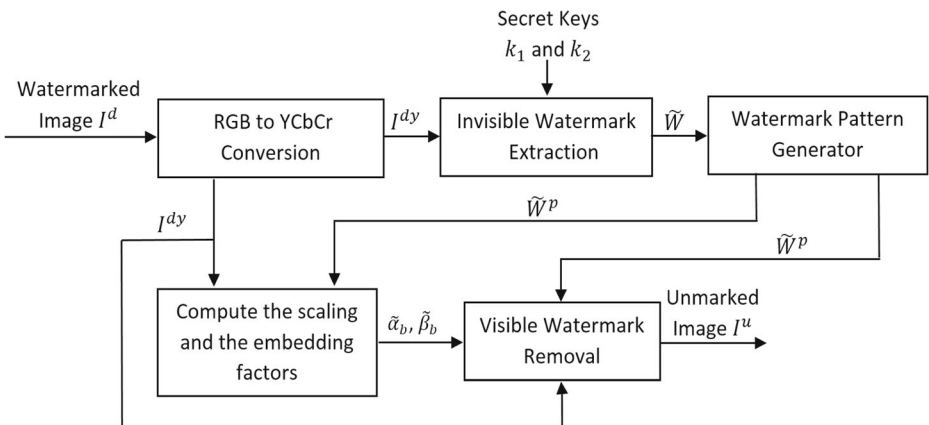




**Fig. 1** Block Diagram of Watermark Embedding

$v^W$  the binary sequence of the binary watermark image  $W$

In the first stage, the host color image  $I$  with RGB format is converted to YCbCr format, and then, the luminance component  $P^y$  is used for the visible watermark embedding. The watermark pattern  $W^p$  is generated from the binary watermark image  $W$ . The scaling ( $\alpha_b$ ) and embedding ( $\beta_b$ ) factors used for the adaptive visible watermarking scheme are computed, taking into account the HVS model to satisfy the previously mentioned contradictory requirements of visible watermarking. The watermark pattern  $W^p$  is embedded into the luminance component  $P^y$  to obtain a visible watermarked image  $P^{yw}$ . Additionally, the original watermark



**Fig. 2** Block Diagram of Visible Watermark Removal

image  $W$  is embedded invisibly into the visible watermarked luminance component  $I^{vw}$  using two secret keys, generating the dual watermarked image  $I^d$ .

The second stage consists of the extraction of the estimated invisible watermark  $\tilde{W}$  from the luminance component  $I^{dy}$  of the dual watermarked image  $I^d$  using the same two secret keys employed in the embedding process.

Next, the watermark pattern  $\tilde{W}^p$  is generated using the extracted watermark image  $\tilde{W}$ . Then, the estimated scaling and embedding factors,  $\tilde{\alpha}_b$  and  $\tilde{\beta}_b$ , are computed to remove the visible watermark from the luminance component of the dual watermarked image  $I^{dy}$ , obtaining the recovered image  $I^r$  without a visible watermark pattern.

### 3.1 Dual watermark embedding

As mentioned before, in the dual watermark embedding stage, both visible and invisible watermarks are embedded into the host color image.

#### 3.1.1 Visible watermark embedding

This procedure is composed of two modules. The first module consists of the design of the watermark pattern  $W^p$ , in which the original watermark  $W$  (Fig. 3(a)) is collocated several times to generate the watermark pattern  $W^p$  (Fig. 3(b)).

In the second module, the visible watermarking energy is determined adaptively according to each DCT block and expressed by two factors: the scaling factor  $\alpha_b$  and the embedding factor  $\beta_b$ . Using these factors, the visible watermark embedding is formulated as

$$I_b^{vw}(i, j) = \alpha_b I_b^y(i, j) + \beta_b W_b^p(i, j), \quad (1)$$

$i = 1, 2, \dots, 8, \quad j = 1, 2, \dots, 8, \quad b = 1, 2, \dots, B$

where  $I_b^y(i, j)$ ,  $W_b^p(i, j)$  and  $I_b^{vw}(i, j)$  are the  $(i, j)^{\text{th}}$  coefficients of the  $b^{\text{th}}$  DCT non-overlapped block of  $8 \times 8$  pixels of the luminance component of the host image, the watermark pattern and the luminance component of the watermarked image, respectively, and  $\alpha_b$  and  $\beta_b$  are scaling and embedding factors of the  $b^{\text{th}}$  DCT block.  $B$  is the total number of blocks [8].

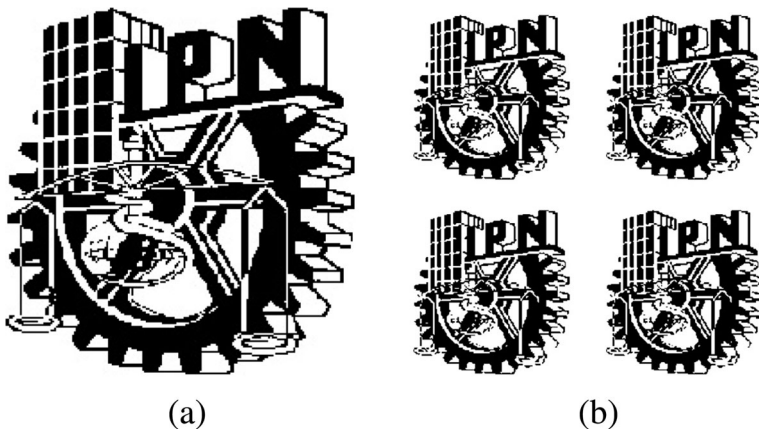


Fig. 3 Watermark Pattern Generator; a Original Watermark  $W$ , b Watermark Pattern  $W^p$

Among several proposals, the visible watermarking algorithm proposed by Yang et al. [19] is considered to be one of the most suitable algorithms from the watermark visibility and unobtrusiveness points of view. This algorithm also performs the visible watermark embedding in the DCT domain, obtaining the HVS sensitivities to the luminance and texture for each DCT non-overlapped block; using the DC and the AC coefficients of each block of the host image and watermark pattern. In [19], the scaling factor  $\alpha_b$  for the  $b^{\text{th}}$  block is calculated as the sum of the HVS sensitivities to luminance  $f_l(I_b^y, W_b^p)$  and texture  $f_t(I_b^y, W_b^p)$ , i.e.,

$$\alpha_b = f_l(I_b^y, W_b^p) + f_t(I_b^y, W_b^p), \quad (2)$$

The sensibility to luminance  $f_l(I_b^y, W_b^p)$  is measured using the value of the DC coefficient, considering that the value of the DC coefficient is proportional to the block luminance. First, the distributions of the DC coefficients of the host image and the watermark pattern are considered as normal distributions, which are

$$I_b^y(0, 0) \sim N(\mu_I, \sigma_I^2), \quad (3)$$

$$W_b^p(0, 0) \sim N(\mu_W, \sigma_W^2), \quad (4)$$

where  $I_b^y(0, 0)$  and  $W_b^p(0, 0)$  are the DC coefficients of the  $b^{\text{th}}$  DCT block;  $\mu_I, \mu_W, \sigma_I^2$  and  $\sigma_W^2$  are the means and variances of the respective DC coefficients. The sum of the DC coefficients of each block  $V_b = I_b^y(0, 0) + W_b^p(0, 0)$  also obeys a normal distribution,  $N(\mu_I + \mu_W, \sigma_I^2 + \sigma_W^2)$ , because the host image and the watermark pattern are independent. Taking into account that the HVS sensibility to luminance is higher in the mean luminance level and that it decays according to the increase or decrease of the luminance level [7],  $f_l(I_b^y, W_b^p)$  is given by

$$f_l(I_b^y, W_b^p) = \frac{1}{\sqrt{2\pi(\sigma_I^2 + \sigma_W^2)}} \exp\left\{-\frac{[V_b - (\mu_I + \mu_W)]^2}{2(\sigma_I^2 + \sigma_W^2)}\right\}, \quad (5)$$

The HVS sensibility to texture of the  $b^{\text{th}}$  block,  $f_t(I_b^y, W_b^p)$ , is calculated using the variances of the insignificant AC coefficients, which are various AC coefficients that become zero after quantization. Considering that  $\chi_b = \chi_I + \chi_W$  is the sum of variances of the insignificant AC coefficients of the  $b^{\text{th}}$  block of the host image and watermark pattern,  $f_t(I_b^y, W_b^p)$  is given by

$$f_t(I_b^y, W_b^p) = \frac{0.8 \times (\ln(\chi_b) - \ln(\chi_{\min}))}{\ln(\chi_{\max}) - \ln(\chi_{\min})} + 0.1, \quad (6)$$

where  $\ln(x)$  is the natural logarithm and  $\chi_{\max}$  and  $\chi_{\min}$  are the maximum and minimum variances of  $\chi_b$ . Finally, the scaling factor  $\alpha_b$  is the sum of (5) and (6), as shown by (2), and the embedding factor  $\beta_b$  is inversely proportional to  $\alpha_b$ , which is given by

$$\beta_b = 1 - \alpha_b, \quad (7)$$

These two factors are normalized within the ranges of [0.78, 0.87] and [0.15, 0.20], respectively. Finally, the visible watermarked image is generated by applying (1) with adaptively calculated and normalized scaling and embedding factors  $\alpha_b$  and  $\beta_b$ .

### 3.1.2 Invisible watermark embedding

One of the main advantages of the proposed system is the ability to remove the visible watermark through a completely blind process in which only two user’s keys  $k_1$  and  $k_2$  are required. This ability is accomplished by

an invisible watermarking scheme in which the original watermark  $W$  is embedded in the visible watermarked image  $P^w$ . Using the extracted invisible watermark, the visible watermark pattern  $W^p$  can be reconstructed, and then, the embedded visible watermark can be removed completely. The use of two secret keys,  $k_1$  and  $k_2$ , prevents illegal removal of the visible watermark. If an unauthorized user tries to remove the visible watermark, the watermarked image suffers severe distortion. It is worth noting that no additional information is required in this process besides the two secret keys. The block diagram of the invisible watermark embedding process is depicted in Fig. 4.

In the invisible watermark embedding process, we first obtain the size  $S$  of the original watermark  $W$ , and then,  $S$  is converted into a 24 bit-sequence,  $v^s$ , where the numbers of rows and columns are represented with the first and last 12 bits, respectively; later,  $v^s$  is divided into three 8-bit sequences  $v_x^s$ , where  $x = 1, 2, 3$ . For example, consider the size of the binary watermark  $W$  as  $S = 238 \times 238$ ; thus,  $W$  contains 56,644 bits and its binary notation  $v^s = '0000\ 1110\ 1110\ 0000\ 1110\ 1110'$ . The three 8-bit sequences are  $v_1^s = '00001110'$ ,  $v_2^s = '11100000'$  and  $v_3^s = '11101110'$ , respectively. Additionally, the binary sequence  $v^w$  of the binary watermark image  $W$  is divided into  $B-3$  sub-sequences with ‘ $n$ ’ bits, which are denoted by  $v_x^w$ , where  $x = 1, 2, \dots, B-3$ . The number of bits ‘ $n$ ’ for each sub-sequence  $v_x^w$  is determined by the remaining number of DCT blocks in the host image and the size of the watermark bit-sequence  $S$ , that is,  $n = S/(B-3)$ . To avoid any visual distortion caused by invisible watermarking, the length of each sub-sequence ‘ $n$ ’ must be less than 8.

The technique used for the invisible watermark embedding is performed by the Quantization Index Modulation–Dither Modulation (QIM-DM) [1] since this method achieves optimal robustness against amplitude scaling distortion [2]. QIM-DM is a

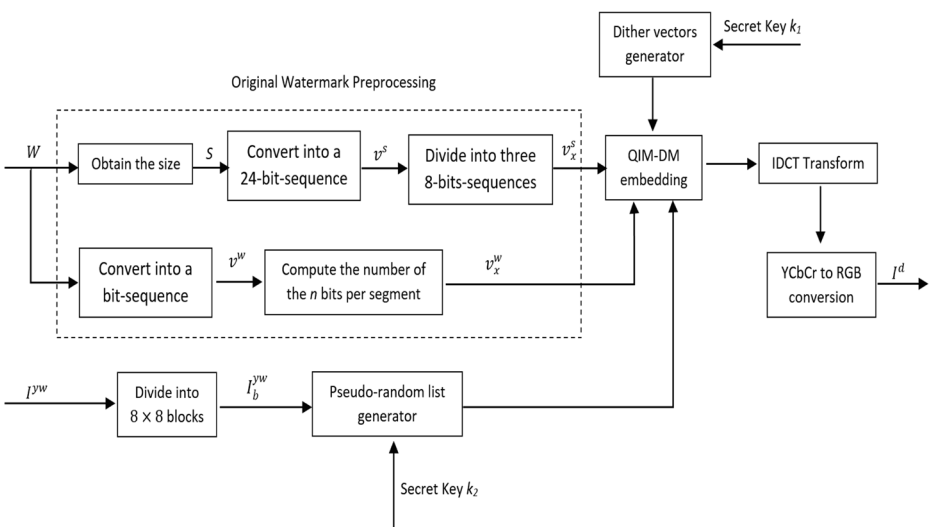


Fig. 4 Block Diagram of Invisible Watermark Embedding

technique based on host signal quantification with different quantifiers, where each of these represents a different watermark symbol. In this process, the dither vectors are generated pseudo-randomly using the secret key  $k_1$ . The QIM-DM technique used in the proposed scheme is given by

$$\tilde{X} = Q_{\Delta}(X + d(msg)) - d(msg) \tag{8}$$

where  $Q_{\Delta}(\cdot)$  is a quantifier with step-size  $\Delta = 12$ ,  $d(\cdot)$  is the dither,  $msg$  is the message bit to be embedded, and  $X$  and  $\tilde{X}$  are the original and watermarked data, respectively.

During the invisible watermark embedding process, the segments  $v_x^s$  are embedded into the first eight AC coefficients with the lowest frequency of the first three  $8 \times 8$  blocks of the luminance component of the visible watermarked image  $I_b^{vw}$ , where  $b = 1, 2, 3$ , using the QIM-DM technique defined by (8). Furthermore, the segments of  $n$  bits,  $v_x^w$ , are embedded into the remaining blocks of  $I_b^{vw}$  for  $b = 4, 5, \dots, B$ , which are selected pseudo-randomly using the second secret key  $k_2$ . The first  $n$  AC coefficients with the lowest frequency of each selected block are used to embed  $n$  bits of  $v_x^w$  using (8). Finally, the inverse DCT is performed for each block  $I_b^{vw}$ , and then, the YCbCr format is converted to the RGB format to obtain the dual watermarked color image  $I^d$ .

### 3.2 Visible watermark removal

#### 3.2.1 Invisible watermark extraction

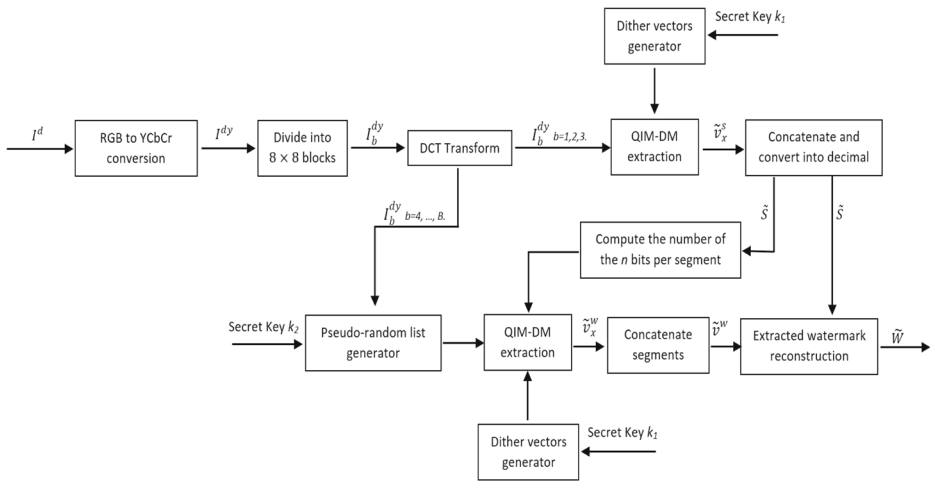
In the visible watermark removal process, the watermark pattern  $W^p$  must be reconstructed using an extracted version  $\tilde{W}$  of the original watermark  $W$ , as mentioned in sub-section 3.1.1. In this sub-section, the invisible watermark extraction process is explained in detail and shown in Fig. 5.

First, the dual watermarked image  $I^d$  is converted from RGB to YCbCr format, and then, the luminance component  $I^{dy}$  of the dual watermarked image is divided into non-overlapped  $8 \times 8$  pixel blocks and converted to the DCT domain. Afterward, the binary sequence  $\tilde{v}_x^s$ , corresponding to the size of the original watermark  $W$ , is extracted from the first eight AC coefficients with the lowest frequency of the first three DCT blocks  $I_b^{dy}$ , where  $b = 1, 2, 3$ , using the QIM-DM extraction technique [11] given by

$$\widehat{msg} = \operatorname{argmin}_{\sum_{i=1}^L} \left| \tilde{X} - Q_{\Delta}(\tilde{X} + d(msg)) - d(msg) \right| \tag{9}$$

where  $L$  is the length of the dither,  $Q_{\Delta}(\cdot)$  is the quantifier with step-size  $\Delta = 12$ ,  $d(\cdot)$  is the dither,  $\tilde{X}$  is the watermarked data, and  $msg$  and  $\widehat{msg}$  are the message bit embedded and the message bit extracted, respectively.

The three extracted binary bit-sequences  $\tilde{v}_x^s$  are concatenated and converted to a decimal value to obtain the size  $\tilde{S}$  of the watermark  $W$ ; later, the pseudo-random list used in the embedding process is obtained by the second secret key  $k_2$ . Using this pseudo-random list, the  $B-3$  DCT blocks  $I_b^{dy}$  are ordered correctly. Then, each bit-sequence  $\tilde{v}_x^w$  with length  $n$  is extracted from the first  $n$  AC coefficients with the



**Fig. 5** Block Diagram of Invisible Watermark Extraction

lowest frequency of each ordered DCT block  $I_b^{dy}$  by applying the QIM-DM watermark extraction given by (9). Finally, the reconstructed watermark  $\tilde{W}$  is obtained from the concatenated bit-sequence  $\tilde{v}^W$  according to the size  $\tilde{S}$ .

### 3.2.2 Visible watermark removal

Once the reconstructed watermark  $\tilde{W}$  is obtained, the estimated visible watermark pattern  $\tilde{W}^p$  is generated from  $\tilde{W}$ . This visible watermark pattern construction process is the same as that in sub-section 3.1.1. The scaling and embedding factors,  $\tilde{\alpha}_b$  and  $\tilde{\beta}_b$ , are estimated from the watermarked luminance channel  $I^{dy}$  and the reconstructed watermark pattern  $\tilde{W}^p$  using (2) and (7) as proposed by [19]. By solving equation (1) with  $I^{dy}$  as the host image,  $\tilde{W}^p$  as the watermark pattern, and the estimated factors  $\tilde{\alpha}_b$  and  $\tilde{\beta}_b$ , a recovered image  $I^u$  is obtained without a visible watermark pattern, which is given by

$$I_b^u(i, j) = \frac{I_b^{dy}(i, j) - \tilde{\beta}_b \tilde{W}_b^p(i, j)}{\tilde{\alpha}_b} \quad (10)$$

$i = 1, 2, \dots, 8; \quad j = 1, 2, \dots, 8; \quad b = 1, 2, \dots, B.$

It is worth noting that, although the estimated values of these two factors,  $\tilde{\alpha}_b$  and  $\tilde{\beta}_b$ , are slightly different from the original factors  $\alpha_b$  and  $\beta_b$ , the resulting recovered image has sufficiently high quality compared with the original one.

## 4 Results and discussion

This section presents experimental results of the proposed system, which were achieved using Matlab R2014b (8.4.0.150421) 64-bits installed in a PC with AMD FX-6300 @ 3.50 GHz CPU, 16 GB Dual-Channel DDR3 @ 666.5 MHz of RAM, and Microsoft Windows 10 Pro (64-bits), for several simulations using different host images and watermarks. To assess the

validity and performance of the proposed system, it is evaluated from the following points of view: a) dual watermarked image quality, quality of the recovered image and required computation time, b) security analysis of the proposed dual watermarking scheme, c) robustness against common attacks and d) comparison with previously proposed systems based on non-blind and blind removal. The proposed system has been evaluated using several binary watermark patterns, whose maximum size should be a quarter of the host image size, and several standard color and gray-scale host images of  $512 \times 512$ , such as “Lena”, “F-16” and “Baboon”. These images present different texture and luminance characteristics.

The following subsections describe in detail the four different evaluations of the proposed scheme mentioned above.

#### 4.1 Dual watermarked image quality, quality of the recovered image and required computation time

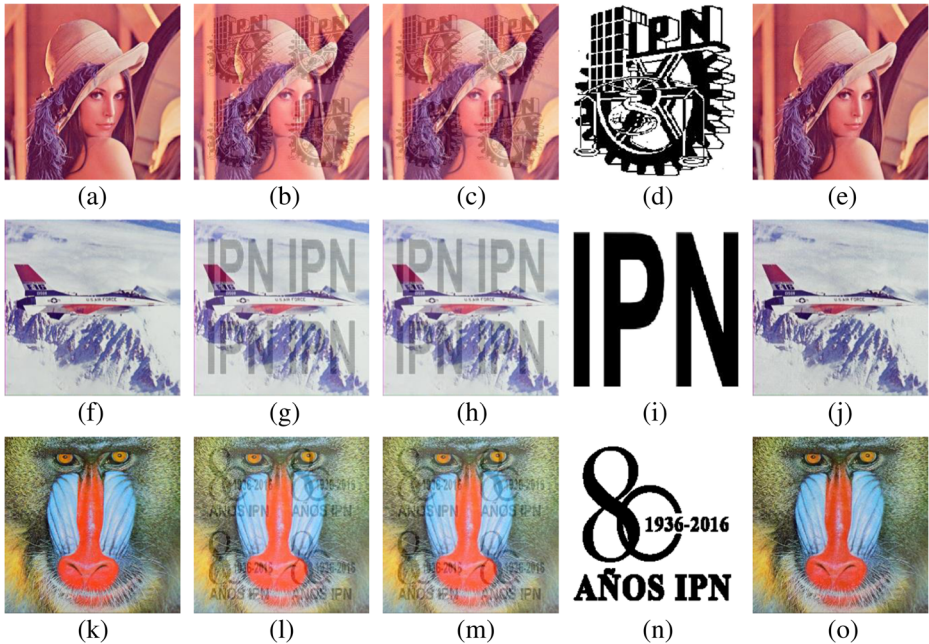
In this section, we evaluate the quality of dual watermarked image generated by the dual watermark embedding stage and the quality of recovered image through the visible watermark removal stage of the proposed dual watermarking system. The image quality is assessed by the objective evaluations, such as the peak-signal-to-noise ratio (PSNR) and the structural similarity index (SSIM), and subjective evaluation, such as the Mean Opinion Score (MOS). Also, we provide computational time required in both stages: the dual watermarking stage and the visible watermark removal stage.

Figure 6 shows the resulting images from each process of the proposed system together with the original versions. Fig. 6a, f and k are the original host images, Fig. 6b, g and l are the visible watermarked images, in which the adequate scaling and embedding factors calculated by [19] provide good characteristics of visible watermarked images, and Fig. 6c, h and m are the dual watermarked images (where the visible and invisible watermarks are embedded). These figures show that the invisible watermarking does not cause any visual distortion compared the visible watermarked images (Fig. 6b, g and l) with the dual watermarked images (Fig. 6c, h and m), obtaining average PSNR and SSIM values of 46.73 dB and 0.9982, respectively. The use of the QIM-DM technique in the DCT domain as an invisible watermarking algorithm provides watermark imperceptibility without sacrificing robustness. In the proposed system, the visible watermark embedding strength can be determined by varying the interpolated ranges for the scaling  $\alpha_b$  and embedding  $\beta_b$  factors, as mentioned in sub-section 3.1.1. If it is necessary to increase the visibility of visible watermark, then the embedding factor  $\beta_b$  must be increased, making the visible watermark more obtrusive; as a consequence of this, the details of the host image are not observed clearly.

Fig. 6d, i and n are the extracted binary watermarks, which are almost exactly the same as the embedded original binary watermarks with an average BER value of 0.000412. Finally, the recovered images by legal removal of the visible watermarks using the correct user’s keys are shown in Fig. 6e, j and o, which provide high visual quality in comparison with the original versions shown in Fig. 6a, f and k, respectively, obtaining average PSNR and SSIM values of 46.47 dB and 0.9773, respectively.

To evaluate the performance of the visible watermark removal process of the proposed system, we apply the MOS assessment. The MOS evaluation was applied to 200 persons regarding the quality of the legal recovered images compared with their corresponding original versions. Table 1 shows the criteria used for the MOS evaluation, and Table 2 shows the





**Fig. 6** **a**, **f** and **k** are the original host images; **b**, **g** and **l** are visible watermarked images; **c**, **h** and **m** are dual watermarked images; **d**, **i** and **n** are extracted binary watermarks; and **e**, **j** and **o** are legal recovered images without visible watermarks

average scores. The MOS evaluation results show that the legal recovered image of the proposed system is fairly good as judged by the human visual system.

Table 3 shows the average computational time required to perform the embedding and removal processes of the proposed system, obtained from 20 tests. The average times shown in Table 3 were obtained using an implementation of the Fast 2D–DCT [14] in Matlab, instead of using the traditional 2D–DCT provided by the development environment, reducing the processing time required for the watermarking embedding, extraction and removal processes. It is important to mention that these times can be further reduced if the Fast 2D–DCT is implemented using the parallel computing paradigm in multicore processors or in graphical processing units (GPU), which is feasible due to the non-dependence of data for its calculation.

### 4.2 Security analysis of the proposed dual watermarking scheme

As mentioned above, the proposed system allows a high-quality restoration of the recovered image without a visible watermark only if the user’s keys  $k_1$  and  $k_2$  are correct. Therefore,

**Table 1** MOS evaluation criterion

Score	Quality of recovered Image
5	Identical images
4	Visual degradation is minimal
3	Visual degradation is moderate
2	Visual degradation is higher
1	Not acceptable quality

**Table 2** Average scores obtained for the Mean Opinion Score (MOS) test

Recovered Image	Average Score
Lena	4.40
F-16	4.35
Baboon	4.42
Tiffany	4.38
Splash	4.30
House	4.20
Peppers	4.45

unauthorized users without the correct secret keys cannot obtain a high-quality recovered image; instead, they obtain a recovered image with high distortion that still shows the visible watermark pattern clearly. The first key  $k_1$  determines the dither vector generation, and the second key  $k_2$  determines the watermark extraction order; both keys are used during the embedding and extraction of the invisible watermark. Figure 7 shows some examples of the recovery process of the proposed system using an incorrect secret key  $k_j$ . Fig. 7a–i are the original host images; Fig. 7b–j are the correspondent dual watermarked images; Fig. 7c–k are the extracted watermark patterns using different incorrect secret keys  $k_1$ ; and Fig. 7d–l are the illegally recovered images.

The secret key  $k_2$  determines the order in which the watermark bit-sequences are extracted; therefore, if the key  $k_2$  used in the visible watermark removal process is incorrect, the reconstructed binary watermark is disordered. Figure 8 shows the visible watermark removal process with an incorrect secret key  $k_2$ . Although in some cases, depending on the incorrect key  $k_2$  selected, the extracted binary watermark is similar to the original one shown in Fig. 8c–k, the recovered images suffer distortion and still show the visible watermark pattern clearly, as shown in Fig. 8d–l. Figure 9 shows the illegally recovered images using two incorrect keys  $k_1$  and  $k_2$ . Table 4 shows the average PSNR and SSIM values for the recovered images using one or two incorrect keys for color host images.

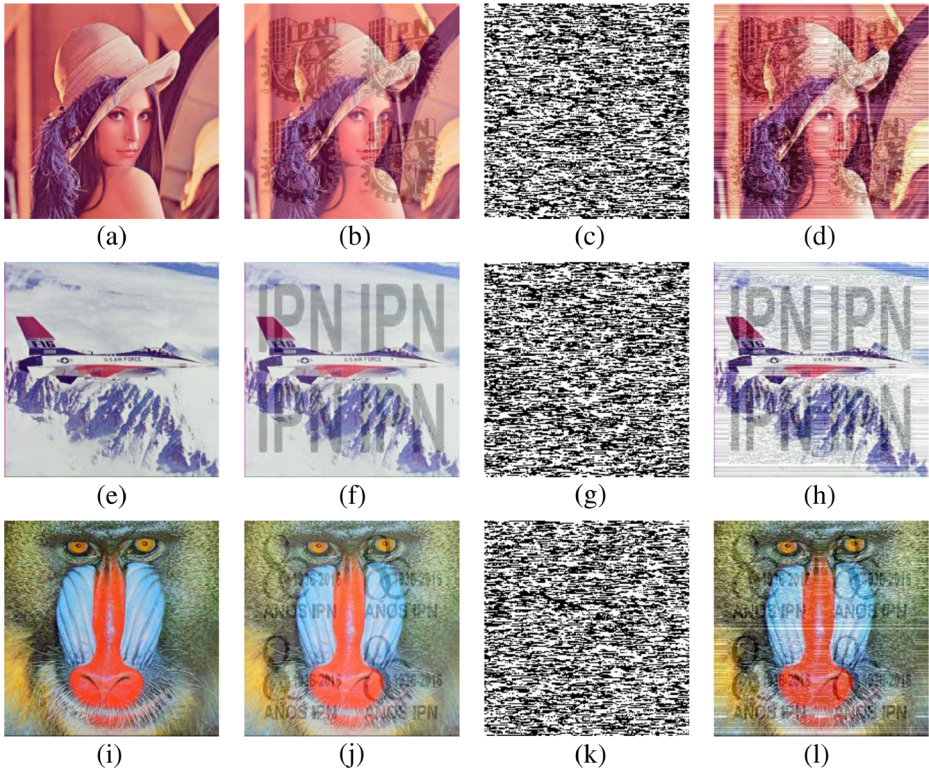
From Fig. 9 and Table 4, we can observe that the illegal removal of the visible watermark pattern using two incorrect secret keys generates distorted images that still have a clear visible watermark pattern. This means that any illegal visible watermark removal, without knowledge of one or both of the secret keys  $k_1$  and  $k_2$ , will be a failure. As a consequence, rightful ownership can be protected.

Table 5 shows the average PSNR and SSIM values for the recovered images  $I''$  obtained in legal and illegal visible watermark removal processes using different binary watermark patterns and color host images. This table demonstrates the effectiveness of the proposed system in both legal and illegal removal processes.

The proposed algorithm satisfies the multi-authorization requirement in which the same host image with the same visible watermark pattern could be distributed to multiple users. However, an authorized user must only recover his own high-quality image without a visible watermark using the assigned correct secret keys. Fig. 10a, b, e, and f show two visible

**Table 3** Computation time required for the watermarking embedding and removal processes

Total Time (sec)	
Embedding	Removal
1.98	1.84



**Fig. 7** Visible watermark removal process with an incorrect key  $k_l$ . Images **a**, **e** and **i** are the host images; **b**, **f** and **j** are dual watermarked images; **c**, **g** and **k** are binary watermark extracted images; and **d**, **h** and **l** are illegally recovered images with the incorrect key  $k_l$

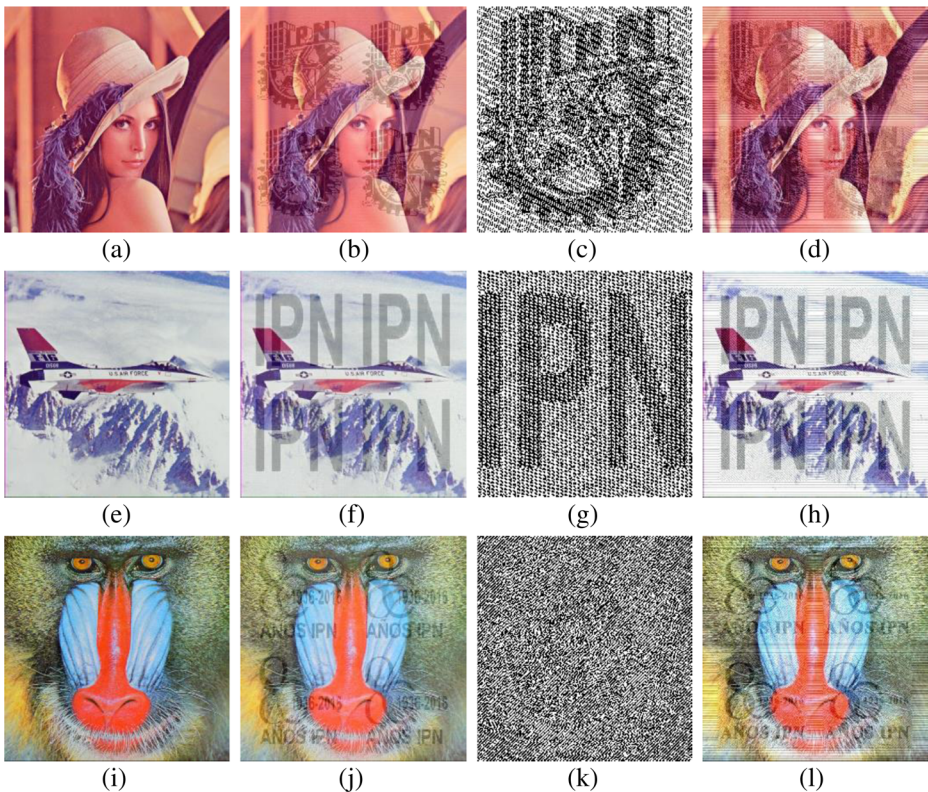
watermarked versions of the same host image with the same watermark pattern; however, they were watermarked with different user's keys. Fig. 10a uses  $k_1 = 12$  and  $k_2 = 23$ , Fig. 10b uses  $k_1 = 47$  and  $k_2 = 78$ , Fig. 10e uses  $k_1 = 778$  and  $k_2 = 547$ , and Fig. 10f uses  $k_1 = 458$  and  $k_2 = 874$ . Fig. 10c and d are the recovered images obtained from 10a and b after exchanging user's keys between them. In a similar case, Fig. 10g and h are the recovered images obtained from 10e and f after exchanging user's keys between them.

The results obtained in Fig. 10 demonstrate that it is possible to offer the same host image with the same embedded visible watermark to different users assigning their own secret keys. Therefore, it is impossible to illegally remove the visible watermark of a protected image using another user's keys, although the watermarked images appear visually identical.

#### 4.3 Robustness of the proposed system against common attacks

This section briefly discusses the performance of the proposed system against some practical attacks such as image processing software, collusion and JPEG compression. The image processing software attack is based on the use of digital image editing tools such as Photoshop® or Gimp®, which have numerous techniques for retouching and restoring images (smoothing, sharpening, filtering, among others). The success of this attack depends directly on the human ability to use the image editing tools and the level



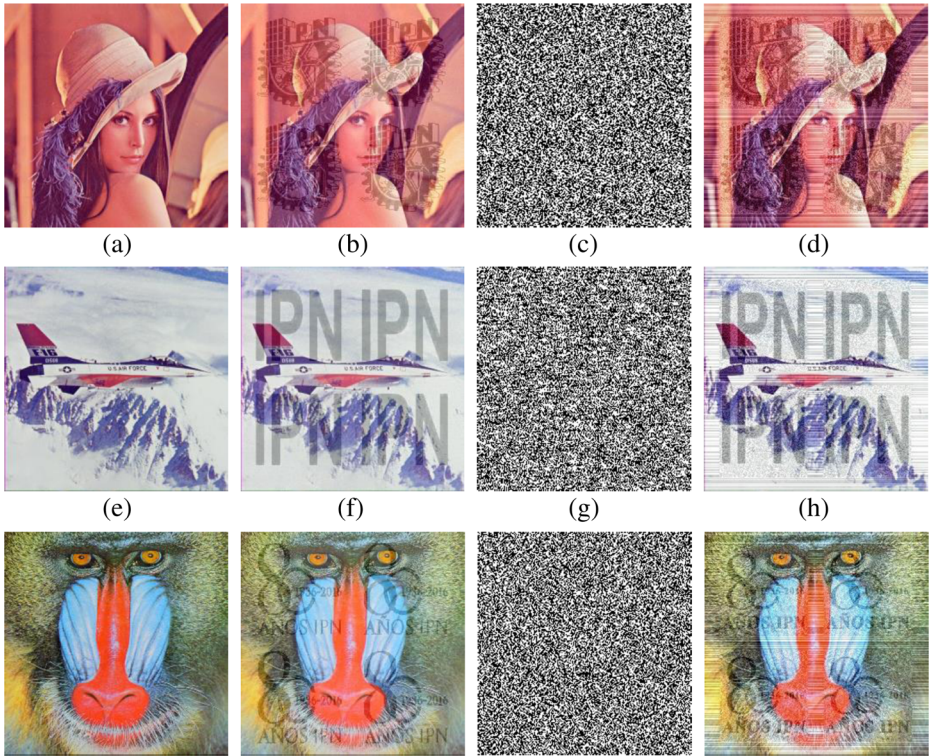


**Fig. 8** Watermark removal process with an incorrect key  $k_2$ . Images **a**, **e** and **i** are the host images; **b**, **f** and **j** are dual watermarked images; **c**, **g** and **k** are binary watermark extracted images; and **d**, **h** and **l** are illegally recovered images with the incorrect key  $k_2$

of expertise in image editing of the person who makes the edition. Figure 11 shows the results after performing  $3 \times 3$  median filtering,  $3 \times 3$  image smoothing and Laplacian image sharpening to the dual watermarked images for the image processing software attack.

The results shown in Fig. 11 demonstrate that these attacks do not completely remove the visible watermark. In order to obtain a visually acceptable image without visible watermark, it is important to invest considerable time and effort to correct all details; even so, it will be difficult to obtain a high quality image quite similar to the original host image.

Another common attack used to attempt to eliminate or degrade a watermark from the host image, is a collusion attack, in which an attacker obtains several different copies of watermarked images, or several different pieces of protected images with the same watermark and combine all the copies to remove all different watermarks [10]. The success of this attack depends directly on how many clients requesting for the same visible watermarked image, get their differently marked versions together and collude them in order to remove or weaken the watermark. Fig. 12 shows the performance of the proposed system against collusion attacks by averaging 10, 20 and 40 different versions of dual watermarked images using different user's keys.



**Fig. 9** Watermark removal process with incorrect keys  $k_1$  and  $k_2$ . Images **a**, **e** and **i** are the host images; **b**, **f** and **j** are dual watermarked images; **c**, **g** and **k** are binary watermark extracted images; and **d**, **h** and **l** are illegal recovered images with the incorrect keys  $k_1$  and  $k_2$

From Fig. 12, we can observe that the proposed system can resist this attack although the attacker has a considerable number of watermarked images. The visible watermark is still perceptible since the watermark is embedded adaptively in the host image.

Nowadays, most images are transmitted and stored through the Internet, so it is necessary to reduce as much as possible the amount of data using compression algorithms, such as JPEG; this kind of lossy image compressor is considered as unintentional attack, where the quality of the compressed image depends directly on the amount of information that is lost. Therefore, it is necessary to verify that the proposed system is robust against this compression scheme, since most of the digital images are in this format.

Figure 13 shows the results obtained by the legally visible watermark removal process applied to different dual watermarked images compressed with quality factors (QF) in the

**Table 4** Average PSNR and SSIM values for illegally recovered images with incorrect keys for color host images

	Wrong key ( $k_1$ ) PSNR(dB) / SSIM	Wrong key ( $k_2$ ) PSNR(dB) / SSIM	Wrong keys ( $k_1$ and $k_2$ ) PSNR(dB) / SSIM
Lena	16.84 / 0.6215	18.12 / 0.6730	16.48 / 0.6146
F-16	17.23 / 0.6491	18.94 / 0.7178	17.45 / 0.6802
Baboon	16.34 / 0.6378	17.73 / 0.6540	16.11 / 0.6138



**Table 5** Average PSNR and SSIM values for legally and illegally recovered images using different binary watermark patterns for color host images

	Legal Removal PSNR(dB) / SSIM	Illegal Removal PSNR(dB) / SSIM
Lena	46.06 / 0.9982	16.84 / 0.6146
F-16	46.83 / 0.9984	17.45 / 0.6802
Baboon	47.30 / 0.9980	16.11 / 0.6138

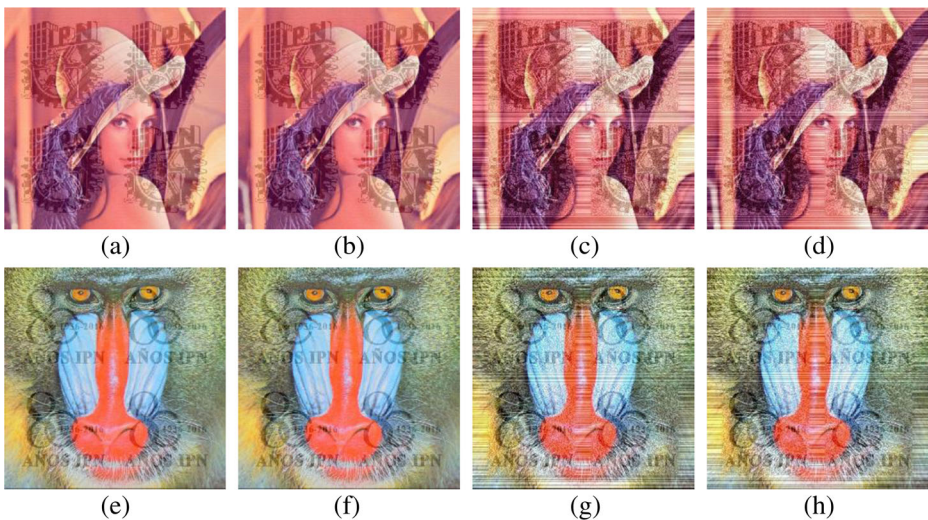
range from 70 to 95. Fig. 13a–m are the dual watermarked compressed images with quality factors 95, 85, 80, 75, 70 respectively; Fig. 13b–n are the extracted binary watermark and Fig. 13c–o are the recovered images after the visible watermark removal process for the different quality factors.

Table 6 shows the average PSNR and SSIM values for the recovered unmarked images and the extracted binary watermarks versus the original host image and the original binary watermark respectively, for different quality factors.

As we can observe in Fig. 13 and Table 6, the proposed system is robust to JPEG compression with the quality factors within a range of 100–80. This ensures that the protected images can be storage, transmitted or shared through the Internet, and later it is possible to remove the visible watermark, obtaining a high quality unmarked image.

#### 4.4 Comparison with related well-known systems based on non-blind and blind removal

The proposed system was compared with other existing removable visible watermarking systems based on non-blind and blind removal schemes in the literature [3, 6, 9, 16, 18, 19] from the point of view of visible watermark removal performance, in which the recovered image quality in legal and illegal processes was evaluated.



**Fig. 10** Effectiveness of the proposed system for multi-authorization requirements. Images a, b and e, f are different watermarked versions produced with different user's keys; c, d and g, h are the recovered images after exchanging the user's keys of a, b and e, f



**Fig. 11** Images obtained after performing some common image processing techniques to the dual watermarked images. Images **a**, **b** and **c** show the results for the  $3 \times 3$  median filtering,  $3 \times 3$  image smoothing and Laplacian image sharpening attacks respectively

The evaluations were performed using the same host (gray-scale) and the same watermark (binary) images because the previous schemes do not work with color images.

#### 4.4.1 Performance analysis of the removable visible watermarking algorithms based on non-blind removal

As previously mentioned in section 1, in any removable visible watermarking scheme, the images obtained by an illegal removal process should present a considerable distortion, and additionally, the visible watermark pattern must remain in the images. Considering the above, algorithms [6, 9, 18, 19] do not satisfy this requirement because the images obtained by an illegal removal process, shown in Fig. 14d–p, are sufficiently clear to observe the contents of the host image. Additionally, the visible watermark pattern is removed from the images. This means that any unauthorized person can remove visible watermark from the watermarked image using any incorrect user's keys and the watermark pattern obtained illicitly by the methods described in section 2.1, invalidating the ownership of the images.

Figure 14 shows legally and illegally recovered images obtained by the visible watermark removal processes of four previously proposed non-blind removal schemes. Fig. 14a–m are the host images, and Fig. 14b–n represent the visible watermarked images. In these figures, the visible watermark is observed with different gray-scales, depending on the method used to



**Fig. 12** Images obtained after performing the collusion attack. Images **a**, **b** and **c** show the results by averaging 10, 20 and 40 different versions of dual watermarked images respectively



embed the visible watermark. However, it is worth noting that, in all cases, the binary watermark patterns are visually recognizable and non-obtrusive. Fig. 14c–o are legally recovered images, while Fig. 14d–p are the illegally recovered images.

Table 7 shows the average PSNR and SSIM values for the recovered images obtained in legal and illegal visible watermark removal processes. According to the results observed in Table 7, the methods proposed by [6, 9, 18, 19] show similar results in all analyzed aspects. The main disadvantage of these systems is that they do not provide a blind removal process for the visible watermark because the original watermark image or additional information derived from it for the visible watermark removal process is necessary, which obviously impedes correct ownership protection of the host image; moreover, unauthorized users, using any incorrect user keys and the illicitly obtained watermark pattern, can obtain an illegally recovered image with high quality, as shown by Fig. 14d, h, and l and Table 7.

Additionally, the proposals [6, 9, 18, 19] do not achieve the multi-authorization requirement because it is possible

for any user who possesses the same watermark pattern to remove the visible watermark of any watermarked

image using that watermark pattern by employing any user keys.

#### 4.4.2 Performance analysis of the removable visible watermarking algorithms based on blind removal

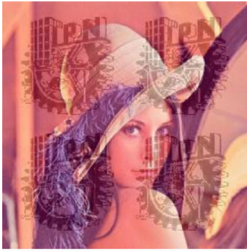
For the removable visible watermarking algorithms based on completely blind removal [3, 16], the original watermark is embedded invisibly into the visible watermarked image, which allows the visible watermark removal process in a completely blind manner, only using the correct user's keys. This provides a secure visible removal process, preventing any illicit attempt to obtain the original watermark pattern for illegal use, and permits the multi-authorization requirement to be achieved.

The proposed system was compared with other existing removable visible watermarking systems based on completely blind removal schemes in the literature [3, 16] from the point of view of visible watermark removal performance, in which the recovered image quality in legal and illegal processes was evaluated. Originally, the algorithm proposed by [16] embeds a single image as a visible watermark that is a quarter of the size of the host image; however, this proposal is modified slightly to compare both algorithms under the same conditions, i.e., the watermark is collocated several times to generate a pattern, as shown in section 3.1.1

Figure 15 shows legally and illegally recovered images for two different watermark patterns obtained by the visible watermark removal process of the previously proposed schemes [3, 16] and the proposed system. Fig. 15 a1, b1, c1, d1, e1 and f1 are the host images, and Fig. 15a2, b2, c2, d2, e2 and f2 are the dual watermarked images. In these figures, the invisible watermark is imperceptible to the naked eye. Fig. 15 a3, b3, c3, d3, e3 and f3 are legally recovered images, and Fig. 15 a4, b4, c4, d4, e4 and f4 are the illegally recovered images using incorrect user's keys, while Fig. 15 a5, b5, c5, d5, e5 and f5 are close-ups of the illegally recovered images.

Table 8 shows a performance comparison among related works [3, 16] and the proposed system.

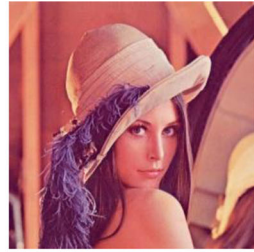
According to Fig. 15 and Table 8, both proposals [3, 16] are not robust to the JPEG compression, which may be serious defect of these methods, since JPEG is one of the most popular image compression format for transmission and storage on the Internet. Another



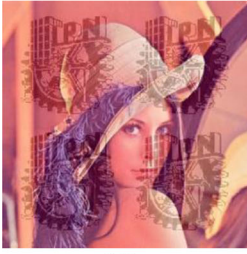
(a)



(b)



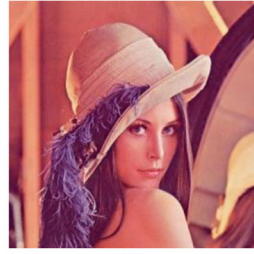
(c)



(d)



(e)



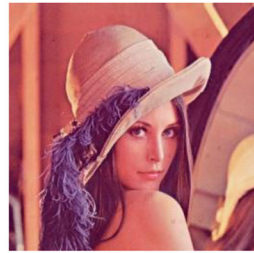
(f)



(g)



(h)



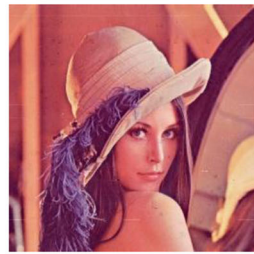
(i)



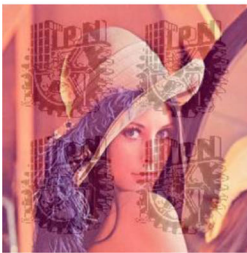
(j)



(k)



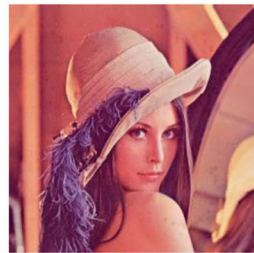
(l)



(m)



(n)



(o)

**Fig. 13** Effectiveness of the proposed system against JPEG compression. The images **a, d, g, j** and **m** represents the compressed dual watermarked image with quality factors 95, 85, 80, 75 and 70 respectively; the images **b, e, h, k** and **n** shows the extracted binary watermark and finally, the images **c, f, i, l**, and **o** shows the recovered image

disadvantage of methods [3, 16], is that the visible watermark pattern related to the owner's logotype is not visually recognizable in the illegally recovered images, as we can observe in Fig. 15 a4, b4, d4 and e4, which means that the ownership over the image cannot be proved any longer.

In the proposed system, the original watermark is embedded invisibly into the visible watermarked image using two user's keys, which allows the visible watermark removal process to proceed in a completely blind manner. For the visible watermark removal process, if the right user's keys are used to remove the visible watermark, the resultant recovered image provides very high quality compared with the original host image (approximately PSNR 47 dB and SSIM 0.9923) even if the watermarked image has been compressed by JPEG compressor. Alternately, if any incorrect keys are used in the removal process, the recovered image suffers considerable distortion in whole image (approx. PSNR 16.82 dB and SSIM 0.2455); however, the visible watermark pattern related to the owner's logotype remains visually recognizable, as shown in Fig. 15 c4, c5, f4 and f5.

## 5 Conclusions

This paper presents a removable visible watermarking scheme for color and gray-scale digital images performing in the DCT domain. We used Yang's algorithm [19] as the visible watermark embedding process, which adaptively determines the scaling and embedding factors, taking account of the luminance and texture features of the host and the watermark images.

The removal of the visible watermark is carried out using an invisible watermarking technique based on QIM-DM. This process is carried out through a completely blind process, in which no additional information, such as the original watermark or the original host image, is required. Only the correct user's secret keys are required to completely remove the visible watermark and generate the recovered image. Moreover, the proposed system allows multiple authorizations for a unique pair of host and watermark images, improving the viability and flexibility of the system.

**Table 6** Average PSNR and SSIM values for the recovered unmarked images and the extracted binary watermark for different quality factors

Quality Factor	Extracted Binary Watermark PSNR(dB) / SSIM	Recovered Unmarked Image PSNR(dB) / SSIM
95	47.45 / 0.9822	45.54 / 0.9812
90	44.32 / 0.9607	43.98 / 0.9670
85	37.78 / 0.9347	39.32 / 0.9367
80	33.21 / 0.8994	37.57 / 0.9122
75	29.34 / 0.8501	33.61 / 0.8957
70	27.74 / 0.8398	30.17 / 0.8714



**Fig. 14** The first column represents the host image, the second column the watermarked image, the third column the legally recovered image and, finally, the fourth column the illegally recovered image. **a-d** Hu’s system, **e-h** Yang’s system, **i-l** Lin’s system, and **m-p** Yang’s system

**Table 7** Comparisons among related works based on non-blind removal, considering the average PSNR (dB)/SSIM values for different legally and illegally recovered images

	[6] PSNR (dB)/SSIM	[19] PSNR (dB)/SSIM	[9] PSNR (dB)/SSIM	[18] PSNR (dB)/SSIM
Legal Removal (correct user keys)	44.15 / 0.9782	40.75 / 0.9658	55.92 / 0.9932	32.72 / 0.5784
Illegal Removal (incorrect user keys)	38.84 / 0.9579	34.09 / 0.9223	46.09 / 0.9760	14.84 / 0.1974





**Fig. 15** The first column represents the host images, the second column the dual watermarked images, the third column the legally recovered images, the fourth column the illegally recovered image and, finally, the fifth column close-ups of the illegally recovered images. **a1-a5, d1-d5** show the results obtained by [16], **b1-b5, e1-e5** show the results obtained by [3], and **c1-c5, f1-f5** show the results obtained by the proposed system

In the visible watermark removal process, only users who possess the correct keys can remove the visible watermark, obtaining a very high-quality recovered image without the

**Table 8** Comparisons among related works and the proposed system considering the average PSNR(dB)/SSIM values for different legally and illegally recovered images

	[16] PSNR (dB)/ SSIM	[3] PSNR (dB)/ SSIM	Proposed System PSNR (dB)/ SSIM
Legal Removal (correct user keys)	55.67 / 0.9987	43.92 / 0.9988	47.24 / 0.9923
Legal Removal after JPEG Compression QF = 90	24.94 / 0.6015	21.35 / 0.5420	42.20 / 0.9810
Illegal Removal (incorrect user keys)	25.98 / 0.7036	20.35 / 0.5225	16.82 / 0.2455
Multi-authorization	Yes	Yes	Yes

watermark. While some unauthorized persons may try to remove the watermark using any incorrect keys, the resultant image suffers considerable distortion and the visible watermark pattern remains visually recognizable, which allows the owner to prove his or her ownership over the image after this intentional attack.

The performance of the proposed system is compared with six removal visible watermarking systems reported in the literature. The comparison results show that the proposed system outperforms the previously proposed schemes in several aspects, such as the following: 1. the visible watermark removal process is carried out in a completely blind manner, in which no additional information is required; 2. the recovered image obtained by the legal removal process presents very high quality compared with the original host image; 3. the resultant image obtained by any illegal removal process suffers distortion, whereas the visible watermark still remains visibly recognizable; 4. The proposed algorithm is robust to several intentional and unintentional attacks including JPEG compression and 5. the proposed scheme provides multi-authorization.

As a future work, we will consider the development of a more sophisticated visible watermarking algorithm, considering more complex HVS features and the Just Noticeable Distortion (JND) model.

**Acknowledgements** Authors thank the National Council of Science and Technology of Mexico (CONACyT) and IPN for financial support to carry out this work.

## References

1. Chen B, Wornell GW (1998) Digital watermarking and information embedding using dither modulation, Workshop on Multimedia Signal Processing pp 273–278
2. Chen B, Wornell GW (2001) Quantization index modulation methods for digital watermarking and information embedding of multimedia. *J VLSI Sig Proc Syst Sig, Image and Video Technol* 27:7–33
3. Chen CC, Tsai YH, Yeh HC (2016) Difference-expansion based reversible and visible image watermarking scheme. *Multimed Tools Appl* 76:8497–8516
4. Farfoura ME, Horng SJ, Lai JL, Run RS, Chen RJ, Khan MK (2012) A blind reversible method for watermarking relational database on a time-stamping protocol. *Expert Syst Appl* 39:3185–3192
5. Horng SJ, Rosiyadi D, Fan P, Wang X, Khan MK (2014) Adaptive watermarking scheme for e-government document image. *Multimed Tools Appl* 72:3085–3103

6. Hu Y, Kwong S, Huang J (2006) An algorithm for removable visible watermarking. *IEEE Trans Circuits Syst Video Technol* 16:129–133
7. Huang BB, Tang SX (2006) A contrast-sensitive visible watermarking scheme. *IEEE Multimedia* 13:60–66
8. Kankanhalli MS, Ramakrishnan KR (1999) Adaptive visible watermarking of images. *International Conference on Multimedia Computing and Systems*, Florence, Italy, pp 568–573
9. Lin PY, Chen YH, Chang CC, Lee JS (2013) Contrast-adaptive removable visible watermarking (CARVW) mechanism. *Image Vis Comput* 31:311–321
10. Matheson LR, Mitchell SG, Shamoan TG, Tarjan RE, Zane F (1998) Robustness and security of digital watermarks, *International Conference on financial cryptography*. *Lect Notes Comput Sci* 1465:227–240
11. Phadikar A, Maity SP (2010) An efficient m-ary QIM data hiding algorithm for the application to image error concealment. *Int J Netw Security Appl* 2:169–188
12. Poisel R, Tjoa S (2011) Forensics investigations of multimedia data: a review of the state-of-the-art, sixth *International Conference on IT security incident management and IT forensics*, pp 48–61
13. Qi H, Zheng D, Zhao J (2008) Human visual system based adaptive digital image watermarking. *Signal Process* 88:174–188
14. Strang G (1999) The discrete cosine transform. *SIAM Rev* 41:135–147
15. Tsai MJ (2009) A visible watermarking algorithm based on the content and contrast aware (COCO) technique. *J Vis Commun Image Represent* 20:323–338
16. Tsai HM, Chang LW (2010) Secure reversible visible image watermarking with authentication. *Signal Process Image Commun* 25:10–17
17. Weng CY, Zhang YH, Lin CL (2013) Visible watermarking images in high quality of data hiding. *J Supercomput* 66:1033–1048
18. Yang H, Yin J (2015) A secure removable visible watermarking for BTC compressed images. *Multimed Tools Appl* 74:1725–1739
19. Yang Y, Sun X, Yang H (2008) Removable visible image watermarking algorithm in the discrete cosine transform domain. *J Electron Imaging* 17:033008–033008



**Kevin Rangel-Espinoza** received the M. E. degree in Security and Information Technology and the B.S. degree in Computer Engineering both from the Mechanical–Electrical Engineering School of the Instituto Politécnico Nacional (IPN) of Mexico in 2014 and 2017, respectively. Currently he is the Ph.D. student of the Electronic and Communications Program in the IPN. His research interest are information security and image processing.





**Eduardo Fragoso-Navarro** received the M. S. degree in Microelectronics from the Mechanical–Electrical Engineering School of the Instituto Politécnico Nacional (IPN) of Mexico in 2017 and the B.S. degree in Mechatronics Engineering from the Interdisciplinary Professional Unit in Engineering and Advanced Technologies (UPIITA) of the IPN in 2011. Currently he is the Ph.D. student of the Electronic and Communications Program in the IPN. His research interest are image processing and watermarking.



**Clara Cruz-Ramos** received the B.S. degree in Communications and Electronics Engineering from the Instituto Politécnico Nacional (IPN), of Mexico City, in 1999, the M.Sc. degree in Microelectronic and the Ph.D. degree in Electronic and Communications both from IPN in 2003 and 2009, respectively. In January 2002, she joined the Computer Department of the Mechanical–Electrical Engineering School of the IPN, where she is now a lecturer, and from 2004 she joined the Graduate Section of the IPN as an assistant professor. Her research interests are digital image processing, information security, watermarking and related fields.



**Rogelio Reyes-Reyes** received the B.S. degree in Communications and Electronics Engineering from the Mechanical–Electrical Engineering School of Instituto Politécnico Nacional (IPN) of Mexico, in 1999, the M.Sc. degree in Microelectronics and the Ph.D. degree in Communication and Electronic Engineering from the Graduate Section of the IPN, in 2003 and 2009, respectively. In 2002, he joined the Computer Department of the Culhuacan Campus of the IPN where he is now a professor. His main research fields are video and image processing, embedded security systems and related fields.



**Mariko Nakano-Miyatake** received the B.S. and M.E. degrees in Electrical Engineering from the University of Electro-Communications, Tokyo Japan in 1983 and 1985, and her Ph. D in Electrical Engineering from The Universidad Autonoma Metropolitana (UAM), Mexico City, in 1998. From July 1992 to February 1997 she was a Department of Electrical Engineering of the UAM Mexico. In February 1997, she joined the Graduate Department of The Mechanical and Electrical Engineering School Culhuacan Campus of The National Polytechnic Institute of Mexico, where she is now a Professor. In 1999 she received the Research Award from the National Polytechnic Institute of Mexico. Her research interests are in adaptive systems, pattern recognition information security and related fields. Nakano is a member of the IEEE, RISP and the National Researchers System of Mexico.



**Hector M. Pérez-Meana** received the M.S. degree from the University of Electro-Communications, Tokyo Japan, a Ph. D. degree in Electrical Engineering from Tokyo Institute of Technology, Tokyo, Japan, in 1989. In 1981 he joined the Electrical Engineering Department of the Metropolitan University, Mexico City, where he was a Professor. From March 1989 to September 1991, he was a visiting researcher at Fujitsu Laboratories Ltd., Kawasaki, Japan. In February 1997, he joined the Graduate Department of The Mechanical and Electrical Engineering School, Culhuacan Campus (ESIME-C) of the National Polytechnic Institute of Mexico, where he is now a Professor. From 2006 to 2010 he was Dean of the Graduate Department of the ESIME-C; and from 1999 to 2006 to 2010–2013 Chair of the PhD program on Communications and Electronics Engineering of the IPN. In 1991 he received the IEICE excellent Paper Award, and in 1999 and 2000 the IPN Research Award. In 1998 he was Co-Chair of the ISITA'98, and general Chair of The Midwest Symposium on Circuit and Systems, 209. His principal research interests are adaptive systems, image processing, pattern recognition, information security and related fields. Dr. Perez-Meana is a member of the IEEE, IEICE, the National Researchers System of Mexico and the Mexican Academy of Science.