Copyright Protection of Color Imaging Using Robust-Encoded Watermarking

Manuel CEDILLO-HERNANDEZ 1, Antonio CEDILLO-HERNANDEZ 1, Francisco GARCIA-UGALDE 1, Mariko NAKANO-MIYATAKE 2, Hector PEREZ-MEANA 2

1 Electric Engineering Division, Engineering Faculty, National Autonomous University of Mexico, Circuito Exterior, Ciudad Universitaria, Coyoacan 04510, Mexico City, Mexico
2 Postgraduate Section, Mechanical Electrical Engineering School, National Polytechnic Institute of Mexico, 1000 Santa Ana Avenue, San Francisco Culhuacan, Coyoacan 04430, Mexico City, Mexico

mcedillohdz@hotmail.com, antoniochz@hotmail.com, fgarciau@unam.mx, mariko@infinitum.com.mx, hmpm@prodigy.net.mx

Abstract. In this paper we present a robust-encoded watermarking method applied to color images for copyright protection, which presents robustness against several geometric and signal processing distortions. Trade-off between payload, robustness and imperceptibility is a very important aspect which has to be considered when a watermark algorithm is designed. In our proposed scheme, previously to be embedded into the image, the watermark signal is encoded using a convolutional encoder, which can perform forward error correction achieving better robustness performance. Then, the embedding process is carried out through the discrete cosine transform domain (DCT) of an image using the image normalization technique to accomplish robustness against geometric and signal processing distortions. The embedded watermark coded bits are extracted and decoded using the Viterbi algorithm. In order to determine the presence or absence of the watermark into the image we compute the bit error rate (BER) between the recovered and the original watermark data sequence. The quality of the watermarked image is measured using the well-known indices: Peak Signal to Noise Ratio (PSNR), Visual Information Fidelity (VIF) and Structural Similarity Index (SSIM). The color difference between the watermarked and original images is obtained by using the Normalized Color Difference (NCD) measure. The experimental results show that the proposed method provides good performance in terms of imperceptibility and robustness. The comparison among the proposed and previously reported methods based on different techniques is also provided.

1. Introduction

During the last decades, demand for multimedia data such as digital image, video and audio technologies, has increased dramatically due to its wide use within home computers, mobile devices and open networks. However the growth of digital multimedia has several advantages, it has created problems related to the preservation of copyright. Illegal media contents have the same visual quality as the original ones and they are very easy to reproduce and distribute. Digital watermarking is considered as a suitable solution for copyright protection of digital multimedia. In not visible digital watermarking, a short message called “watermark” is embedded into an image, audio or video signal without affecting the perceptive quality such that it can be detected using a detection algorithm. In public digital image watermarking methods, the synchronization loss, between the embedding and detection stages, causes watermark detection errors. Geometric distortions are frequently the principal factors of this problem.

Different techniques have been proposed in the literature to address the problem related to geometrically resilient image watermarking [1–7]. However, almost all the algorithms [1–7] are designed to grayscale images and their application to color images is often inadequate since they usually work with an individual color channel [8]. The use of color in image and video processing systems has become a key element in the recent years within security, steganography, and watermarking applications of multimedia data [9]. Unlike other applications, in the image watermarking field, the color cannot be considered as a simple RGB color model decomposition and the whole intrinsic information must be integrated into the embedding and detection processes. While several methods have been proposed to watermark grayscale images, only a few have been specifically designed for color images [8]. In the recent years, several color image watermarking methods have been proposed in the literature, these methods could be classified as those which are based on the frequency transform domain [10], pixel modification in the spatial
domain [11], histogram modification [12] and image normalization [13]. Almost all the methods mentioned above have shown watermark robustness to geometrical distortion; however they cannot provide enough robustness against common signal processing, such as filtering, noise contamination and image compression neither some aggressive combinations of geometric attacks and common signal processing operations. In order to increase the watermark robustness, an effective technique consists in developing hybrid algorithms which combine the use of a frequency domain in conjunction with an image normalization process based on geometric moments, introduced by [14]. Image normalization is based on a concept that the normalized version obtained from the original image and their geometric distorted versions are exactly the same. Based on this concept, the watermark embedding and detection processes may be carried out in the normalized version of the image, and thereby; theoretically the problem of synchronization loss between both processes not occurs. However in practice, because the image normalization process contains interpolation; the visual quality distortion in the watermarked image is significant [15], [16].

To solve this inconvenience, authors in [5] proposed two image watermarking schemes for copyright protection purposes, the first one is based on image normalization and blind detection, meanwhile, the second one is based on an elastic graph and non-blind detection. Thus, in the first method proposed in [5], to avoid the visual quality distortion of the watermarked image, instead of the original image the watermark signal is normalized and is embedded in the spatial domain. This algorithm gets robustness against several geometric and signal processing distortions; however, obtained bit error rate (BER) is not quite low in the detection stage.

In order to obtain a lower BER value, watermark strength must be increased and, as consequence, quality distortion over the watermarked image cannot be avoided. On the other hand, together with the image normalization procedure, in order to obtain geometric invariance the authors in [13] proposed a robust color watermarking method based on support vector regression (SVR) and non-subsampled contourlet transform (NSCT). Here, color image is decomposed in three RGB color model components and a significant region is obtained from the normalized components using the invariant centroid theory. Then, the NSCT is performed on the G channel of the significant region. Finally, the watermark is embedded into the original color image by modifying the low frequency NSCT coefficients, in which a human visual system (HVS) masking is used to control the watermark embedding strength. According to the high correlation among different channels of the color image, digital watermark can be recovered using the SVR technique. This algorithm presents robustness against several geometric and signal processing distortions, including cropping attacks; however, the method presents an important drawback: high computation time is needed for the SVR training, the computation of the NSCT as well as the image normalization process.

In this context, our proposal presents a robust-encoded watermarking method applied to color images for copyright protection. The scope is oriented in the same way as the related works presented in [5] and [13], where using the image normalization procedure together within a frequency domain. Nevertheless, our proposed algorithm presents significant improvements compared with them; with respect to [5]: a) the improvement of watermark imperceptibility in terms of PSNR metric, without affecting the robustness of the method, b) the design of a robust-encoded watermarking scheme based on the DCT domain; preserving the robustness against JPEG compression obtained in [5] and at the same time improving the robustness against aggressive geometric attacks such as cropping, image, and c) the application of the proposed method to color images. On the other hand, with regard to [13]: a) the proposed method can save high computational time by providing a simple design which gets a better imperceptibility and robustness performance.

The rest of this paper is organized as follows. Sec. 2 shows the basic theory about the image normalization procedure. Sec. 3 describes the embedding and detection process of the proposed algorithm. Experimental results including comparison with the previously reported watermarking algorithms are presented in Sec. 4. Finally, Sec. 5 concludes this work.

2. Background

In the proposed algorithm, original color image and the watermark pattern are normalized in order to develop a watermarking scheme robust against geometric and signal processing distortions. In this section, a description about the image normalization technique is provided, which is based on the invariant moment theory proposed in [14]. Here we describe in detail the procedures of invariant moment calculi and image normalization procedure.

2.1 Invariant Moments

The geometric moments \( m_{pq} \) and the central moments \( \mu_{pq} \) of a given image \( f(x,y) \) are defined by (1) and (2) respectively.

\[
m_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q f(x,y), \tag{1}
\]

\[
\mu_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (x-x_0)^p (y-y_0)^q f(x,y), \tag{2}
\]

where \( p, q = 1,2,\ldots\), and \( (x_0,y_0) \) is the centroid of the image, which is obtained as follows:

\[
\bar{x} = \frac{m_{10}}{m_{00}}, \quad \bar{y} = \frac{m_{01}}{m_{00}}. \tag{3}
\]
2.2 Image Normalization Procedure

The image normalization procedure of a given image \( f(x,y) \) consists of the following stages:

1) Translate the original image \( f(x,y) \) with the values \((d_x, d_y)\) in order to generate a new image \( f(x_0+y_0) \), in which the center is equal to the centroid of \( f(x,y) \). This operation is given by (4) using an affine transformation.

\[
\begin{pmatrix}
x_a \\
y_a
\end{pmatrix} = A \cdot \begin{pmatrix}
x \\
y
\end{pmatrix} - d,
\]

where:

\[
A = \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix},
\]

\[
d = \begin{pmatrix}
d_x \\
d_y
\end{pmatrix},
\]

whose elements are:

\[
d_x = \frac{m_{00}}{m_{00}}, d_y = \frac{m_{01}}{m_{00}}.
\]

This procedure normalizes an image with respect to the translation.

2) Apply a shearing transformation in \( x \)-direction to the image \( f_1(x,y) \) using:

\[
A_x = \begin{pmatrix}
1 & \beta \\
0 & 1
\end{pmatrix}.
\]

The resultant image is denoted as \( f_2(x,y) \), which is normalized against the effect caused by the shearing in the \( x \)-direction.

3) Apply a shearing transformation in \( y \)-direction to the image \( f_2(x,y) \) using:

\[
A_y = \begin{pmatrix}
1 & 0 \\
\gamma & 1
\end{pmatrix}.
\]

The resultant image is denoted as \( f_3(x,y) \), which is normalized against the effect caused by the shearing in the \( y \)-direction.

4) Change the size of the image \( f_3(x,y) \) in both directions, using:

\[
A_s = \begin{pmatrix}
\alpha & 0 \\
0 & \delta
\end{pmatrix}.
\]

The resultant image is denoted as \( f_4(x,y) \), which is normalized against the effect caused by the scaling in both directions.

5) Rotate the image \( f_4(x,y) \) using:

\[
A_r = \begin{pmatrix}
\cos(\phi) & \sin(\phi) \\
-\sin(\phi) & \cos(\phi)
\end{pmatrix}.
\]

The resultant image is denoted as \( f_5(x,y) \), which is normalized against the effect caused by the rotation. Finally, the image \( f_5(x,y) \) is the normalized version of the image obtained from the original one \( f(x,y) \). It is noteworthy that the above normalization procedures are totally reversible, applying the inverse matrices \( A_r, A_s, A_y, A_x, A_tr, A_s, A_y, A_x, A_tr \) and adding the vector \( d \) to the normalized image \( f_5(x,y) \), getting the original image \( f(x,y) \). However, for a discrete implementation of both processes, the normalization and the inverse procedures require an interpolation, which causes visual quality degradation of the image. The determination of the parameters \( \alpha, \beta, \phi, \gamma, \delta \) is given by the following theory [14].

If the image \( g(x,y) \) is a transformed image of \( f(x,y) \), applying a general affine transformation:

\[
A = \begin{pmatrix}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{pmatrix},
\]

\( g(x,y) \) is given by \( g(x,y) = A \cdot f(x,y) \). The invariant moments of image \( g(x,y) \), \( m_p^q \) are given by:

\[
m_p^q = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q g(x,y) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} A \cdot x^p \cdot y^q \cdot f(x,y). \quad (12)
\]

Applying the general affine transformation \( A \) in a coordinate \( (x,y) \), the transform coordinate \( (x', y') \) is obtained by:

\[
x' = a_{11}x + a_{12}y \\
y' = a_{21}x + a_{22}y
\]

Replacing the coordinates \( (x', y') \) in (12), we obtain:

\[
m_p^q = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (a_{11}x + a_{12}y)^p (a_{21}x + a_{22}y)^q f(x,y). \quad (14)
\]

Applying the binomial theorem in (14), we have:

\[
(a_{11}x + a_{12}y)^p = \sum_{i=0}^{p} \binom{p}{i} a_{11}^i x^i y^{p-i}
\]

\[
= \sum_{i=0}^{p} \binom{p}{i} a_{11}^i x^i y^{p-i}
\]

\[
(a_{21}x + a_{22}y)^q = \sum_{j=0}^{q} \binom{q}{j} a_{21}^j x^j y^{q-j}
\]

Replacing (15) and (16) in (14), we obtain:

\[
m_p^q = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{i=0}^{p} \sum_{j=0}^{q} \binom{p}{i} \binom{q}{j} a_{11}^i a_{21}^j x^i y^j f(x,y)
\]

\[
= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{i=0}^{p} \sum_{j=0}^{q} \binom{p}{i} \binom{q}{j} a_{11}^i a_{21}^j x^i y^j f(x,y)
\]

\[
= \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{i=0}^{p} \sum_{j=0}^{q} \binom{p}{i} \binom{q}{j} a_{11}^i a_{21}^j x^i y^j f(x,y)
\]

(17)
Using the definition in (1), we obtain:

\[
m_{i+j,p+q+i-j} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y). \tag{18}
\]

Finally, replacing (17) in (18), we obtain:

\[
m'_{i+j,p+q+i-j} = \sum_{i=0}^{p} \sum_{j=0}^{q} \left( \sum_{i=0}^{p} \sum_{j=0}^{q} \left( p_{i+j} \right) q_{i+j} \right) a_{i+j} a_{i+j}' m_{i+j,p+q+i-j}. \tag{19}
\]

In the same manner, we obtain \( \mu'_{i+j,p+q+i-j} \) as follows:

\[
\mu'_{i+j,p+q+i-j} = \sum_{i=0}^{p} \sum_{j=0}^{q} \left( p_{i+j} \right) q_{i+j} a_{i+j} a_{i+j}' \mu_{i+j,p+q+i-j}. \tag{20}
\]

Using this relationship between the invariant moments of the normalized and the original image, we estimate the parameters \( \alpha, \beta, \gamma, \delta \) and the normalization matrices \( A_x, A_z, A_y, A_z \). Interested readers can refer to [5] for more details. Fig. 1 shows an example of image normalization and the visual quality degradation of the reconstructed image produced by the interpolation used in the inverse procedure, where (c) is the normalized version of both images (a) original and (b) geometric distorted, (d) is the image reconstructed after the inverse procedure. For illustrative purposes, partial content obtained from the blue circular patch is zoomed and shown within a square at the left down corner of the images (a) original and (d) reconstructed, in order to perceive the visual degradation with more detail.

![Fig. 1. (a) Original image. (b) Geometric distorted version of (a). (c) Normalized version of (a) and (b). (d) Reconstructed image after inverse normalization procedure.](image)

3. Proposed Algorithm

The robust-encoded proposed watermarking method has been designed in order to get the following requirements: a) Blind detection, which means the original image is not needed during the detection process of the watermark algorithm; b) Robustness against common signal processing operations such as median and Gaussian filtering, as well as JPEG compression, impulsive and Gaussian noise contamination, among others; c) Robustness against geometric attacks such as rotation, scaling, aspect ratio, affine transformations, cropping, among others; d) Robustness against combined distortions composed by common signal processing operations together with geometric attacks; e) Improved watermark imperceptibility; and f) Oriented to color images applications.

3.1 Color Model Determination

One of the major issues in color image processing is to find the appropriate color model for the problem being addressed [17]. Whereas the application context often defines the original color model, the color model used for embedding a watermark has to be discussed according to the objective of the watermark scheme, i.e., fragile, semi-fragile or robust scheme. According to [8], the RGB color model has the most correlated components while the YCbCr color model components are less correlated. Also, the forward and backward transformations between RGB and YCbCr color models are linear. Considering this fact, if the correlated color model such as RGB is used, the modification of one component independently to the others is not the best choice, because the perceived colors are dependent of the three components together. This is the reason why the RGB model is called a correlated color model. On the other hand, YCbCr model allows to obtain non-correlated components and has the advantage of separating the luminance information from the chrominance information [8], [17]. According to this, YCbCr model is adopted as suitable color model in the watermarking method proposed.

3.2 Embedding Process

The embedding process is described as follows:

1. Convert the RGB color model of the original image \( I \) to the YCbCr color model representation. Separate the luminance component \( Y \) from the YCbCr color model representation.
2. Get a normalized version of the luminance component \( Y \) using the normalization procedure described in Sec. 2.2. 3. Build a binary pseudo-random prototype pattern generated by any secret key, whose dimensions are the same as the original color image. 4. The watermark is a zero mean 1-D binary pseudo-random pattern composed by \( \{1, 0\} \) values generated by a user’s secret key \( k_1 \). \( W = \{w_n\}, \ n = 1, ..., L \), where \( L \) is the length of the watermark. 5. Encode the watermark \( W \) using the convolutional code, proposed in [18] with the following characteristics: code rate \( = 1/3 \), constraint length \( K = 5 \), free distance \( d_f = 12 \) and the generator polynomials \( g_1 = [11111], g_2 = [11011] \) and \( g_3 = [10101] \). The encoder output is then \( E = \{e_1, e_2, ..., e_L\} \). In a digital communication system, the
convolutional encoding adds redundancy to the information bits [18]. These additional redundant bits are used at the receiver to perform a forward error correction (FEC) with the purpose of achieving a lower bit error rate. In the case of the watermark system, the convolutional encoding increases the robustness of the watermark against attacks. Fig. 2 shows the convolutional encoder used in the proposed method.

6) Once the prototype pattern is generated, it is masked using the normalized version of the luminance component (Y) (obtained in the step 2 of this procedure) as a template. The template used in this masking operation is a binary pattern composed by {1, 0} values and their implementation considers to assign the value ‘1’ in places that contain information of the luminance component (Y) normalized (i.e. white area of the “Template”) and preserve the value ‘0’ on the area outside the support of the normalized version (i.e. black area of the “Template”). This masking ensures that the watermark data bits are embedded only into information of the original image to be protected. On the other hand, the information of the area outside the support of the normalized version will be discarded by the inverse normalization procedure when is applied, as is illustrated in Fig. 1 of this paper. Later, it defines a region of interesting (ROI) using the centroid resulting from the normalization procedure. It divides this ROI in blocks of 8x8 pixels. The ROI’s dimensions and the amount of blocks are in direct relation of the convolutional encoder output E. In this way, we determine the watermark length experimentally as \( L = 108 \), in consequence, the amount of elements of \( E \) is \( h = 399 \) (including the zero padding needed to put the convolutional decoder at the final null state), thereby, in the proposed method, 399 blocks of 8x8 pixels are needed for the watermark embedding. 7) Once the prototype pattern is masked and the ROI together with 8x8 pixel blocks are defined, the watermark embedding process is performed as follows. In order to preserve the trade-off between imperceptibility and robustness, firstly, the encoder output \( E \) is multiplied by a first watermark strength factor \( \alpha_1 \), \( E = \{e_1 \alpha_1, e_2 \alpha_1, ..., e_h \alpha_1\} \). Later, each 8x8 block of the ROI is processed as shown in Fig. 3, this process is described as follows: a) replace the DC coefficient by its corresponding value of the encoder output \( E \) and then b) apply the inverse discrete cosine transform (IDCT).

8) Apply the inverse image normalization procedure to the prototype pattern which contains the encoded watermark. The final prototype pattern is denoted as \( P \). 9) In order to preserve high watermark imperceptibility, the pattern \( P \) is multiplied by a second watermark strength factor \( \alpha_2 \). Finally, the pattern \( P \) is embedded into the original image using an additive insertion in the spatial domain, given by (21):

\[
Y_w = Y_o + P \cdot \alpha_2,
\]

where \( Y_w \) and \( Y_o \) are the watermarked and the original luminance components respectively. Restore the watermarked luminance component \( Y_w \), in conjunction with the chrominance components \( CbCr \) to RGB color model representation and obtain the final watermarked color image \( I_w \). The general diagram of the embedding process is shown in Fig. 4. The above procedure is equivalent to embedding the encoded watermark pattern into the DCT domain of the normalized image. It is important to note that within the proposed algorithm we have chosen to transform the prototype pattern which contains the watermark signal in order to fit the cover image instead of embedding directly the watermark into the normalized image. The above characteristic represents some advantages for the proposed algorithm. Firstly, it avoids any perceptual quality distortion which might otherwise have incurred to the color image.
Additionally, another advantage consists in discarding the information within the area outside the support of the prototype pattern obtained in the step 6 (i.e. black area). This can save computational time and provide an easier implementation. Because every DC coefficient replacement is carried out using only prototype pattern information, we can avoid any visual quality perceptual distortion into the color image controlling the watermark strength factors and at the same time improving the robustness against JPEG compression.

### 3.3 Detection Process

The detection process is described as follows:

1) Convert the watermarked color image $I_w$ from RGB to YCbCr color model representation. Separate the watermarked luminance component ($Y_w$) from the YCbCr color model representation.

2) Get the normalized version from the $Y_w$ component using the normalization procedure presented in Sec. 2.2. Later, reconstruct the region of interesting (ROI) using the centroid resulting from the normalization procedure and divide this in blocks of 8x8 pixels.

3) Apply the DCT transform to each block and extract the first coefficient (DC coefficient) from each DCT block. Concatenate these coefficients into a vector $V = (v_1, v_2, ..., v_h)$.

4) The encoded watermarked coefficients $\hat{E}$ are recovered performing the following operation to the elements of the vector $V$:

$$\hat{E} = [\hat{e}_1, \hat{e}_2, ..., \hat{e}_{n-1}, \hat{e}_h]$$  \hspace{1cm} (22)

where $\hat{e}_{k,ab} = \text{sign}(v_{k,ab})$, and sign is the sign function.

5) The decoding is performed using the Viterbi algorithm with hard decision [19], thus obtaining the retrieved watermark pattern $W'$.

6) Once that $W'$ was recovered, compute the BER between the original $W$ and the recovered $W'$ watermarks. Assuming ergodicity the BER is defined as the ratio between the number of incorrectly decoded bits and the total number of embedded bits. A threshold value $T_{BER}$ must be defined to determine if the watermark $W$ is present or not into the image. In this concern, considering a binomial distribution with success probability equal to 0.5, the false alarm probability $P_{fa}$ for $L$ bits embedded watermark data is given by (23), and a threshold value $T$ must be controlled in order to get a smaller value of $P_{fa}$ than a predetermined one.

$$P_{fa} = \sum_{i=0}^{L} \left( \frac{1}{2} \right)^L \frac{L!}{z!(L-z)!}$$  \hspace{1cm} (23)

where $L$ is the total number of watermark data bits, whose value is empirically set to 108 and, based on the Bernoulli trials assumption, $z$ is an independent random variable with binomial distribution [20]. The false alarm probability must be less than $P_{fa} = 4.9516 \times 10^{-11}$ which is set to satisfy the requirements of most watermarking applications for a reliable detection [20], and then an adequate threshold value $T_{BER} = \min(1-T/L, 1-(87/108)) = 0.20$, according to the fact that the bit error rate (BER) + the bit correct rate (BCR) must be equal to 1. If the BER value between $W$ and $W'$ is greater than 20% (more than 21 percent error bits), the watermark detection is failed, otherwise, the watermark detection is successful and the detection process is terminated. The general diagram of the detection procedure is shown Fig. 5.

### 4. Experimental Results

In this section, the performance of the proposed algorithm is evaluated considering watermark imperceptibility and robustness grades and using a variety of well-known digital images in the literature. We have used different images with a variety of texture content (e.g., Goldhill, Sailboat, Lena, Airplane, Baboon, Peppers, among others) of 512 x 512 pixels size and color resolution of 24 bits per pixel which can be found in the following academic database: http://sipi.usc.edu/database/ and some of them in the Matlab© Integrated Development Environment (IDE). Our experiments are carried out on a personal computer running Microsoft Windows 7 OS© with an Intel© Core i7 processor (4@3.4 GHz) and 8 GB RAM memory while the embedding and extracting procedures were implemented on Matlab© version 7.10. In these conditions, the average computing time for the embedding procedure has been measured in 6.22 seconds while an average of 5.46 seconds was needed for the detection procedure. A 1D binary pseudorandom sequence of size $L = 108$ bits is used as the watermark pattern $W$. The false alarm probability is set to $P_{fa} = 4.9516 \times 10^{-11}$ when $T_{BER} = 0.20$. The convolutional code described in the embedding process has been used. The watermark strength parameters used in the watermark embedding process has been determined to be $\alpha_1 = 35$ and $\alpha_2 = 0.003$, whose setting procedure will be explained in the next section. The watermarked image visual quality distor-
tion is measured using the following well known indices: Peak Signal to Noise Ratio (PSNR), Visual Information Fidelity (VIF) and Structural Similarity Index (SSIM). Finally, our experimental results are compared with some of the most important methods reported previously in the literature whose aim is to be robust against most common geometric and signal processing attacks.

4.1 Watermark Imperceptibility and Setting of Watermark Strengths $\alpha_1$, and $\alpha_2$

Using a watermark strength factor $\alpha_2 = 0.003$, and the parameters mentioned above, a watermark length $L = 108$, and a variable watermark strength value $\alpha_1$ from 5 to 55; the watermark imperceptibility was evaluated in terms of the PSNR, VIF [21] and SSIM [22] visual image quality metrics defined by (24), (25) and (26) respectively.

$$PSNR(dB) = 10\log_{10}\left(\frac{MaxPixelValue^2}{(MSE_{I_1} + MSE_{I_2} + MSE_{I_3})/3}\right)$$  \hspace{1cm} (24)

$$VIF = \frac{\sum_{\text{channels}} I(C^{Z,\omega}; G^{Z,\omega} | s^{Z,\omega})}{\sum_{\text{channels}} I(C^{Z,\omega}; E^{Z,\omega} | s^{Z,\omega})}.$$  \hspace{1cm} (25)

In (25) we sum over the channels of interest, where $C^{Z,\omega}$ represent $Z$ elements of the random field RF $C_\omega$ which describes the coefficients from channel $\omega$, and so on [21]. $E$ and $G$ denote the visual signal at the output of the Human Visual System model (HVS) from the original and the watermarked images respectively, from which the human brain extracts cognitive information. The terms $I(C^{Z,\omega}; E^{Z,\omega} | s^{Z,\omega})$ and $I(C^{Z,\omega}; G^{Z,\omega} | s^{Z,\omega})$ represent the information that can ideally be extracted by the brain from a particular channel in the original and the watermarked images respectively [21].

$$SSIM(I_o, I_w) = \frac{(2\mu_{I_o} \mu_{I_w} + C_1)(2\sigma_{I_o I_w} + C_2)}{\mu_{I_o}^2 + \mu_{I_w}^2 + C_1(\sigma_{I_o}^2 + \sigma_{I_w}^2) + C_2}.$$  \hspace{1cm} (26)

In (26) $I_o$ and $I_w$ are the original and watermarked images respectively and $C_1$, $C_2$ are small constant values [22]. As it is known in the literature the VIF value reflects perceptual distortions more precisely than PSNR. The range of VIF is $[0, 1]$ and the closer value to 1 represents the best fidelity respect to the original image. It is also well known in the literature that the SSIM value reflects perceptual distortions more precisely than PSNR. The range of SSIM is $[0, 1]$, and the closer value to 1 represents an identical quality respect to the original image, i.e. a value of 1 means that the original and the reference images are the same. In Figs. 6 and 7, the PSNR of ten test color images and average VIF-SSIM are plotted versus the variable watermark strength $\alpha_1$ ranging from 5 to 55 respectively.

A greater value of $\alpha_1$ could increase the robustness of the watermark, but as shown in Figs. 6 and 7, the watermark imperceptibility is diminished. Hence, there is a trade-off between robustness and imperceptibility. To preserve the trade-off between robustness and imperceptibility, based on our experiments, we considered a watermark strength of $\alpha_1 = 35$ as a suitable value, obtaining the following average values: $PSNR = 44.19$ dB, $VIF = 0.9559$ and $SSIM = 0.9967$.

Using a watermark strength $\alpha_1 = 35$, the parameters mentioned above, a watermark length $L = 108$, and a variable watermark strength $\alpha_2$ from 0.001 to 0.005; the watermark imperceptibility was evaluated in terms of the PSNR image quality metric and a subjective test based on the Mean Opinion Score (MOS) statistically supported in our experiments supported by the opinion of 100 persons of different academic levels. In Figs. 8 and 9, the PSNR and the average MOS of the ten test color images used are plotted versus the variable watermark strength $\alpha_2$ respectively.

A bigger value of $\alpha_2$ could increase the robustness of the watermark, but as shown in Figs. 8 and 9, the watermark imperceptibility is diminished. Hence ones again there is a trade-off between robustness and imperceptibility. To preserve the trade-off between robustness and imperceptibility, based on our experiments, we considered a watermark strength of $\alpha_2 = 0.003$ as a suitable value.
An example of perceptual distortion is shown in Fig. 10, when the watermark strength is set to $\alpha_2 = 0.005$ and $\alpha_1 = 35$. To illustrative purposes, the central content of Barb image is zoomed. Fig. 10(c) shows the distortion into the watermarked color image when $\alpha_1 = 35$.

To conclude the setting of the watermark strengths values, a pair of experiments related with the robustness against signal processing distortions, are performed with the following characteristics: a) using a variable watermark strength $\alpha_1$ ranging from 5 to 55 and $\alpha_2 = 0.003$, b) using a variable watermark strength $\alpha_2$ ranging from 0.001 to 0.005 and $\alpha_1 = 35$; both in conjunction with a watermark length $L = 108$, and a threshold value $T_{BER} = 0.20$. The robustness of the proposed method when ten watermarked test color images are contaminated with Gaussian noise with $\mu = 0$ and $\sigma^2 = 0.006$ is shown in Figs. 11 and 12, respectively.

A larger value of $\alpha_1$ and $\alpha_2$ increases the robustness of the watermark, but as shown in Figs. 6-9, the watermark imperceptibility is decreased. To preserve the trade-off between robustness and imperceptibility, based on our experiments, we considered a watermark strengths of $\alpha_1 = 35$ and $\alpha_2 = 0.003$ as suitable values. Three test color images (a) with their watermarked version (b) are shown in Figs. 13, 14 and 15 respectively.
Fig. 14. a) Gold hill image, b) Watermarked version.

Fig. 15. a) Airplane F-16 image, b) Watermarked version.

Algorithms [5] and [13] are two of the most robust watermarking techniques published with similar purposes as our proposed scheme. To get a proper comparison, we consider a homogeneous format of color images of 512×512×24 bits. The imperceptibility performance is compared in our simulations with those reported by algorithms in [5] and [13].

| Algorithm | PSNR (dB) |
|-----------|-----------|
| Proposed method | 44.19 |
| Method in [5] | 40.11 |
| Method in [13] | 41.18 |

Tab. 1. Average comparative results of imperceptibility using the PSNR (dB) metric.

From Tab. 1 it follows that the proposed scheme provides a fairly good fidelity of the watermarked color image, achieving a PSNR greater than 44 dB, avoiding the visual quality distortions in the color images.

On the other hand, the normalized color difference (NCD) metric [23], [24] is based on the CIELAB color space and it is applied to measure the difference of color between two images. NCD is given by (27) [23], [24]:

\[
NCD = \frac{1}{\sqrt{2}} \sqrt{\frac{\sum \sum (L_o(x,y) - L_w(x,y))^2 + (a_o(x,y) - a_w(x,y))^2 + (b_o(x,y) - b_w(x,y))^2)}{\sum \sum (L_o(x,y))^2 + (a_o(x,y))^2 + (b_o(x,y))^2}}
\]

where \(L_o, L_w\) represent lightness values and \(a_o, a_w, b_o, b_w\) the chrominance values corresponding to the original \(I_o\) and the watermarked \(I_w\) images expressed in the CIE Lab color space. Finally, in Tab. 2, we show NCD values calculated between the ten watermarked testing images used and its original versions.

From Tab. 2 and Figs. 13, 14 and 15, it can be seen that the proposed scheme provides good imperceptibility since the difference of colors between the watermarked image and the original one is insignificant [25].

4.2 Watermark Robustness

To evaluate the watermark robustness of the proposed algorithm we use the StirMark Benchmark [26], performing attacks of several geometrical distortions, signal processing and a combination of them. In order to carry out a representative comparison in terms of watermark robustness with respect to the related works reported in [5] and [13]; we have used one thousand color images with resolution of 24 bits per pixel of size 512×512.

Experimental results are classified in geometric, common signal processing, and combined distortions. For illustrative purposes, in Tab. 3 we show the average BER obtained in our proposed method and in those schemes reported in [5] and [13], after applying geometric distortions, and combined distortions composed by a JPEG compression with quality factor QF = 20 together with one or more geometric distortions. When the BER value is more than the predefined threshold value \(T_{BER} = 0.20\) (more than 21 error bits), the watermark detection is reported with italics and corresponds to the case where the watermark detection has failed.

Analyzing the results in Tab. 3, we show that our proposed method presents good robustness against several geometric distortions, including scaling from 0.5 to 2, rotation by several angles, general affine transformation, shearing 5% in x and y directions, cropping attack with 50%, aspect ratio in x and y directions by 1.2 and 0.9, respectively, horizontal and vertical flipping and combined attacks all of them with JPEG 20 compression. In all cases we have obtained BER values less than the predefined threshold value \(T_{BER} = 0.20\), except when the image is distorted by the Stirmark Random Bending Attack (RBA).
In both cases, the obtained BER values are greater than 0.20 (more than 21 error bits) the watermark cannot be recovered adequately. In the case where the watermark detection has failed.

On the other hand, the method proposed in [5] obtains a similar performance against the above mentioned geometric and combined distortions; however, the method is not robust against cropping attacks as well as RBA attack. In both cases, the obtaining BER values are greater than the predefined threshold value \( T_{BER} = 0.20 \). The weakness against cropping attacks is due to the fact that the watermark is embedded into the mid-range DCT coefficients of the whole image, thus, when the image is cropped from the center or the edges, several DCT blocks are removed and the watermark cannot be recovered adequately. In the case of the method proposed in [13], it obtains a similar performance against the above mentioned geometric and combined distortions, except against RBA attack. Although the performance is similar, the method in [13] is outperformed in detection accuracy when the image is cropped or distorted by vertical and horizontal flipping, obtaining BER values greater than 0.1, whereas that, our proposed method obtains BER values closer up to 0. Additionally, Tab. 4 shows the average BER obtained in our proposed method and the schemes reported in [5] and [13] respectively, after applying common signal processing, and combined attacks all of them with JPEG 20 compression. Similarly, when the BER value is more than the predefined threshold value \( T_{BER} = 0.20 \) (more than 21 error bits) the watermark detection is reported in with italics and corresponds to the case where the watermark detection has failed.

Tab. 3. Average BER obtained from one thousand watermarked images after geometric and combined distortions.

| Geometric and combined distortions | Bit Error Rate (BER) |
|-----------------------------------|----------------------|
|                                   | Proposed method | Method in [5] | Method in [13] |
| Without distortion                | 0              | 0             | 0              |
| Rotation by 5°                    | 0              | 0.03          | 0.01           |
| Rotation by 45°                   | 0.01           | 0             | 0.03           |
| Scale 0.5                         | 0.02           | 0             | 0.04           |
| Scale 2                           | 0.007          | 0.04          | 0.02           |
| Cropping 50%                      | 0.03           | 0.52          | 0.12           |
| Affine [0.9,0.9,0.1,1,0.2,0,0,0,1] | 0.01           | 0             | 0.02           |
| Affine [-1.1,-0.2,0,0.2,0.8,0,0,0,1] | 0.02           | 0             | 0.02           |
| Shearing (5%, 5%)                 | 0.004          | 0             | 0.02           |
| Aspect ratio (1,2,0.9)            | 0.03           | 0             | 0.03           |
| Aspect ratio (1.2,1.0)            | 0.03           | 0             | 0.02           |
| Horizontal flip                   | 0.01           | 0             | 0.10           |
| Vertical flip                     | 0              | 0             | 0.15           |
| JPEG 20 + Rotation 45°           | 0.02           | 0.03          | 0.05           |
| JPEG 20 + Scale 1.5              | 0.03           | 0.02          | 0.09           |
| JPEG 20 + Affine [0.9,0.2,0.1,1,2,0,0,0,1] | 0.02          | 0.01          | 0.05           |
| JPEG 20 + Cropping 50%           | 0.03           | 0.53          | 0.15           |
| JPEG 20 + Shearing (5%, 5%)      | 0.01           | 0.01          | 0.04           |
| JPEG 20 + Aspect ratio (1,0.1,2)  | 0.02           | 0.01          | 0.03           |
| JPEG 20 + Horizontal flip        | 0              | 0             | 0.12           |
| Stirmark Random Bending Attack    | 0.53           | 0.59          | 0.51           |

Tab. 4. Average BER obtained from one thousand watermarked images after common signal processing, and combined distortions.

Analyzing the results in Tab. 4 we show that the algorithm [13] and ours present good robustness against several common signal processing operations, including JPEG compression with several quality factors ranging from 50 to 20. Also they present robustness against median, Gaussian and sharpen filters, all of them with window size of 3x3, impulsive noise with a density of 0.01 and Gaussian noise contamination with zero mean and variance 0.006. In all cases both algorithms have a BER value less than the predefined normalized threshold value \( T_{BER} = 0.20 \). Also, we have combined the methods composed by a JPEG 20 compression together with the common signal processing mentioned above. The robustness of both methods is not affected by this kind of combined attacks, obtaining BER values less than \( T_{BER} = 0.20 \). However, the method in [13] is outperformed in detection accuracy when the image is contaminated by impulsive noise with a density of 0.01, obtaining BER values equal to or greater than 0.1, whereas our proposed method obtains BER values closer up to 0.

On the other hand, the method proposed in [5] obtains a similar performance against the above mentioned geometric and combined distortions; however, the method is not robust against cropping attacks as well as RBA attack. In both cases, the obtaining BER values are greater than the threshold value \( T_{BER} = 0.20 \). The weakness against cropping attacks is due to the fact that the watermark is embedded into the mid-range DCT coefficients of the whole image, thus, when the image is cropped from the center or the edges, several DCT blocks are removed and the watermark cannot be recovered adequately. In the case of the method proposed in [13], it obtains a similar performance against the above mentioned geometric and combined distortions, except against RBA attack. Although the performance is similar, the method in [13] is outperformed in detection accuracy when the image is cropped or distorted by vertical and horizontal flipping, obtaining BER values greater than 0.1, whereas that, our proposed method obtains BER values closer up to 0.

5. Conclusions

Using the combination of the image normalization process, the convolutional encoding and the robustness of the DCT domain, we have developed a robust encoded watermarking method for copyright protection applied to color images. We combined five key elements in our method: a) the image normalization procedure, b) DCT
embedding domain, c) convolutional encoding, d) Viterbi decoder, e) the masking procedure. The watermark imperceptibility of the proposed algorithm was evaluated in terms of three well-known image quality distortion metrics (PSNR, VIF and SSIM), concluding that the visual distortion caused by the proposed watermarking algorithm is imperceptible, providing 44.19 dB, 0.9559 and 0.9967 values respectively. Watermark robustness of the proposed algorithm is evaluated using a wide range of attacks and a fairly good performance is obtained. From the evaluation results, we can conclude that our proposed algorithm outperforms the algorithms proposed in [5] and [13] that are two of the most efficient algorithms recently proposed for image watermarking, in terms of imperceptibility and detection accuracy. Experimental results show that our proposed method is robust against very aggressive attacks, such as scaling, rotation by several angles, general affine transformation, shearing in x and y directions, cropping attack, aspect ratio in x and y directions, horizontal and vertical flipping and combined attacks all of them with JPEG 20 compression. Obtained robustness against several geometric, signal processing and combined attacks, high imperceptibility and the compact design of our proposed method make it to be applied in a wide range of applications. As a future work, the proposed method will be extended to the authentication of digital video.

Acknowledgements

The authors thank the Post-Doctorate Scholarships Program and the PAPIIT IN-112513 project from DGAPA in the National Autonomous University of Mexico (UNAM), and the National Polytechnic Institute of Mexico (IPN) by the support provided during the realization of this research.

References

[1] AGOYI, M., CELEBI, E., ANBARJAFARI, G. A watermarking algorithm based on chirp z-transform, discrete wavelet transform, and singular value decomposition. Signal, Image and Video Processing, 2014, DOI: 10.1007/s11760-014-0624-9.
[2] TAO, H., CHONGLIN, L., ZAIN, J. M., ABDALLA, A. N. Robust image watermarking theories and techniques: A review. Journal of Applied Research and Technology (JART), 2014, vol. 12, p. 122–138.
[3] ZHANG, Y., ZHOU, Z-H., ZHANG, C., LI, Y. An anti-geometric digital watermark algorithm based on histogram grouping and fault-tolerance channel. Intelligent Science and Intelligent Data Engineering Lecture Notes in Computer Science, 2012, vol. 7202, p. 753–760. DOI: 10.1007/978-3-642-31919-8_96
[4] YAN, L., JIYING, Z. A new video watermarking algorithm based on 1D DFT and Radon transform. Signal Processing, 2010, vol. 90, p. 626–639. DOI: 10.1016/j.sigpro.2009.08.001
[5] DONG, P., BRANKOV, J. B., GALATSANOS, N. P., YANG, Y., DAVoine, F. Digital watermarking to geometric distortions.

IEEE Transactions on Image Processing, 2005, vol. 14, no. 12, p. 2140–2150. DOI: 10.1109/TIP.2005.857263

[6] CEDILLO, M., NAKANO, M., PEREZ, H. A robust watermarking technique based on image normalization. Rev. Fac. Ing. Univ. Antioquia / Journal of the Engineering Faculty University of Antioquia, 2010, vol. 52, p. 147–160.
[7] MOUSAVI, S. M., NAGHSH, A., ABU-BAKAR, S. A. R. Watermarking techniques used in medical images: A survey. Journal of Digital Imaging, 2014, vol. 27, no. 6, p. 714–729. DOI: 10.1007/s10278-014-9700-5
[8] CHAREYRON, G., DA RUGNA, J., TRÉMEAU, A. Color in image watermarking. In A. Al-Haj (Ed.), Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications, 2010, p. 36–56. DOI: 10.4018/978-1-61520-903-3.ch003
[9] TRÉMEAU, A., TOMINAGA, S., PLATANIOTIS, K. Color in image and video processing: Most recent trends and future research directions. EURASIP Journal on Image and Video Processing, 2008, p. 1–26. DOI:10.1155/2008/581371
[10] MAITY, S. P., KUNDU, M. K. DHT domain digital watermarking with low loss in image informations. AEU - International Journal of Electronics and Communications, 2009. DOI: 10.1016/j.aeue.2008.10.004
[11] ZHANG, X., WANG, S. Fragile watermarking scheme using a hierarchical mechanism. Signal Processing, 2009, vol. 89, no. 4, p. 675–679. DOI: 10.1016/j.sigpro.2008.10.001
[12] CEDILLO, M., GARCIA, F., NAKANO, M., PEREZ, H. Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification. Signal Image and Video Processing, 2015, vol. 8, no. 1, p. 49–63. DOI: 10.1007/s11760-013-0459-9.
[13] PAN-PAN NIU, XIANG-YANG WANG, YI-PING YANG, MING-YU LU. A novel color image watermarking scheme in non sampled contourlet-domain. Expert Systems with Applications, 2011, vol. 38, no. 3, p. 2081–2098. DOI: 10.1016/j.eswa.2010.07.147
[14] HU, M.-K. Visual pattern recognition by moment invariants. IRE Transactions on Information Theory, 1962, vol. 8, no. 2, p. 179–187. DOI: 10.1109/TIT.1962.1057692
[15] ALGHIONIEMY, M., TEWFIK, A. H. Geometric invariance in image watermarking. IEEE Transactions on Image Processing, 2004, vol. 13, no. 2, p. 145–153. DOI: 10.1109/TIP.2004.823831
[16] QI SONG, GUANG-XI ZHU, HANG-JIAN LUO. Geometrically robust image watermarking based on image normalization. In Proceedings of International Symp. on Intelligent Signal Processing and Communication Systems ISPACS 2005. Hong-Kong (China), 2005, p. 333–336. DOI: 10.1109/ISPACS.2005.1595414
[17] LUKAC, R., PLATANIOTIS, K. Color Image Processing. CRC Press, 2007.
[18] SKLAR, B. Digital Communications: Fundamentals and Applications. Second ed. System View, 2001.
[19] BATSON, B. H., MOOREHEAD, R. W. Simulation Results for the Viterbi Decoding Algorithm. NASA-TR-R-396, Technical report, 1972.
[20] TANG, C. W., HANG, H. M. A feature-based robust digital image watermarking scheme. IEEE Transactions on Signal Processing, 2003, vol. 51, no. 4, p. 950–959. DOI: 10.1109/TSP.2003.809367
[21] SHEIKH, H. R., BOVIK, A. C. Image information and visual quality. IEEE Transactions on Image Processing, 2006, vol. 15, no. 2, p. 430–444. DOI:10.1109/TIP.2005.859378
[22] WANG ZHOU, BOVIK, A. C., SHEIKH, H. R., SIMONCELLI, E. P. Image quality assessment: From error measurement to structural similarity. IEEE Transactions on Image Processing,
[23] CHANG, H. A., CHEN, H. H. Stochastic color interpolation for digital cameras. *IEEE Transactions on Circuits and Systems for Video Technology*, 2007, vol. 17, no. 8, p. 964–973. DOI: 10.1109/TCSVT.2007.897471

[24] PLATANIOTIS, K. N., VENETSANOPoulos, A. N. *Color Image Processing and Applications*. Berlin: Springer Verlag, 2000.

[25] SAHOO, A., SINGH, M. P. Fuzzy weighted adaptive linear filter for color image restoration using morphological detectors. *International Journal on Computer Science and Engineering*, 2009, vol. 1, no. 3, p. 217–221.

[26] PETITCOLAS, F. A. P. Watermarking schemes evaluation. *IEEE Signal Processing*, 2000, vol. 17, no. 5, p. 58–64. DOI: 10.1109/79.879339

**About the Authors**

**Manuel CEDILLO-HERNANDEZ** was born in Mexico. He received the B.S. degree in Computer Engineering, M.S. degree in Microelectronics Engineering and his PhD in Communications and Electronic from the National Polytechnic Institute of Mexico in 2003, 2006 and 2011, respectively. From August 2005 to August 2011 he was in Federal Electoral Institute (IFE) and Government Secretary (SEGOB) of Mexico in several information technologies areas. Currently, he is a full-time researcher at the Electric Engineering Division, Engineering Faculty, National Autonomous University of Mexico. His principal research interests are image and video processing, watermarking, software development and related fields.

**Antonio CEDILLO-HERNANDEZ** was born in Mexico. He received the B.S. degree in Computer Engineering, M.S. degree in Microelectronics Engineering and his PhD in Communications and Electronic from the National Polytechnic Institute of Mexico in 2003, 2006 and 2011, respectively. He holds a certification as Project Management Professional (PMP®). He worked in Mexican Government Ministry (SEGOB) as a Contract and Project Management for five years. From September 2013 to December 2014 he was with the Polytechnic Metropolitan University of Hidalgo where he was a full-time researcher. Currently, he courses a postdoctoral residence at the Electric Engineering Division, Engineering Faculty, National Autonomous University of Mexico. His principal research interests are video processing, watermarking, software development and related fields.

**Francisco GARCIA-UGALDE** was born in Mexico. He obtained his bachelor in 1977 in Electronics and Electrical System Engineering from National Autonomous University of Mexico, his Diplôme d’Ingénieur in 1980 from SUPELEC France, and his PhD in 1982 in Information Processing from Université de Rennes I, France. Since 1983, he is a full-time professor at UNAM, Engineering Faculty. His current interest fields are: Digital filter design tools, analysis and design of digital filters, image and video coding, image analysis, watermarking, theory and applications of error control coding, turbo coding, applications of cryptography, parallel processing and data bases.

**Mariko NAKANO-MIYATAKE** was born in Japan. She received the M.E. degree in Electrical Engineering from the University of Electro-Communications, Tokyo, Japan in 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 with the Department of Electrical Engineering, UAM Mexico. In February 1997, she joined the Graduate Department of the Mechanical and Electrical Engineering School, National Polytechnic Institute of Mexico, where she is now a Professor. Her research interests are in information security, image processing, pattern recognition and related field.

**Hector PEREZ-MEANA** was born in Mexico. He received his M.S: Degree in Electrical Engineering from the Electro-Communications University of Tokyo, Japan in 1986 and his Ph. D. degree in Electrical Engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1989. From March 1989 to September 1991, he was a visiting researcher at Fujitsu Laboratories Ltd, Kawasaki, Japan. From September 1991 to February 1997, he was with the Electrical Engineering Department of the Metropolitan University of Mexico City where he was a Professor. In February 1997, he joined the Graduate Studies and Research Section of the Mechanical and Electrical Engineering School, National Polytechnic Institute of Mexico, where he is now a Professor. His principal research interests are adaptive systems, image processing, pattern recognition, watermarking and related fields.