SIViP (2014) 8:49–63
DOI 10.1007/s11760-013-0459-9

ORIGINAL PAPER

Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification

Manuel Cedillo-Hernández · Francisco García-Ugalde · Mariko Nakano-Miyatake · Héctor Manuel Pérez-Meana

Received: 26 October 2012 / Revised: 7 March 2013 / Accepted: 8 March 2013 / Published online: 5 April 2013

Abstract In this paper, we present a robust hybrid watermarking method applied to color images for authentication, which presents robustness against several distortions. Due to the different nature of common signal processing and geometrical attacks, two different techniques for embed a same watermark are used in this method. In the first one, the luminance component (Y) information is used to embed the watermark bit sequence into the magnitude of the middle frequencies of the Discrete Fourier Transform (DFT). In the second one, a selected region of 2D histogram composed by blue-difference and red-difference (Cb–Cr) chrominance components is modified according to the watermark bit sequence. The quality of the watermarked image is measured using the following well-known indices peak signal to noise ratio (PSNR), visual information fidelity (VIF) and structural similarity index (SSIM). The difference color of the watermarked image is obtained using the normalized color difference (NCD) measure. The experimental results show that the proposed method provides robustness against several geometric distortions, signal processing operations, combined distortions and photo editing. The comparison with the previously reported methods based on different techniques is also provided.

Keywords Authentication · Robust watermarking · Histogram modification · Geometric attacks · Hybrid watermarking

M. Cedillo-Hernández (✉) · F. García-Ugalde
Electric Engineering Division, Engineering Faculty, National Autonomous University of Mexico, Circuito Exterior, Ciudad Universitaria, 04510 Coyoacan, Mexico City, Mexico
e-mail: mcedillohdz@hotmail.com
URL: http://dps.fi-p.unam.mx/FGU/FGU.html

F. García-Ugalde
e-mail: fgarciau@unam.mx

M. Nakano-Miyatake · H. M. Pérez-Meana
Postgraduate Section, Mechanical Electrical Engineering School, National Polytechnic Institute of Mexico, 1000 Santa Ana Avenue, San Francisco Culhuacan, 04430 Coyoacan, Mexico City, Mexico
e-mail: mariko@infinitum.com.mx
URL: http://www.posgrados.esimecu.ipn.mx/index.php

H. M. Pérez-Meana
e-mail: hmpm@prodigy.net.mx

1 Introduction

During the last decades, digital image, video and audio technologies, widely used within home computers, mobile devices and open networks have grown dramatically. Allowing that, digital media data may be easily copied, manipulated or format converted without any control. This fact suggests the necessity to develop some efficient methods to solve these problems. Digital watermarking is considered as a suitable solution for authentication of digital materials. In digital watermarking, a short message called "watermark" is embedded into an image, audio or video 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, such as cropping, rotation, scaling and any affine transformation, which are common in practice, are the principal factors of this problem. In the literature, several approaches are related to geometrically resilient image watermarking. Firstly, we find algorithms based on invariant domains such as Fourier–Mellin domain [1,2], log polar domain [3], Radon transformation domain [4], geometric moments [5,6] and Zernike moments [7] which are used to embed the watermark and maintain synchronization under geometric transforms.

These approaches show robustness against rotation and scaling distortions, because these methods embed the watermark into geometric invariant domains, however, may be typically highly vulnerable against cropping attacks and other aggressive geometric transformations, such as affine and projective transformations. On the other hand, almost all the algorithms mentioned above 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 in the recent years a key element in security, steganography, and watermarking applications of multimedia data [9]. Unfortunately, in the watermarking field, the color cannot be considered as a simple RGB color model decomposition and all of their intrinsic information must be integrated into the watermarking embedding and detection processes. While several methods have been proposed to watermark grayscale images, only a few have been designed specifically for color images [8]. In this way, several color image watermarking methods have been proposed in the literature, and some of them are based on the frequency domain transform [10–12], pixel modification in the spatial domain [13–15] and histogram modification [16–22]. Thus, because the image histogram is one of the geometric invariant domains, one way to embed a watermark pattern into a color image is to use its color histogram. If the watermark can be embedded into this domain, it should survive to most geometric transformations. Authors of [16] use an exact histogram specification to embed a watermark into the images. In [17], the histogram-specification method proposed by Coltuc and Bolon [16] is extended to chromatic histograms and a watermark sequence is embedded in the chromatic plane of a color image. Authors of [18] proposed a watermarking method into a color histogram using constrained Earth Mover Distance (EMD) to optimize the modification of the image, according to a target histogram. In [19], authors proposed a partition and modify the feature space composed by a 3D histogram to insert the watermark pattern. Authors of [20] proposed a digital watermark algorithm based on histogram grouping, where fault tolerance channels are introduced to reduce and eliminate the disturbance brought by geometric attacks. In [21], a reversible watermarking scheme for images is proposed, which is based on 1D histogram modification. Almost all previous works based on histogram modification have shown watermark robustness to geometrical distortion; however, they cannot provide sufficient 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. To increase the robustness without decreasing the watermark imperceptibility, a very promising research direction consist in developing hybrid algorithms which combine the spatial and color image information [8]. In this way, authors of [22] proposed a hybrid watermarking scheme for authentication purposes. Due to the different nature of common signal processing and geometrical distortions, two different watermarks are embedding in this algorithm. The first one is embedded in the discrete cosine transform (DCT) domain combined with a chaotic function. The second watermark is embedded in a 1D histogram modification of the image. This hybrid watermarking method combines the robustness of DCT-chaotic domain against filtering, noise and compression attacks with the robustness of histogram domain against geometric distortions. The method shows the watermark robustness against some geometric distortions, common signal processing and artistic filters supported by commercial Photoshop®. However, it shows some vulnerability with respect to the cropping attack as well as to the combined attacks that involves this geometrical distortion. In this context, our paper presents a robust hybrid watermarking method applied to color images for authentication, which presents robustness against several distortions. As mentioned above, due to the different nature of common signal processing and geometrical attacks, two different techniques to embed a same watermark for authentication are used in this method. In the first one, the luminance component (Y) information is used to embed the watermark bit sequence into the magnitude of the middle frequencies of the Discrete Fourier Transform (DFT). In the second one, a selected region of 2D histogram composed by blue-difference and red-difference (Cb–Cr) chrominance components is modified according to the watermark bit sequence. The quality of the watermarked image is measured using the following well-known indices PSNR, VIF and SSIM. The difference color of the watermarked image is obtained using the NCD measure. Experimental results show that the proposed method provides robustness against several geometric distortions, signal processing operations, combined distortions and photo editing. The comparison with the previously reported methods based on different techniques is also provided. The rest of the paper is organized as follows: Sect. 2 describes the embedding and detection process of the proposed algorithm, and experimental results including comparison with previously reported watermarking algorithms are presented in Sect. 3. Finally, Sect. 4 concludes this work.

2 Proposed algorithm

The hybrid proposed watermarking method uses two distinct watermarking techniques to embed the same watermark into a color image. The proposed color image watermarking hybrid method supports the following features:

- Blind detection, in which, the original image is not needed during the detection of the watermark.

- Robustness against common signal processing operations such as median and Gaussian filtering, sharpness, brightness, contrast changes, JPEG compression, impulsive and Gaussian noise perturbation, among others.
- Robustness against geometric attacks such as rotation, scaling, aspect ratio, affine and projective transformations, cropping, among others.
- Robustness against combined distortions composed by common signal processing operations together with geometric attacks.
- Robustness against artistic filter attacks such as jitter, glass, motion blurred, among others.
- Good watermark imperceptibility.
- Oriented to color images.

The proposed watermarking method consists of the embedding and detection process, which are explained in detail as follows.

2.1 Definition of the color model

The literature in the area contains different color models which have been used to represent several color components which can be more or less independent. One of the major issues in color image processing is to find the appropriated color model for the problem being addressed [23]. Whereas the application context often defines the original color model, particularly RGB model for color images; the color model used for embedding a watermark has to be discussed according to the expectative 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 the less correlated. Also, the forward and backward transformations between RGB and YCbCr color models are linear. Taking into account this fact, if the correlated color model such like RGB is used, the modification of one component independently to the others is not necessarily the best choice, because the perceived colors are dependant of the three components together. This is the reason why the RGB model is called a correlated color model. On the other hand, YCbCr allows obtaining non-correlated components and has the advantage of separating the luminance information from the chrominance information [8,23]. According to this fact, YCbCr is adopted as suitable color model in this watermarking method.

2.2 Embedding process

Embedding process consists of two stages: frequency domain embedding and 2D histogram modification, respectively. Moreover, the embedding sequence is designed in order to avoid one embedding procedure interfering in the other.

2.2.1 Frequency domain embedding

Watermark embedding in the DFT domain has a certain number of robust properties with respect to rotation, scaling and translation (RST) invariance as well as watermark robustness against common signal processing such as JPEG compression, filtering, and noise contamination, among others. Frequency domain embedding process is described as follows, according to the next eleven steps (1) Convert the RGB color model of the original image I to YCbCr color model representation. And isolate the luminance component (Y) from YCbCr color model representation. (2) The watermark is a zero mean 1D binary pseudorandom pattern composed by {1,0} values generated by a secret key k_1, $W = \{w_i | i = 1, \ldots, L\}$, where L is the length of the watermark. (3) Apply the 2D DFT transform to the original luminance component $Y(x, y)$. The 2D DFT transform of $Y(x, y)$ of size $N_1 \times N_2$ is given by (1):

$$\mathrm{YF}(u, v) = \sum_{x=1}^{N_1} \sum_{y=1}^{N_2} Y(x, y) e^{-j2\pi(f_1 x/N_1 + f_2 y/N_2)}. \tag{1}$$

(4) Get the magnitude $M(u, v) = |\mathrm{YF}(u, v)|$ and phase $P(u, v)$ of the 2D DFT transform $\mathrm{YF}(u, v)$. Translations in the spatial domain do not affect the magnitude of the DFT transform, as shown in (2):

$$|\mathrm{DFT}[Y(x + x_1, y + y_1)]| = M(u, v). \tag{2}$$

Concerning the scaling in the spatial domain, it causes an inverse scaling in the frequency domain, as shown in (3):

$$\mathrm{DFT}[Y(\rho x, \rho y)] = \frac{1}{\rho} \mathrm{YF}\left(\frac{u}{\rho}, \frac{v}{\rho}\right). \tag{3}$$

where ρ is the scaling factor. And rotation in the spatial domain causes the same rotation in the frequency domain, as shown in (4):

$$\begin{aligned} &\mathrm{DFT}[Y(x \cos\theta - y \sin\theta, x \sin\theta + y \cos\theta)] \\ &= \mathrm{YF}(u \cos\theta - v \sin\theta, u \sin\theta + v \cos\theta) \end{aligned} \tag{4}$$

Thus, selecting the DFT domain to embed the watermark W has a certain number of advantages for rotation, scaling and translation (RST) invariance as well as watermark robustness against common signal processing. However, the DFT domain presents weak robustness against other aggressive geometric distortions such as affine and projective transformations, aspect ratio changes, flipping image, among others. Thus, in order to increase the robustness without decreasing the watermark imperceptibility, a very promising research direction consist in developing hybrid algorithms which combine the spatial and color image information [8]. In our

method, the proposed 2D histogram modification is designed to complement and increase the robustness against geometric distortions and is explained in the following section.

(5) Select a pair of radiuses r_1 and r_2 in YF $(u,\ v)$ and the annular area $A = \pi(r_2^2 - r_1^2)$ between r_1 and r_2 that should cover the middle frequency components in the DFT domain around the zero frequency term; because modifications in the magnitude of lower frequencies of the DFT will cause visible distortion in the spatial domain of the image. On the other hand, the magnitudes of the higher frequencies are vulnerable to the JPEG compression. Thus, the watermark pattern should be embedded in the band of the middle frequencies because, in this spectral region, it will be robust against JPEG compression and at the same time imperceptible. (6) Divide the DFT magnitude into four quadrants and select the middle frequencies DFT magnitude coefficients. So that to ensure the correct watermark embedding, the condition $(A/4) \geq L$ should be satisfied, where A corresponds to the annular area between radiuses r_1 and r_2, and L is the watermark length. In case that the condition $(A/4) \geq L$ is not satisfied, the pair of radiuses r_1 and r_2 can be adjusted so that the total number of magnitude coefficients in the middle frequencies is enough to embed the L watermark data bits. (7) Scramble the watermark data bits in order to guarantee their security using a self-inverse Quadratic Permutation Polynomial (QPP) over δ_2^l, where $l \geq 2$ [24]. (8) Obtain the magnitude difference denoted by d between the magnitude coefficients from first and second quadrants of the upper half part of the DFT magnitude, respectively, $d = M_i(u_j,\ v_j) - M_i\ (-u_j,\ v_j)$. (9) Once the difference d is obtained, consider a watermark strength parameter α in order to modify the DFT middle frequency magnitude in a controlled manner. If the watermark data bit $w_i = 0$ and $d < (-\alpha)$, then $M_i(u_j,\ v_j)$, $M_i\ (-u_j,\ v_j)$ are not modified. On the other hand, if $d \geq (-\alpha)$, then $M_i(u_j,\ v_j)$, $M_i(-u_j,\ v_j)$ are modified according to (5):

$$\begin{aligned} M_i'(u_j, v_j) &= M_i(u_j, v_j) - (\alpha + d) \\ M_i'(-u_j, v_j) &= M_i(-u_j, v_j) + (\alpha + d), \end{aligned} \tag{5}$$

where the difference d is added to the watermark strength α in order to force the compliance of the condition $d < (-\alpha)$ when $w_i = 0$, providing a large enough margin between $M_i'(u_j,\ v_j)$ and $M_i'\ (-u_j,\ v_j)$ in order to preserve $d < (-\alpha)$ after that the watermarked color image is processed by a common signal processing or a geometric distortion.

If the watermark data bit $w_i = 1$ and $d > \alpha$, then $M_i(u_j,\ v_j)$, $M_i\ (-u_j,\ v_j)$ are not modified. On the other hand, if $d \leq \alpha$, then $M_i(u_j,\ v_j)$, $M_i\ (-u_j,\ v_j)$ are modified according to (6):

$$\begin{aligned} M_i'(u_j, v_j) &= M_i(u_j, v_j) + (\alpha - d) \\ M_i'(-u_j, v_j) &= M_i(-u_j, v_j) - (\alpha - d), \end{aligned} \tag{6}$$

where the difference d is subtracted from the watermark strength α in order to force the compliance of the condition $d > \alpha$ when $w_i = 1$, providing a large enough margin between $M_i'(u_j,\ v_j)$ and $M_i'\ (-u_j,\ v_j)$ in order to preserve $d > \alpha$ after that the watermarked color image is processed by a common signal processing or a geometric distortion. In (5) and (6), $i = 1, \ldots, L$ denotes an index mapping corresponding to the w_i watermark data bits, $M_i(u_j,\ v_j)$, and $M_i(-u_j,\ v_j)$ denotes the original magnitude coefficients. $M_i'(u_j,\ v_j)$ and $M_i'(-u_j,\ v_j)$ denote the watermarked magnitude coefficients. A larger value of α would increase the robustness of the watermark, on the other hand, the watermark imperceptibility is less affected for a small value of α. Hence, there is a trade-off between robustness and imperceptibility. According to DFT symmetrical properties, in order to produce real values after the DFT magnitude modification, watermark was embedded into the upper half part of middle frequencies of the DFT magnitude coefficients, and subsequently, the lower half part of the middle frequency band should be modified symmetrically. By repeating the abovementioned procedure, the total L watermark data bits can be embedded in the annular region. (10) Finally, the watermarked luminance component $\mathrm{Y}_w(x,\ y)$ is obtained applying the inverse DFT (IDFT) to the watermarked magnitude $M'(u,\ v)$ and the corresponding original phase $P(u,\ v)$ as shown follows:

$$\mathrm{Y}_w = \mathrm{IDFT}(\mathrm{YF}'), \quad \mathrm{YF}' = (M',\ P). \tag{7}$$

(11) Once the watermarked luminance component Y_w is obtained, the watermarking embedding procedure is ready for switching to the 2D histogram modification and thus getting the watermarked color image, which is explained in the following section.

2.2.2 Modification of the 2D Cb–Cr histogram

In computer graphics and photography, a color histogram is a representation of the color distribution in an image, derived by accumulating the number of pixels of each color. These representations can be one-dimensional (1D), two-dimensional (2D) or three-dimensional (3D). In this paper, we use 2D Cb–Cr color histogram to embed a binary watermark sequence. The embedding process comprises the next six steps:

(1) Using the blue-difference and the red-difference (Cb–Cr) chrominance components, compute a 2D Cb–Cr color histogram $H_{\mathrm{Cb-Cr}}$. (2) Scramble the watermark data bits to guarantee their security using a self-inverse Quadratic Permutation Polynomial (QPP) over δ_2^l, where $l \geq 2$ [24]. (3) Reshape the watermark sequence W in a pattern W_r of size $L = P \times Q$ (where P and Q are any integers). (4) Segment the histogram $H_{\mathrm{Cb-Cr}}$ into blocks of size $L = P \times Q$ and

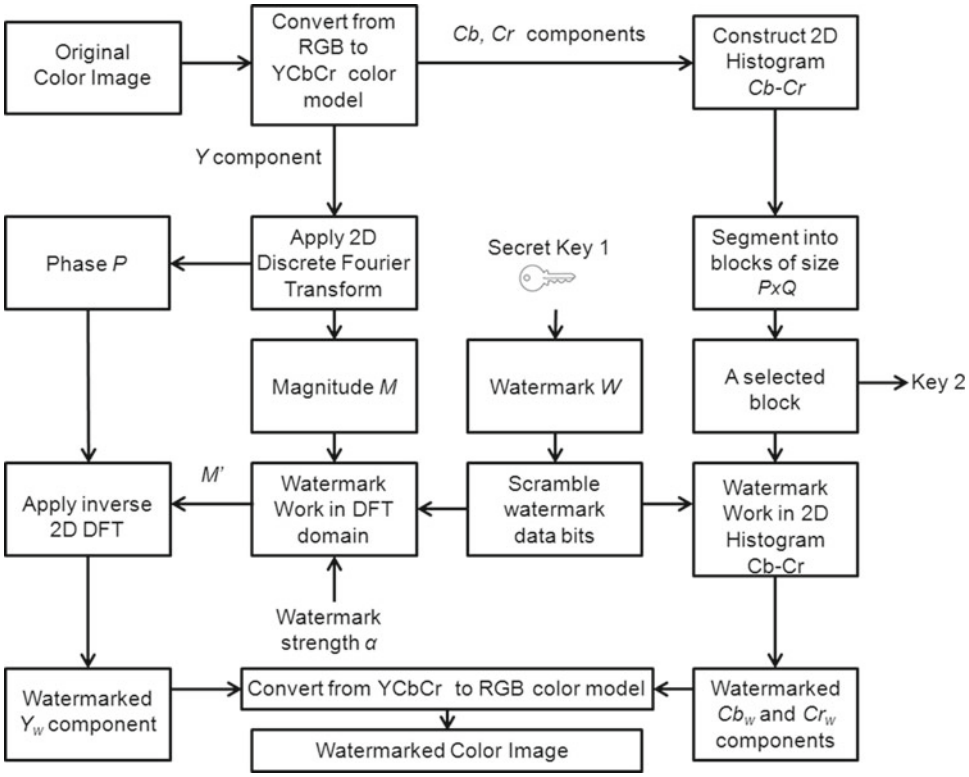

Fig. 1 General diagram of watermark embedding process

select an adequate block $\mathrm{BH}_{\mathrm{Cb-Cr}}$ to embed the watermark sequence. The principal characteristic for an adequate block to be chosen is that almost all pixel values in the block must be nonzero. Fortunately, there are many blocks that satisfy this condition; among them, one block is selected randomly, whose block number will be provided as secret key k_2 in the detection stage. The pixel value of $\mathrm{BH}_{\mathrm{Cb-Cr}}(m, n)$ is modified according to the watermark bit $W_r(m, n)$, as shown in (8):

$$\begin{aligned} &\text{if } W_r(m,n) = 0 \quad \text{then } \mathrm{BH}_{\mathrm{Cb-Cr}}(m,n) \leftarrow 0 \\ &\text{if } W_r(m,n) = 1 \quad \text{then } \mathrm{BH}_{\mathrm{Cb-Cr}}(m,n) \leftarrow 1 \\ &\qquad m = 1 \ldots P, n = 1 \ldots Q. \end{aligned} \tag{8}$$

Several situations may arise: If $W_r(m, n) = 0$ and $\mathrm{BH}_{\mathrm{Cb-Cr}}(m, n) = 0$ as well as $W_r(m, n) = 1$ and $\mathrm{BH}_{\mathrm{Cb-Cr}}(m, n) \neq 0$, then it is not necessary to modify the $\mathrm{BH}_{\mathrm{Cb-Cr}}(m, n)$. However, if these conditions are not satisfied, $\mathrm{BH}_{\mathrm{Cb-Cr}}(m, n)$ must be modified. In the upper case of (8), $\mathrm{BH}_{\mathrm{Cb-Cr}}(m, n)$ must be forced to zero, distributing its value as uniformly as possible among its four neighbors. In the lower case, $\mathrm{BH}_{\mathrm{Cb-Cr}}(m, n)$ must be forced to be nonzero, which can be achieved subtracting one pixel from its largest neighbor and assigning it to $\mathrm{BH}_{\mathrm{Cb-Cr}}(m, n)$. This embedding method ensures the watermark imperceptibility, because the modified values are assigned to the neighbor pixels, so that causes slight changes in the image colors, leaving the total number of pixels unaltered with respect to the original ones.

(5) Once the histogram $H_{\mathrm{Cb-Cr}}$ was modified, all pixel values are restored and watermarked chrominance components Cb_w and Cr_w are obtained. (6) Finally, the watermarked image I_w is constructed using the watermarked luminance component Y_w obtained in the frequency domain embedding procedure and the watermarked chrominance components Cb_w and Cr_w, thus restoring the $\mathrm{Y}_w\,\mathrm{Cb}_w\,\mathrm{Cr}_w$ watermarked components to RGB color model representation. The diagram of the embedding process is shown in Fig. 1. The secret keys k_1 and k_2 shown in Fig. 1 are also known by the watermark detector. These secret keys are used as the seed for generating the watermark pattern and the block number used in the modification of the 2D Cb–Cr histogram, respectively.

Figure 2 shows an example of original and watermarked images with their 2D Cb–Cr color histograms, respectively.

2.3 Detection process

The detection process diagram is shown in Fig. 3 and it is described as follows:

(1) Convert the RGB color model of the watermarked image I_w to YCbCr color model representation and obtain the watermarked components $\mathrm{Y}_w\mathrm{Cb}_w\mathrm{Cr}_w$. (2) Using the blue-difference and the red-difference (Cb_w–Cr_w) watermarked chrominance components, compute a 2D Cb_w–Cr_w color histogram $H_{\mathrm{Cbw-Crw}}$, which is segmented into blocks of size

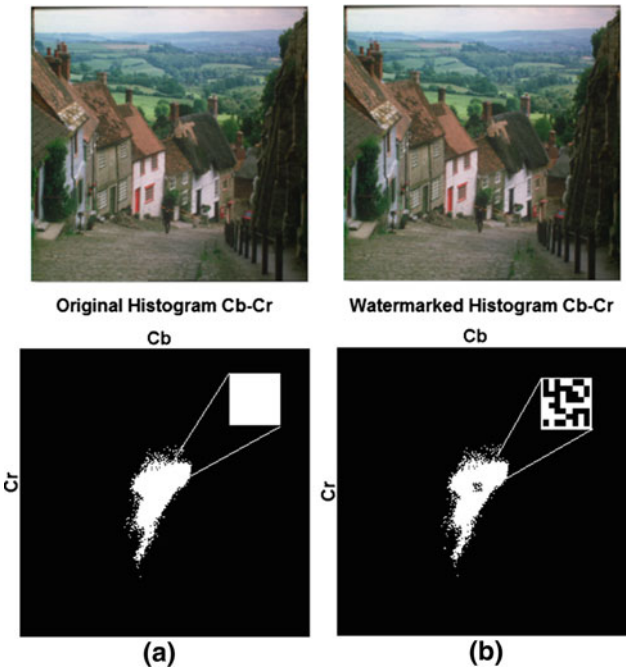

Fig. 2 Example of original and watermarked Gold hill images with their 2D Cb–Cr color histogram. **a** Original image and 2D Cb–Cr color histogram with zoom of the selected region. **b** Watermarked image and 2D Cb–Cr color histogram with zoom of the watermarked region (color figure online)

$L = P \times Q$. (3) Using secret key k_2 extract the region Hr_W, in which the watermark was embedded. From this region, the watermark pattern W_1 is extracted according to the following conditions: if $\mathrm{Hr}_W(m, n) > 0$ then $W_1(m, n) = 1$, otherwise $W_1(m, n) = 0, m = 1 \ldots P, n = 1 \ldots Q$. (4) Reorder the watermark pattern W_1 into a 1D stream. (5) Once the watermark pattern W_1 is restored, obtain the bi-dimensional DFT transform $(\mathrm{YF}'u, v)$ of the watermarked luminance component $\mathrm{Y}_w(x, y)$. Then, from $(\mathrm{YF}'u, v)$ the watermarked magnitude $M'(u, v) = |\mathrm{YF}'(u, v)|$ and phase $P(u, v)$ are obtained. (6) The annular area A is computed with the same pair of radiuses r_1 and r_2 used in the frequency domain embedding process. (7) Split the DFT magnitude $M'(u, v)$ in four quadrants and obtain the result of applying the subtraction operation $s_i = M'_i(u_j, v_j) - M'_i(-u_j, v_j)$ of the first and second quadrants of the upper half part of the watermarked DFT magnitude of the annular region A. (8) Recover the watermark pattern W_2 using the sign function as follows: if $\mathrm{sign}(s_i)$ is '+' or '0' then $w'_i = 1$, otherwise $w'_i = 0$, where $i = 1, \ldots, L$. (9) Once W_1 and W_2 are recovered, re-arrange each one using the self-inverse Quadratic Permutation Polynomial (QPP) used in each embedding stage. (10) Reconstruct the original watermark pattern W with the secret key k_1 and obtain the bit error rate (BER) between W and W_1.

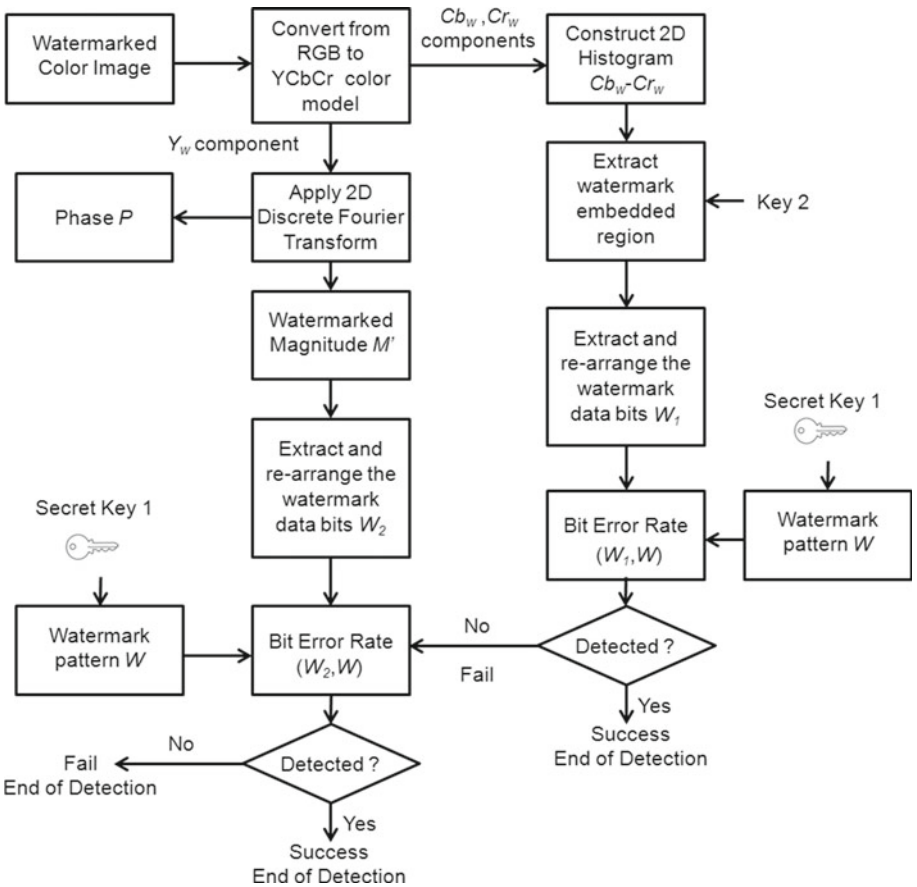

Fig. 3 General diagram of watermark detection process

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 whether 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 r bits embedded watermark data is given by (9), and a threshold value T must be controlled in order to make P_{fa} smaller than a predetermined value.

$$P_{\mathrm{fa}} = \sum_{l=T}^{r} \left(\frac{1}{2}\right)^{r} \cdot \left(\frac{r!}{l!(r-l)!}\right), \tag{9}$$

where r is the total number of watermark data bits, whose value is empirically set to 64. The false alarm probability must be less than $P_{\mathrm{fa}} = 9.4048 \times 10^{-7}$ which is to be able to satisfy the requirements of most watermarking applications for a reliable detection, and then, an adequate threshold value $T_{\mathrm{BER}} (= 1 - (T/r) = 1 - (51/64))$ is equal to 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_1 is greater than 20 % (more than 13 error bits), the watermark detection is failed, and then, the detection process switch to obtain the BER between W and W_2, otherwise, the watermark detection is successful and the detection process is terminated. The same condition is applied to the BER between W and W_2; if this is greater than 20 %, the watermark detection is failed and the detection process is terminated, otherwise, the watermark detection is successful and the detection process is terminated.

3 Experimental results

In this section, the performance of the proposed algorithm is evaluated considering the watermark payload, imperceptibility and robustness grades using a variety of digital images. We have used many images with different texture content (e.g., Goldhill, Sailboat, Lena, Airplane, Baboon, Peppers, among others) of size 512 × 512 and color resolution of 24bits per pixel which can be found in http://sipi.usc.edu/database/. Our experiments are carried out on a personal computer running win7© with an AMD© Athlon processor (2.7 Ghz) and 4 GB RAM while the embedding and extracting procedures were implemented on Matlab© 7.10. In our system, the average computing time for the embedding procedure has been 11.85 s while an average of 8.72 s was needed for the detection procedure. A 1D binary pseudorandom sequence of size $L = 64$ bits is used as the watermark pattern W. The false alarm probability is $P_{\mathrm{fa}} = 9.4048 \times 10^{-7}$ when $T_{\mathrm{BER}} = 0.20$. The pair of radiuses used in the frequency domain embedding were $r_1 = 80$ and $r_2 = 81$. The watermark strength used

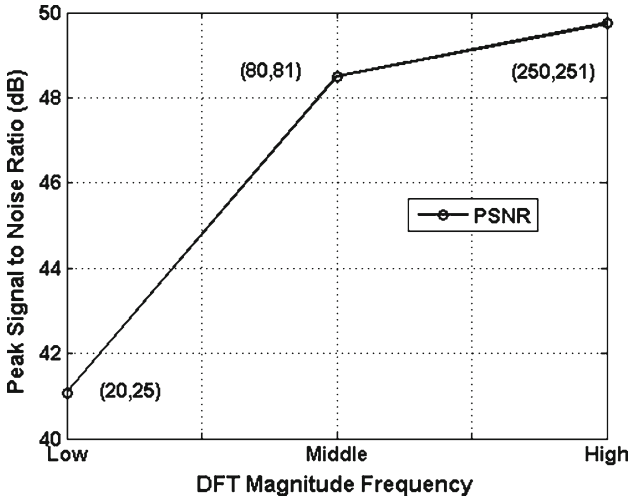

Fig. 4 Average PSNR after the watermark embedding in each spectral region. Radiuses $r_1 = 20$, $r_2 = 25$ for low, $r_1 = 80$, $r_2 = 81$ for middle and $r_1 = 250$, $r_2 = 251$ for high DFT magnitude frequency

in the frequency domain embedding is equal to α = 15,000. P and Q integers used in the 2D Cb–Cr histogram modification have the values of $P = 8$ and $Q = 8$ when $L = 64$. The watermarked image quality is measured using the following well-known indices PSNR, VIF and SSIM. The difference color of the watermarked image is obtained using the NCD measure. Finally, our experimental results are compared with previous reported watermarking works.

3.1 Settings of radiuses r_1, r_2 and watermark strength α

Considering the frequency domain embedding process into the luminance component (Y) from YCbCr color model of the original color image, a watermark strength α = 15,000, a pair of experimental radiuses $r_1 = 20$, $r_2 = 25$ for low, $r_1 = 80$, $r_2 = 81$ for middle and $r_1 = 250$, $r_2 = 251$ for high DFT magnitude frequency, respectively, and a value of $L = 64$, in Fig. 4, we show the average PSNR after the watermark embedding in each spectral region, obtaining 41.08 dB for low, 48.50 for middle and 49.75 for high DFT magnitude frequency, respectively. Although it may be considered that an acceptable average PSNR is 41.08 dB, the modifications in the magnitude of lower frequencies of the DFT will cause visible distortion in the spatial domain of the image. To illustrate the visible distortions in the spatial domain, in Fig. 5, we show the watermarked Lena image when watermark was embedded into the low (a), middle (b) and high (c) DFT magnitude frequency, with 38.95, 49.45 and 49.76 dB, respectively. On the other hand, the magnitudes of the higher frequencies are vulnerable to the JPEG compression. Considering the same parameters used in the above experiment and applying a JPEG compression to the watermarked image with quality factor equals to 20, in Fig. 6 we show the average BER after the watermark embedding in each spectral

Fig. 5 Visible distortions in the spatial domain from watermarked Lena image when watermark was embedded into the low (**a**), middle (**b**) and high (**c**) DFT magnitude frequency, with 38.95, 49.45 and 49.76 dB, respectively

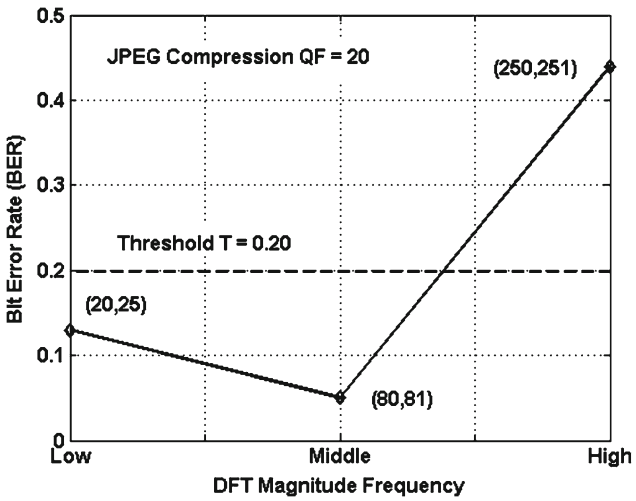

Fig. 6 Average BER after the watermark embedding in each spectral region. BER = 0.13 for low, BER = 0.05 for middle and BER = 0.44 for high DFT magnitude frequency, respectively

region, obtaining 0.13 for low, 0.05 for middle and 0.44 for high DFT magnitude frequency respectively. In low and middle frequencies, we have obtained BER values less than the threshold value $T_{\text{BER}} = 0.20$, however, using the high frequencies, the BER value is greater than the threshold value $T_{\text{BER}} = 0.20$, confirming the vulnerability of the higher frequencies against JPEG compression. Thus, the watermark pattern should be embedded in the band of the middle frequencies $r_1 = 80$, $r_2 = 81$ because, in this spectral region, it will be robust against JPEG compression and at the same time imperceptible.

Once that the pair of radiuses $r_1 = 80$ and $r_2 = 81$ are set, considering a value of $L = 64$ and the variable watermark strength α with values 1,000, 5,000, 10,000, 15,000 and 20,000, respectively, the suitable watermark strength α is estimated. For this test, the watermarked image is attacked by an aggressive JPEG compression with QF = 10. In Table 1, we show the BER obtained for each value of α in order to obtain the more robust value against this signal processing and illustrate the reason of the selected range of values α. When the BER value is greater than 20 % (more than 13 error

Table 1 Average BER obtained with variable watermark strength α against JPEG with QF = 10

BER				
α =1,000	α = 5,000	α = 10,000	α = 15,000	α = 20,000
0.46	*0.42*	*0.26*	0.15	0.14

bits), the watermark detection is reported in *italics* and indicates that the watermark detection has failed. From Table 1, we show that α values greater than or equal to 15,000 presents good robustness against JPEG QF = 10p; however, to preserve the trade-off between robustness and imperceptibility, based on our experiments, we considered a watermark strength $\alpha = 15{,}000$ as a suitable value.

3.2 Watermark payload

Considering the frequency domain embedding process into the luminance component (Y) from YCbCr color model of the original color image, a watermark strength α = 15,000, a pair of radiuses $r_1 = 80$ and $r_2 = 81$ and variable value of L from 16 to 512 bits have been used. In Fig. 7, we show that a large value of L would increase the capacity of the watermarking method; however, the robustness of the watermarking algorithm would decrease for large L. Hence, there is a trade-off between capacity and robustness. From Fig. 7, we show that for $L = 16$ to 64, the BER obtained are null, which indicates a good performance in robustness terms. On the other hand, while the value of L is increased, the robustness is affected. According to this behavior, $L = 16$, 32 or 64 are considered a suitable set of values. In order to preserve the trade-off between capacity, robustness and imperceptibility, in the proposed watermarking method, we adopted the value $L = 64$ in conjunction with the rest of the frequency domain embedding parameters.

3.3 Watermark imperceptibility

As explained in the previous paragraphs, the proposed algorithm embeds a watermark sequence twice in two different

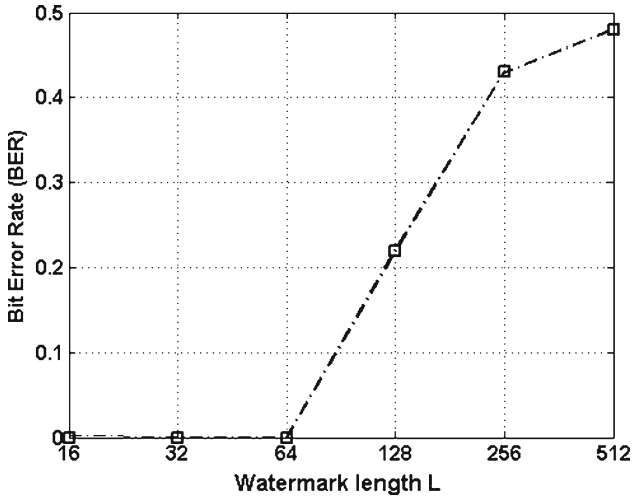

Fig. 7 Bit error rate with watermark length L variable

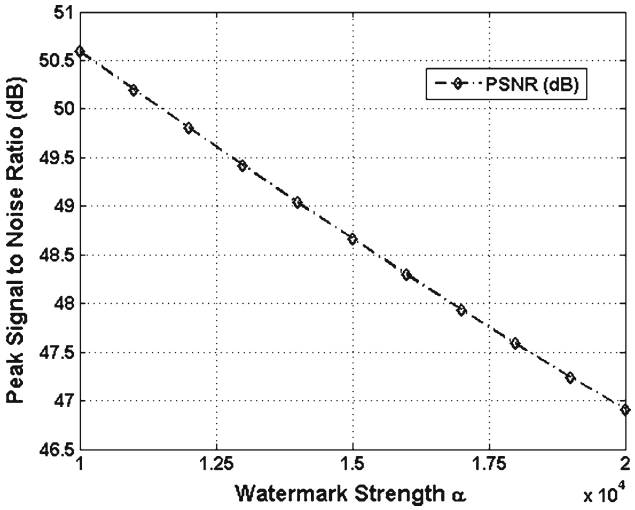

Fig. 8 Average PSNR (dB) obtained with variable watermark strength α

domains, i.e., DFT frequency domain and 2D histogram, respectively; therefore careful watermark imperceptibility evaluation is compulsory. Using a pair of radiuses $r_1 = 80$ and $r_2 = 81$, watermark length $L = 64$ and variable watermark strength α from 10 to 20 $\times 10^3$; the watermark imperceptibility was evaluated in terms of the PSNR, VIF [25] and SSIM [26] image quality metrics defined by (10), (11) and (12), respectively.

$$\mathrm{PSNR(dB)} = 10\log_{10}\left(\frac{\mathrm{MaxPixelValue}^2}{(\mathrm{MSE}_Y + \mathrm{MSE}_{\mathrm{Cb}} + \mathrm{MSE}_{\mathrm{Cr}})/3}\right), \quad (10)$$

$$\mathrm{VIF} = \frac{\sum_{k\in\mathrm{channels}} I(\vec{C}^{Z,k}; \vec{F}^{Z,k}|s^{Z,k})}{\sum_{k\in\mathrm{channels}} I(\vec{C}^{Z,k}; \vec{E}^{Z,k}|s^{Z,k})}, \quad (11)$$

where we sum over the channels of interest, $\vec{C}^{Z,k}$ represent Z elements of the random field RF C_k that describes the coefficients from channel k and so on [25]. E and F 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 brain extracts cognitive information. $I(\vec{C}^{Z,k}; \vec{E}^{Z,k}|s^{Z,k})$ and $I(\vec{C}^{Z,k}; \vec{F}^{Z,k}|s^{Z,k})$ represent the information that can ideally be extracted by the brain from a particular channel in the original and the watermarked images, respectively, [25].

$$\mathrm{SSIM}(I_o, I_w) = \frac{(2\mu_{I_o}\mu_{I_w} + C_1)(2\sigma_{I_oI_w} + C_2)}{(\mu_{I_o}^2 + \mu_{I_w}^2 + C_1)(\sigma_{I_o}^2 + \sigma_{I_w}^2 + C_2)}. \quad (12)$$

where I_o, I_w are original and watermarked images, respectively, and C_1, C_2 are small constant values [26].

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 better fidelity with respect to the original image. Also it is well known in the literature that the SSIM value reflects perceptual

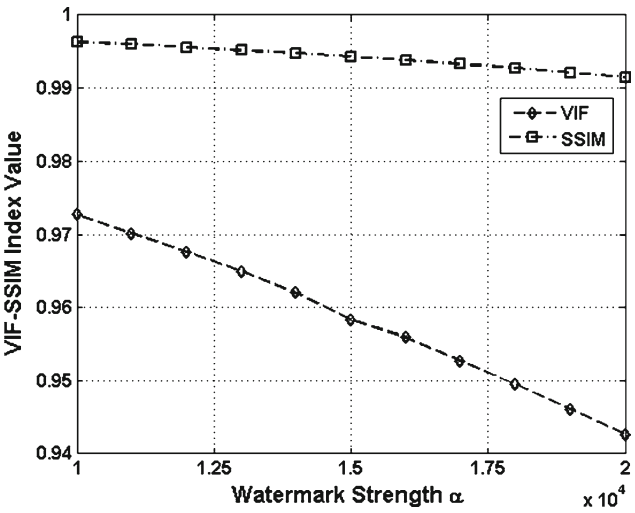

Fig. 9 Average VIF and SSIM obtained with variable watermark strength α

distortions more precisely than PSNR. The range of SSIM is [0, 1], and the closer value to 1 represents the better quality with respect to the original image; a value 1 indicates that the original and the reference image are the same. In Figs. 8 and 9, the average PSNR and VIF-SSIM are plotted with variable watermark strength α ranging from 10 to 20 $\times$ 10^3, respectively. As shown in Figs. 8 and 9, a larger value of α would increase the robustness of the watermark, but 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 α = 15,000 as a suitable value. On the other hand, the normalized color difference NCD [27,28] is based on the CIELAB color space and it is applied to measure the

Table 2 Watermark imperceptibility measured in terms of PSNR, VIF, SSIM and NCD

Images	PSNR (dB)	VIF	SSIM	NCD
Lena	49.4524	0.9625	0.9947	0.0074
Mandrill	47.7395	0.9589	0.9975	0.0084
Barbara	47.58	0.952	0.9936	0.0105
Gold hill	49.1461	0.9627	0.9954	0.0217
Tiffany	50.1741	0.9657	0.996	0.0049
Sailboat	48.4433	0.9629	0.9952	0.0088
Boats	48.0253	0.9409	0.9922	0.0129
House	48.2842	0.9581	0.994	0.0078
Peppers	49.444	0.9644	0.9949	0.0074
Airplane	48.4654	0.9565	0.9926	0.0066

difference of color between two images. NCD is given by (13) [27,28]:

$$\mathrm{NCD} = \frac{\sum_{x=1}^{N_1}\sum_{y=1}^{N_2}\left(\sqrt{(L_o(x,y)-L_w(x,y))^2+(a_o(x,y)-a_w(x,y))^2+(b_o(x,y)-b_w(x,y))^2}\right)}{\sum_{x=1}^{N_1}\sum_{y=1}^{N_2}\left(\sqrt{(L_o(x,y))^2+(a_o(x,y))^2+(b_o(x,y))^2}\right)}, \tag{13}$$

where L_o, L_w represents lightness values and a_o, a_w, b_o, b_w the chrominance values corresponding to the original I_o and watermarked I_w images expressed in the CIE Lab color space.

Finally, using $r_1 = 80$ and $r_2 = 81$, α = 15,000, $P = 8$ and $Q = 8$ with $L = 64$, in Table 2, we show the values of PSNR, VIF, SSIM and NCD of ten watermarked test images with respect to the original ones, and in Fig. 10, some original images (a–f) together with their watermarked version (g–l) are shown.

From Table 2 and Fig. 10, it follows that the proposed scheme provides a fairly good fidelity of the watermarked image, and also, the difference of colors between the watermarked image and the original one is insignificant [29]. From Table 2, we show that the average PSNR is greater than 47 dB, and the SSIM as well as VIF values obtained are near to 1; it follows that the proposed scheme provides a fairly good fidelity of the watermarked image.

3.4 Watermark robustness

To evaluate the watermark robustness of the proposed algorithm, the StirMark Benchmark available on http://www.petitcolas.net/fabien/watermarking/stirmark/, combined attacks of the several geometrical distortions-common signal processing and artistic filter attacks supported by Photoshop® are carried out. Experimental results are classified in geometric, common signal processing, combined distortions and artistic filter attacks. For illustrative purposes, Table 3 shows the BER obtained after applying geometric distortions to five watermarked test images: Mandrill, Gold hill, Sailboat, Boats and Airplane F16. When the BER value is greater than 20 % (more than 13 error bits), the watermark detection is reported in *italics* and indicates that the watermark detection has failed. The detection results are displayed in a 2D-H/DFT form, where 2D-H is the reference to the 2D histogram modification detector output, and DFT corresponds to the frequency domain detector output.

From Table 3, we conclude that the proposed method presents good robustness against several geometric distortions, including scaling from 0.3 to 2, rotation with different angles with and without auto-cropping with re-scaling, general affine transformation, shearing 20 % in x and y directions, centered and common cropping attack with 35 and 75 %, respectively, aspect ratio in x and y directions by 1.5 and 1, respectively, translation by $x = 100$ and $y = 100$, shearing 5 % in each axis, and flipping horizontal, vertical and projective transformation with [0 0; 1 0; 1 1; 0 1], [−4 2; −8 −3; −3 −5; 6 3]. In all cases, we have obtained BER values less than the threshold value $T_{\mathrm{BER}} = 0.20$. In Table 3, we show that both detectors (2D-H/DFT) present good robustness against RST geometric attacks and centered cropping. However, while the DFT detector fails against scaling when the factor is 0.3 as well as to the rest of geometric distortions, the 2D-H detector preserves the good robustness against aggressive attacks, such as 75 % cropping with re-scaling, affine transformation, projective transformation, and rotation with auto-cropping and re-scaling. Because the image histogram is one of the geometric invariant domains, if the watermark can be embedded into this domain, it should survive to most geometric transformations. In Fig. 11, we show the watermarked image before and after applying the above-mentioned aggressive geometric attacks together with the 2D Cb–Cr histogram, and the zoom of the recovered watermarked region into the histogram.

For illustrative purposes, Table 4 shows the BER obtained after applying several signal processing to five watermarked test images: Mandrill, Gold hill, Sailboat, Boats and Airplane F16. From Table 4, we show that also the proposed method presents good robustness against several common signal processing operations, such as JPEG compression with several quality factors ranging from 70 to 10; which presents robustness against adjust brightness and contrast, impulsive noise with a density of 0.02 and 0.10, Gaussian noise perturbation with zero mean and variance 0.005 and 0.015, Gaussian filter with window size 3 × 3, median filter

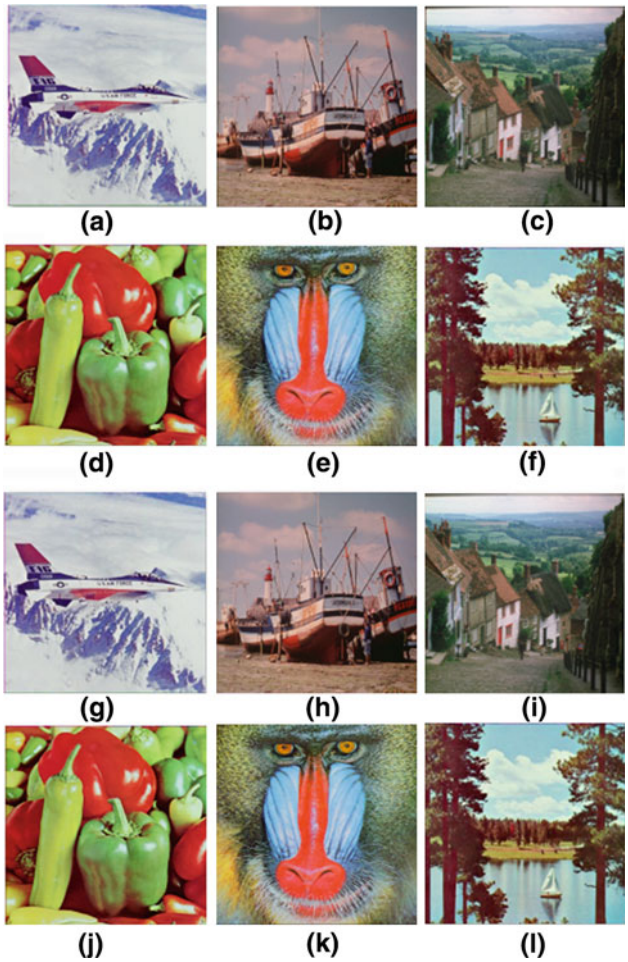

Fig. 10 Original (**a**–**f**) and watermarked (**g**–**l**) six test images

with windows sizes 3 × 3 and 9 × 9, sharpening by 3 × 3, and histogram equalization are also consider.

In all cases, we obtain a BER value less than the threshold value $T_{\mathrm{BER}} = 0.20$, except when the watermarked image was compressed with JPEG QF = 10. In Table 4, we show that the DFT detector presents good robustness against all signal processing operations, obtaining BER values less than or near to 0, except when the watermarked image was corrupted by impulsive noise with density equals to 0.10. However, the 2D-H detector fails against all signal processing distortions, except for the impulsive noise, because, as it is well known and happened in several works reported previously in the literature, several image processing may change the histogram distribution of an image, causing the loss of the watermark representation carried out by the histogram modification [21,22].

For illustrative purposes, Table 5 shows the BER obtained applying combined distortions to five watermarked test images: Mandrill, Gold hill, Sailboat, Boats and Airplane F16. The combined distortions are composed of a JPEG compression with quality factor QF = 20 together with a common signal processing and geometric attacks. From Table 5, we show that also the proposed method presents good robustness against several aggressive combined attacks composed by a JPEG 20 compression together with a common signal processing and geometric attacks, specifically scaling from 0.5 to 2, rotation with different angles with and without auto-cropping with re-scaling, centered cropping attack with 35 %, translation by $x = 100$ and $y = 100$, adjust brightness and contrast, impulsive noise with a density of 0.02, Gaussian noise perturbation with zero mean and variance 0.005, several

Table 3 BER obtained from five test watermarked images after geometric distortions

Attack	Mandrill 2D-H/DFT	Gold hill 2D-H/DFT	Sailboat 2D-H/DFT	Boats 2D-H/DFT	Airplane 2D-H/DFT
Un-watermarked	*0.53/0.53*	*0.53/0.51*	*0.48/0.45*	*0.53/0.57*	*0.53/0.54*
Rotation 75°	0/0.01	0/0	0/0.01	0/0	0/0
Rotation 75° auto-crop and re-scaling	0/0.06	0.01/0	0/0.09	0/0.03	0/0.04
Translation $x = 100$, $y = 100$	0/0.01	0/0	0/0.01	0/0	0/0
Centered cropping 35 %	0/0.01	0/0	0/0.01	0/0	0/0
Scaling fs = 0.3	0/*0.50*	0/*0.25*	0/*0.23*	0.01/*0.31*	0/*0.23*
Scaling fs = 0.5	0/0.06	0/0.03	0/0.04	0/0	0/0
Scaling fs = 2	0/0.01	0/0	0/0.01	0/0	0/0
Flip horizontal and vertical	0/*0.61*	0/*0.42*	0/*0.56*	0/*0.43*	0/*0.51*
Affine [0.9, 0.2,0; 0.1, 1.2, 0; 0, 0, 1]	0/*0.47*	0.01/*0.54*	0/*0.50*	0/*0.39*	0/*0.43*
Cropping 75 %	0/*0.43*	0/*0.56*	0/*0.58*	0/*0.51*	0/*0.56*
Shearing (0.5, 0.5)	0/*0.51*	0.01/*0.56*	0/*0.42*	0/*0.54*	0/*0.46*
Aspect ratio (1.5, 1)	0/0.20	0/0.09	0/0.17	0/0.20	0/0.06
Projective [0 0; 1 0; 1 1; 0 1], [−4 2; −8 −3; −3 −5; 6 3]	0/*0.57*	0.01/*0.46*	0/*0.51*	0/*0.51*	0/*0.56*

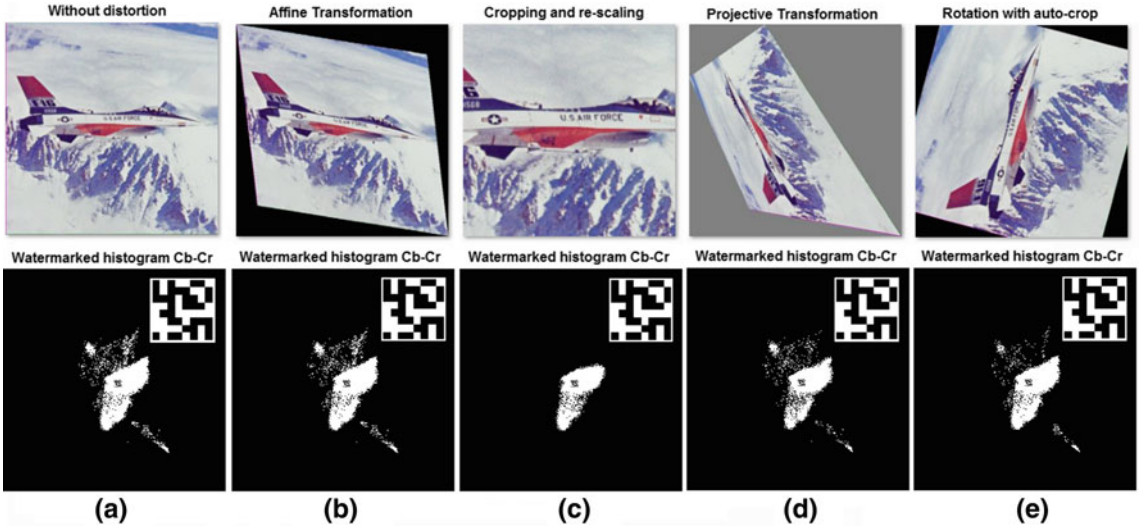

Fig. 11 Watermarked image before and after aggressive geometric attacks, and the 2D Cb–Cr histogram modification together with the zoom of the recovered watermarked region into the histogram. **a** Without distortion. **b** Affine transformation. **c** Cropping with re-scaling. **d** Projective transformation and **e** rotation with auto-cropping and re-scaling

Table 4 BER obtained from five test watermarked images after signal processing distortions

Attack	Mandrill 2D-H/DFT	Gold hill 2D-H/DFT	Sailboat 2D-H/DFT	Boats 2D-H/DFT	Airplane 2D-H/DFT
JPEG compression 70	*0.45*/0.01	*0.56*/0	*0.42*/0.01	*0.45*/0	*0.45*/0
JPEG compression 50	*0.45*/0.01	*0.56*/0	*0.45*/0.01	*0.43*/0	*0.45*/0.01
JPEG compression 20	*0.45*/0.01	*0.59*/0.03	*0.45*/0.07	*0.45*/0.06	*0.43*/0.07
JPEG compression 10	*0.43*/0.10	*0.56*/0.18	*0.45*/*0.23*	*0.46*/*0.32*	*0.43*/*0.28*
Brightness	*0.53*/0.04	*0.53*/0	*0.53*/0.01	*0.53*/0.01	*0.51*/0.01
Contrast	*0.53*/0.01	*0.53*/0.01	*0.53*/0.01	*0.53*/0	*0.53*/0
Gaussian noise (0, 0.005)	*0.53*/0.04	*0.53*/0.04	*0.53*/0.04	*0.53*/0.04	*0.53*/0.03
Gaussian noise (0, 0.015)	*0.53*/0.12	*0.53*/0.17	*0.53*/0.12	*0.53*/0.14	*0.53*/0.06
Impulsive noise density 0.02	0.01/0.03	0.09/0.04	0.01/0.03	0.09/0.04	0/0.01
Impulsive noise density 0.10	0.09/0.18	0.14/*0.28*	0.06/*0.21*	0.14/*0.20*	0/*0.23*
Median filter 3 × 3	*0.53*/0.01	*0.53*/0	*0.53*/0.01	*0.54*/0	*0.53*/0
Median filter 9 × 9	*0.53*/0.14	*0.53*/0.17	*0.48*/0.18	*0.50*/0.18	*0.53*/0.10
Sharpen	*0.53*/0.03	*0.53*/0	*0.53*/0.01	*0.53*/0	*0.53*/0
Gaussian filter 3 × 3	*0.53*/0.01	*0.53*/0	*0.53*/0.01	*0.53*/0	*0.53*/0
Histogram equalization	*0.56*/0.01	*0.55*/0	*0.54*/0.01	*0.55*/0	*0.57*/0

filters including median and Gaussian filters, sharpening, all of them with a window size of 3 × 3 and histogram equalization. The robustness of our method is not affected by this kind of combined attacks, obtaining BER values less than $T_{\mathrm{BER}} = 0.20$ in the DFT detector output.

The watermark is also robust against artistic filter attacks (supported by Photoshop®) such as brightness of lens, cellophane effect, film effect, old photo, glass, engraving, newsprint, jitter, vignette frame, motion blurred, texture add and tiles as shown in Table 6 and depicted in Fig. 12. From Table 6, we show that also the proposed method presents good robustness against several artistic filters, obtaining watermark detection rates greater than 93 % in the DFT detector output.

Finally, this investigation compares the performance of the proposed method with the invariant domain algorithm developed by Wang et al. [30] in 2008, the histogram-oriented watermarking algorithm proposed by Lin et al. [19] in 2006, the watermarking color histogram scheme developed by Roy et al. [18] in 2004 and the hybrid watermarking based on chaos and histogram modification scheme proposed by Chrysochos et al. [22] in 2012, under JPEG lossy, scaling, cropping, affine transformation, rotation, projective transformation, Gaussian noise and artistic filters

Table 5 BER obtained from five test watermarked images after combined distortions

Attack	Mandrill 2D-H/DFT	Gold hill 2D-H/DFT	Sailboat 2D-H/DFT	Boats 2D-H/DFT	Airplane 2D-H/DFT
JPEG 20 + rotation 75°	*0.45*/0.09	*0.59*/0.07	*0.45*/0.12	*0.45*/0.17	*0.43*/0.15
JPEG 20 + rotation 75° auto-crop and re-scaling	*0.48*/0.10	*0.56*/0.09	*0.42*/0.14	*0.45*/0.17	*0.45*/0.16
JPEG 20 + translation $x = 100$, $y = 100$	*0.45*/0.01	*0.59*/0.03	*0.45*/0.07	*0.45*/0.12	*0.43*/0.09
JPEG 20 + centered cropping 35 %	*0.43*/0.03	*0.59*/0.03	*0.45*/0.09	*0.45*/0.16	*0.43*/0.10
JPEG 20 + scaling fs = 0.5	*0.45*/0.09	*0.59*/0.01	*0.42*/0.06	*0.46*/0.17	*0.44*/0.10
JPEG 20 + scaling fs = 2	*0.45*/0.01	*0.59*/0.03	*0.45*/0.07	*0.45*/0.12	*0.43*/0.09
JPEG 20 + brightness	*0.53*/0.04	*0.53*/0.07	*0.51*/0.12	*0.51*/0.10	*0.53*/0.12
JPEG 20 + contrast	*0.53*/0.03	*0.53*/0.03	*0.54*/0.09	*0.53*/0.12	*0.53*/0.09
JPEG 20 + Gaussian noise (0, 0.005)	*0.53*/0.06	*0.53*/0.10	*0.53*/0.10	*0.53*/0.18	*0.53*/0.17
JPEG 20 + impulsive noise 0.02	*0.46*/0.07	*0.59*/0.09	*0.45*/0.17	*0.48*/0.15	*0.44*/0.14
JPEG 20 + median filter 3 × 3	*0.53*/0.01	*0.53*/0.03	*0.51*/0.09	*0.53*/0.12	*0.53*/0.10
JPEG 20 + sharpen	*0.53*/0.03	*0.53*/0.01	*0.55*/0.09	*0.53*/0.07	*0.53*/0.10
JPEG 20 + Gaussian filter 3 × 3	*0.51*/0.01	*0.53*/0.03	*0.51*/0.09	*0.53*/0.12	*0.53*/0.09
JPEG 20 + histogram eq.	*0.56*/0.04	*0.55*/0.05	*0.54*/0.09	*0.55*/0.10	*0.57*/0.10

Table 6 BER obtained from watermarked Lena image after artistic filters

Attack	Image Lena	
	2D-H	DFT
(a) Brightness of lens	0.53	0
(b) Cellophane effect	0.53	0.03
(c) Film effect	0.48	0
(d) Old photo	0.46	0.07
(e) Glass	0.50	0.07
(f) Engraving	0.46	0.03
(g) Newsprint	0.50	0.03
(h) Jitter	0.50	0.03
(i) Vignette frame	0.45	0.06
(j) Motion Blurred	0.46	0
(k) Texture added	0.53	0.07
(l) Tiles	0.54	0

distortions. Table 7 compares the performance of the watermark detector outputs, the watermark data length and the kind of image associated with each algorithm. Table 7 presents also the tolerance under distortions and designates the capacity to resist as either "detected" or "fail," when the tolerance is not given in detail by the other four methods mentioned above. A grid-cell is marked with a dash for attack simulations not mentioned in the literature. These results show better performance of the proposed method compared with principal methods reported previously against most common geometric, signal processing and artistic filter attacks.

4 Conclusions

In this paper, we present a robust hybrid watermarking method for authentication, which is very robust against geometric distortions including rotation by several angles with and without cropping, affine transformation, projective transformation, scaling, aspect ratio and aggressive cropping attacks among others. Also, the method is robust against several common signal processing distortions such as JPEG compression, median and Gaussian filtering, impulsive and Gaussian noise perturbation, brightness, contrast and sharpen and histogram equalization. The method presents good robustness against combined distortions composed by several geometric and signal processing attacks. In the experiments, the watermark is also robust against artistic filter attacks supported by Photoshop® such as brightness of lens, cellophane effect, film effect, old photo, glass, engraving, newsprint, jitter, vignette frame, motion blurred, texture add and tiles. In the first embedding technique, the luminance component (Y) information is used to embed the watermark bit sequence into the magnitude of the middle frequencies of the Discrete Fourier Transform (DFT). While in the second one, a selected region of 2D histogram composed by blue-difference and red-difference (Cb–Cr) chrominance components is modified according to the watermark bit sequence. In this way, this hybrid watermarking scheme combines the robustness of DFT domain against RST geometric distortions, JPEG compression, noise, filtering attacks and other common signal processing, with the robustness of histogram domain against geometrical attacks. Other hybrid watermarking schemes like the one reported in [22] which shows similar performance to the proposed method against

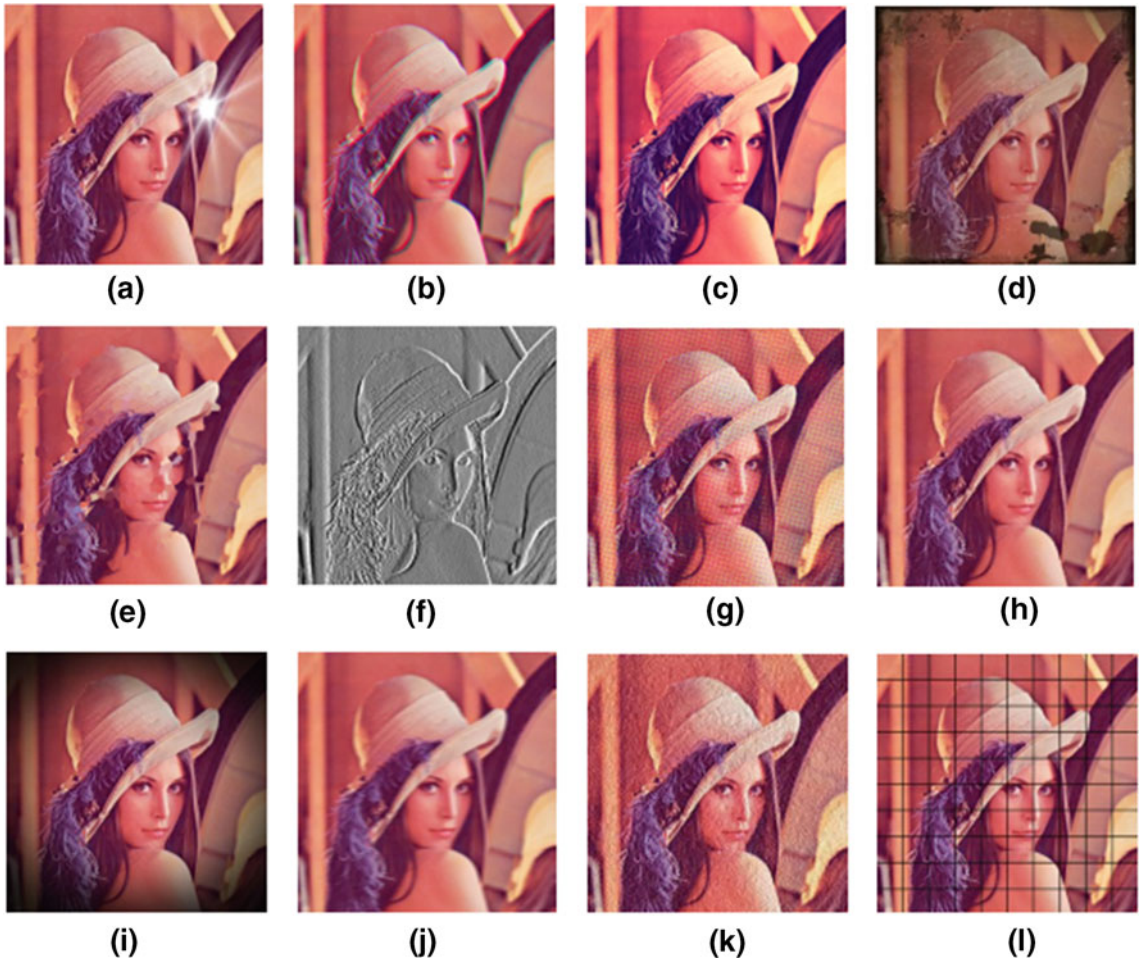

Fig. 12 Artistic filters in watermarked Lena image

Table 7 Performance comparison

Comparison	Wang et al. [30] (SIFT-DFT based)	Lin et al. [19] (3D histogram-oriented)	Roy et al. [18] (2D color histogram)	Chrysochos et al. [22] (hybrid chaos-1D histogram)	Proposed method (hybrid DFT-2D histogram)
JPEG (quality factor)	30–100	20–100	Detected	25–100	20–100
Scaling	0.8–1.2	0.75–1.5	Detected	Detected	0.5–2
Cropping	Up to 10 %	Up to 15 %	Up to 60 %	Fail	Up to 75 %
Affine	–	Detected	–	–	Detected
Rotation	0°–20°	0°–10°	Detected	0–360 %	0°–360°
Projective	–	–	–	–	Detected
Gaussian noise	Detected	–	Detected	(0, 0.95)	(0, 0.015)
Artistic filters	–	–	–	Success	Success
Watermark length	32 bits	128 bits	61 bits	30 bits	64 bits
Image kind	Grayscale	Color	Color	Grayscale	Color

geometric, signal processing and artistic filters is outperformed in terms of robustness against cropping attack as well as to the combined attacks that involves this geometrical distortion.

Acknowledgments We thank the Program of Post Doctoral Scholarships DGAPA in the UNAM of Mexico, the National Polytechnic Institute of Mexico by support provided during the realization of this research, and DGAPA-UNAM project PAPIIT IN-112513.

References

1. Ruanaidh, J.Ó., Pun, T.: Rotation, scale and translation invariant spread spectrum digital image watermarking. Signal Process. **66**, 303–317 (1998)
2. Bum-Soo, K., Jae-Gark, C., Chul-Hyun, P., Jong-Un, W., Dong-Min, K., Sang-Keun, O., et al.: Robust digital image watermarking method against geometrical attacks. Real-Time Imaging **9**, 139–149 (2003)
3. Ridzon, R., Levicky, D.: Log-Polar Mapping in Robust Digital Image Watermarking. Institute of Electric and Electronics Engineers Computer Society, Brno (2007)
4. Yan, L., Jiying, Z.: A new video watermarking algorithm based on 1D DFT and Radon transform. Signal Process. **90**, 626–639 (2010)
5. Dong, P., Brankov, J.B., Galatsanos, N.P., Yang, Y., Davoine, F.: Digital watermarking to geometric distortions. IEEE Trans. Image Process. **14**(12), 2140–2150 (2005)
6. Cedillo, M., Nakano, M., Perez, H.: A robust watermarking technique based on image normalization. Rev. Fac. Ing. Univ. Antioquia J. Eng. Fac. Univ. Antioquia Medellin Colombia **52**, 147–160 (2010)
7. Kim, H.S., Lee, H.-K.: Invariant image watermark using Zernike moments. IEEE Trans. Circuits Syst. Video Technol. **13**(8), 766–775 (2003)
8. Chareyron, G., Da Rugna, J., Trémeau, A.: Color in image watermarking. In: Al-Haj, A. (ed.) Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications, IGI Global, pp. 36–56 (2010). 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 J. Image Video Process. **2008**(7), 1–26 (2008)
10. Huang, H., Chu, C., Pan, J.: The optimized copyright protection system with genetic watermarking. Soft Comput. **13**(4), 333–343 (2008)
11. Maity, S.P., Kundu, M.K.: DHT domain digital watermarking with low loss in image informations. Int. J. Electron. Commun. (AEU) **64**(3), 243–257 (2010)
12. Huang, P.S., Chiang, C.: Novel and robust saturation watermarking in wavelet domains for color images. Opt. Eng. **44**(11), 117002 (2005)
13. Battiato, S., Catalano, D., Gallo, G., Gennaro, R.: Robust watermarking for images based on color manipulation. In: Proceedings of the Third International Workshop on Information Hiding. Springer, vol. 1768, pp. 302–317 (2000)
14. Zhang, X., Wang, S.: Fragile watermarking scheme using a hierarchical mechanism. Signal Process. **89**(4), 675–679 (2009)
15. Kougianos, E., Mohanty, P., Mahapatra, R.N.: Hardware assisted watermarking for multimedia. Comput. Electr. Eng. **35**(2), 339–358 (2009)
16. Coltuc, D., Bolon, P.: Robust watermarking by histogram specification. In: Proceedings of 6th IEEE Conference on Image Processing (ICIP' 99). Kobe, Japan, vol. 2, pp. 236–239 (1999)
17. Chareyron, G., Macq, B. and Tremeau, A.: Watermarking of color images based on segmentation of the XYZ color space. In: CGIV Second European Conference on Color in Graphics, Imaging and Vision, Aachen, Germany, pp. 178–182 (2004)
18. Roy, S., Chang, E.C.: Watermarking color histogram. In Proceedings of IEEE Internaional Conference on Image Processing, Singapore, pp. 2191–2194 (2004)
19. Lin, C.H., Chan, D.Y., Su, H., Hsieh, W.S.: Histogram oriented watermarking algorithm: color image watermarking scheme robust against geometric attacks and signal processing. IEE Proc. Vis. Image Signal Proces. **153**(4), 483–492 (2006)
20. Xiaolin, J., Yanli, Q., Liping, S., Xiaobo, J.: An anti-geometric digital watermark algorithm based on histogram grouping and fault-tolerance channel. In: Intelligent Science and Intelligent Data Engineering. Lecture Notes in Computer Science (2012). doi:10.1007/978-3-642-31919-8_96
21. Chrysochos, E., Fotopoulos, V., Skodras, A. Xenos, M.: Reversible image watermarking based on histogram modification. In: Proceedings of 11th Panhellenic Conference on Informatics with International Participation (PCI), B, pp. 93–104 (2007)
22. Chrysochos, E., Fotopoulos, V., Xenos, M., Skodras, A.N.: Hybrid watermarking based on chaos and histogram modification. Signal Image Video Process. (2012). doi:10.1007/s11760-012-0307-3
23. Lukac, R., Plataniotis, K.: Color Image Processing. CRC Press, London (2007)
24. Tapia-Recillas, H.: Remarks on self-inverse quadratic permutation polynomials. Int. J. Algebra **4**(19), 931–938 (2010)
25. Sheikh, H.R., Bovik, A.C.: Image information and visual quality. IEEE Trans. Image Process. **15**(2), 430–444 (2006)
26. Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P.: Image quality assessment: From error measurement to structural similarity. IEEE Trans. Image Process. **13**(4), 600–612 (2004)
27. Chang, H., Chen, H.H.: Stochastic color interpolation for digital cameras. IEEE Trans. Circuits Syst. Video Technol. **17**(8), 964–973 (2007)
28. Plataniotis, K.N., Venetsanopoulos, A.N.: Color Image Processing and Applications. Springer, Berlin (2000)
29. Sahoo, A.: Fuzzy weighted adaptive linear filter for color image restoration using morphological detectors. Int. J. Comput. Sci. Eng. **1**(3), 217–221 (2009)
30. Wang, X., Hou, L., Wu, J.: A feature-based robust digital image watermarking against geometric attacks. Image Vis. Comput. **26**(7), 980–989 (2008)