Benoraira *et al. EURASIP Journal on Advances in Signal Processing* (2015) 2015:55
DOI 10.1186/s13634-015-0239-5

EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

Blind image watermarking technique based on differential embedding in DWT and DCT domains

Ali Benoraira*, Khier Benmahammed and Noureddine Boucenna

Abstract

This paper presents a new blind and robust image watermarking scheme based on discrete wavelet transform (DWT) and discrete cosine transform (DCT). Two DCT-transformed sub-vectors are used to embed the bits of the watermark sequence in a differential manner. The original sub-vectors are obtained by the sub-sampling of the approximation coefficients of the DWT transform of the host image. During the extraction stage, the simple difference between the corresponding sub-vectors of the watermarked image, gives directly the embedded watermark sequence. Experimental results demonstrate that the proposed technique successfully fulfills the requirement of imperceptibility and provides high robustness against a number of image-processing attacks, such as JPEG compression, noise adding, low-pass filtering, sharpening, and bit-plane removal. Our scheme exhibits also an acceptable to good performance against some geometrical attacks such as resizing and cropping.

Keywords: Blind watermarking; Differential embedding; DWT; DCT; Subsampling

1 Introduction

The process of embedding a watermark in a multimedia (image, audio, or video) object is termed as digital watermarking. Content providers want to embed watermarks in their multimedia objects (digital content) for several reasons like copyright protection, content authentication, tamper detection, etc [1–3]. More and more researchers are particularly attracted to the area of image watermarking because of the property of the image as it has a lot of redundant information contained in it which can be exploited to be used for watermark embedding. The embedding process is guided by the use of a secret key which decides the locations within the image where the watermark would be embedded. When the owner wants to check the watermarks in the possibly attacked and distorted digital images, s/he relies on the secret key that was used to embed the watermark. Using the secret key, the embedded watermark sequence can be extracted. In order to be successful, the watermark should be invisible and robust against common image processing operations such as additive noise, compression, cropping, filtering, and resizing [2]. If the watermark is placed in perceptually significant coefficients of the image, the robustness against image distortion is better achieved. These coefficients do not change much after common image processing and compression operations. Also, if these coefficients are destroyed, the reconstructed image is different from the original image and the digital watermark becomes irrelevant. Although, embedding the watermark in perceptually significant coefficients could alter the perceived visual quality of the image. Thus, two essential prerequisites for a powerful watermarking scheme, robustness and invisibility, conflict with each other [4].

Watermarking techniques can be broadly categorized into two distinct categories: non-blind or blind depending on whether the original image is necessary for watermark extraction or not. In real-world practices, non-blind watermarking algorithms are unsuitable for many practical applications in that they require the non-watermarked data to be presented during extraction or detection [2].

Watermarking techniques can be also classified according to the domain in which the watermark is embedded, i.e., the spatial domain or the transform domain. While

*Correspondence: benoraira@gmail.com
Department of Electronics, University of Sétif, 19000 Sétif, Algeria

the spatial domain techniques are having least complexity and high payload, they can not withstand image compression and other common image processing attacks [2, 3]. Transform domain watermarking schemes like those based on the discrete Fourier transform (DFT) [5], the discrete cosine transform (DCT) [6], and the discrete wavelet transform (DWT) [7, 8] typically provide higher image imperceptibility and are much more robust to image manipulations. However, DWT has been used more frequently in digital image watermarking due to its time/frequency decomposition characteristics, which resemble to the theoretical models of the human visual system [8].

Further performance improvements in DWT-based digital image watermarking methods could be obtained by jointing DWT with other transformation domain so that effective watermarking approaches could be developed [9–16].

An algorithm based on joint DWT and DFT transform is proposed in [9]. In the DWT domain, a spread spectrum-based watermark is embedded in the coefficients of the LL sub-band while in DFT domain a template is embedded in the middle frequency component.

Zhao et al. proposed a watermarking approach implemented as a DCT-DWT dual domain algorithm and applied for the protection and compression of cultural heritage imagery [10]. They employed Haar DWT domain to embed the watermark in the components of the image that are of perceptual significance. These components are identified using a block-based (DCT) transform. They specifically demonstrated that watermark embedding in the Haar DWT domain does not interfere with watermark generation in the DCT domain.

In the algorithm proposed in [11], the watermarking was carried out through the embedding of the watermark in the first- and second-level DWT sub-bands of the host image followed by the application of DCT on a selected DWT coefficient sets. It has been shown that the combination of the two transforms improved the watermarking performance considerably when compared to the DWT-only watermarking approach.

In [12], the authors proposed a watermarking scheme based on adaptive quantization index modulation and SVD in a hybrid DWT and DCT domain. The watermark bits are embedded in the singular values' vector of blocks within low frequency sub-band in host image hybrid DWT-DCT domain. To embed the watermark imperceptibly and robustly, they model the adaptive quantization steps by utilizing human visual system (HVS) characteristics and PSO algorithm.

In [13], Feng et al. have proposed a blind DWT-DCT watermarking approach. After scrambling the binary watermark, a block-based DCT transform of the first-level DWT LL sub-band is computed and two PN-sequences of the watermark bits are embedded in the mid frequency coefficients of the corresponding DCT blocks. In the extraction process, the same steps as the embedding process is used to extract the DCT middle frequencies of the LL sub-band. Finally, correlation between mid-band coefficients and PN-sequences is calculated to determine the watermarked bits.

A similar approach is presented in [14], where a multiple sub-bands of the third-level DWT transform of a host image are used to insert the watermark instead of the first-level LL sub-band.

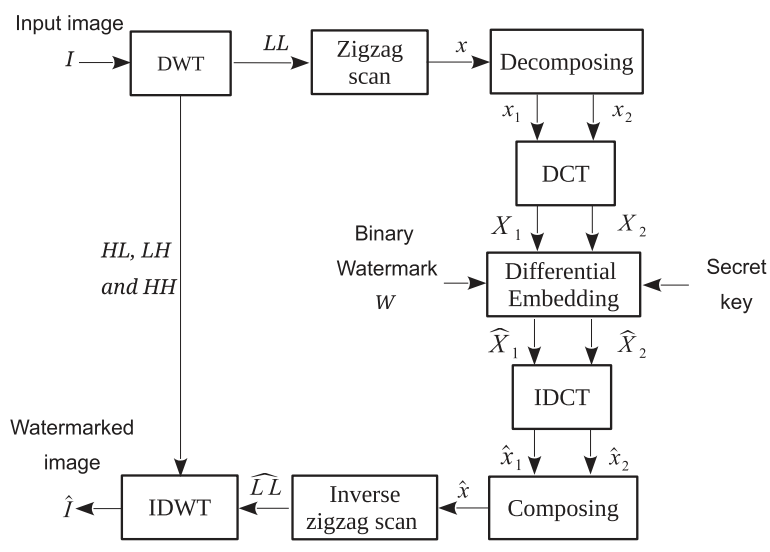

Fig. 1 The embedding procedure of the DWT-DCT method

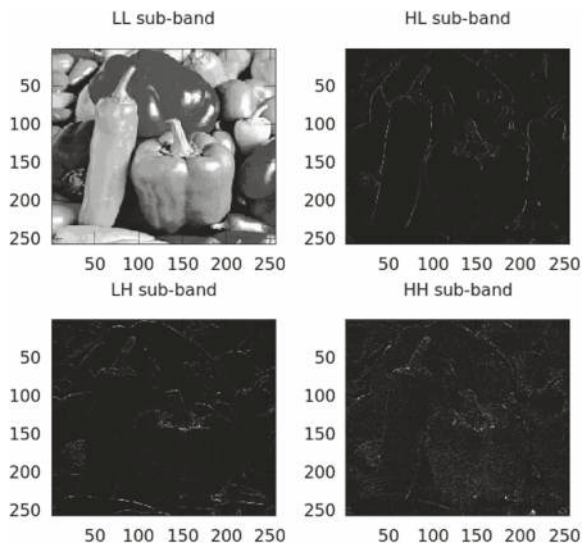

Fig. 2 First-level DWT of the image of peppers

In the method proposed in [16], the wavelet first-level LL sub-band and the watermark image are transformed using DCT and SVD. The S vector of watermark information is embedded in the S component of the host image. Watermarked image is generated by inverse SVD on modified S vector and original U, V vectors followed by inverse DCT and inverse DWT.

Our method is also linked to schemes that use the sub-sampling of the image data [6, 15, 17, 18]. The sub-sampling techniques offer more room for watermarking by, for example, dividing the original image into sub-images and applying different modifications to transformed coefficients belonging to different sub-images [6, 17].

In this paper, a binary watermark sequence is embedded in the host image using DWT and DCT domains and the technique of differential embedding. The DCT is applied on two sub-vectors obtained by the sub-sampling of the DWT *LL* sub-band of the image. The differential embedding of the watermark in the resulting two DCT-transformed sub-vectors ensures the blind extraction of it.

To further emphasize the efficiency of combining DWT and DCT domains, we propose also a reduced DCT-based version of our method which is based on the DCT domain only. The results of comparison between the combined DWT-DCT and the DCT-only methods justify the combining of DWT and DCT domains.

The rest of the paper is structured as follows. In Section 2, we present the new DWT-DCT blind watermarking scheme. The reduced DCT-only method is outlined in Section 3. Numerical experimental results and comparisons with other methods are given in Section 4. Finally, we draw conclusion and suggest future work in Section 5.

2 Proposed method

2.1 The embedding process

The proposed watermark embedding scheme is shown in Fig. 1.

Let I denote the gray-scale square image of size $M \times M$ to be watermarked by the bipolar $\{-1, 1\}$ binary sequence W of size L, the embedding process can be described as follows:

- **Step 1**: Perform the first-level DWT of the input image I. This produces the approximation coefficients matrix (LL sub-band) and a set of detail coefficients (HL, LH, and HH sub-bands).
- **Step 2**: Perform zigzag scanning [19] to convert the matrix LL into a vector of approximation coefficients $x(n)$, $n = 1, \ldots, N$, where $N = M.M/4$. Since adjacent pixels are highly correlated in real images and the first-level LL sub-band represents a close approximation of the original image (Fig. 2); the zigzag scanning of the LL matrix helps to cluster high correlated approximation coefficients in the vector $x(n)$.

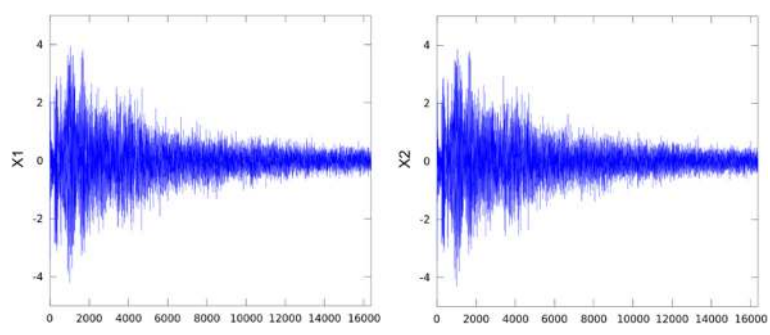

Fig. 3 The first half of DCT-transformed sub-vectors X_1 and X_2 (without the DC component) for the image of peppers

- **Step 3**: Decompose the vector of approximation coefficients x into two (correlated) sub-vectors x_1 and x_2 using the following sub-sampling operations:

$$x_1(k) = x(2k) \tag{1}$$
$$x_2(k) = x(2k-1) \tag{2}$$

where $k = 1, \ldots, N/2$.

- **Step 4**: Perform DCT on x_1 and x_2 to produce their DCT-transformed versions X_1 and X_2 (Fig. 3):

$$X_1 = dct(x_1) \tag{3}$$
$$X_2 = dct(x_2) \tag{4}$$

- **Step 5**: Insert the watermark sequence bits $W(i)$ for $i = 0, 2, \ldots, L-1$, in the transformed sub-vectors X_1 and X_2 using a differential embedding technique. This will produce two transformed and modified (by watermarking) sub-vectors $\hat{X}_1$ and $\hat{X}_2$ as follows:

$$\hat{X}_1(i') = \frac{1}{2}\left[X_1\left(i'\right) + X_2\left(i'\right)\right] + \alpha W\left(i\right) \tag{5}$$

$$\hat{X}_2(i') = \frac{1}{2}\left[X_1\left(i'\right) + X_2\left(i'\right)\right] - \alpha W\left(i\right) \tag{6}$$

where α is the gain factor and i' are the random locations within the high energy band of X_1 and X_2 in which the watermark bits are embedded (Fig. 4). These locations are the elements of a vector r which can be generated using a random permutation function:

$$i' = r(i) \tag{7}$$
$$r = \mathrm{RandPerm}(S, a, b) \tag{8}$$

where S is the seed of the associated pseudo random number generator (PNRG), a and b are, respectively, the starting and the ending locations of the high energy band used to insert the watermark (Fig. 4).

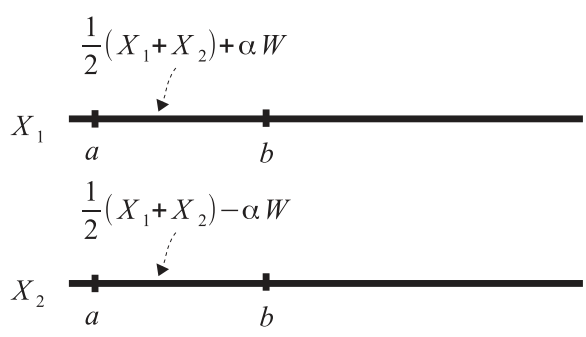

Fig. 4 The differential embedding of the watermark in the high energy band of the transformed sub-vectors X_1 and X_2

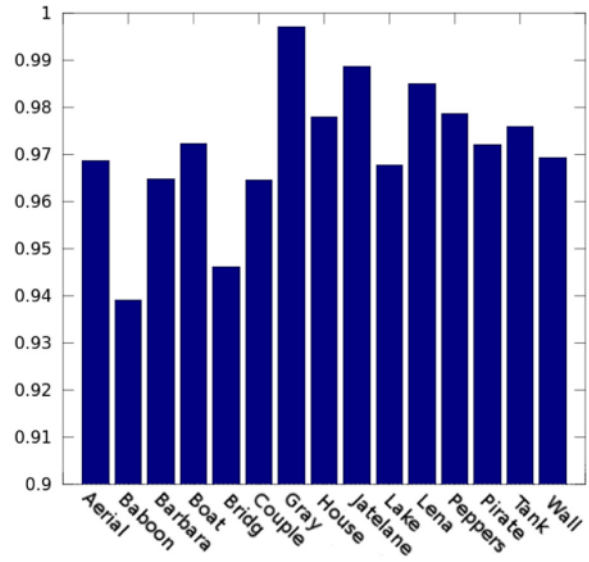

Fig. 5 Correlation between X_1 and X_2 for 15 test images

Therefore, the user's secret key is $key = (S, a, b)$, which prevent the watermark from tempering or unauthorized access by attackers.

- **Step 6**: Perform the inverse DCT on $\hat{X}_1$ and $\hat{X}_2$:

$$\hat{x}_1 = idct(\hat{X}_1) \tag{9}$$
$$\hat{x}_2 = idct(\hat{X}_2) \tag{10}$$

- **Step 7**: Combine the two modified sub-vectors $\hat{x}_1$ and $\hat{x}_2$ using the opposite operation in (1) and (2) in order to produce the modified vector of approximation coefficients $\hat{x}$:

$$\hat{x}(2k) = \hat{x}_1(k) \tag{11}$$
$$\hat{x}(2k-1) = \hat{x}_2(k) \tag{12}$$

for $k = 1, \ldots, N/2$.

- **Step 8**: Convert the modified vector $\hat{x}$ into the matrix of a modified approximation coefficients $\widehat{LL}$ using

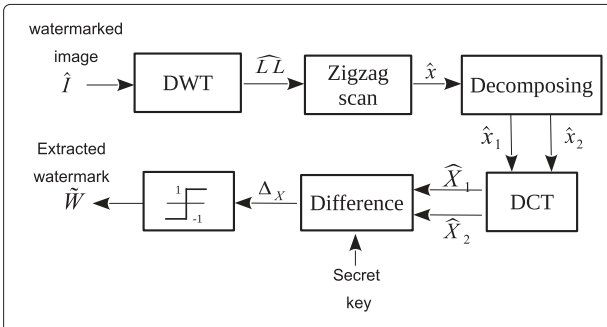

Fig. 6 The extraction procedure of the DWT-DCT method

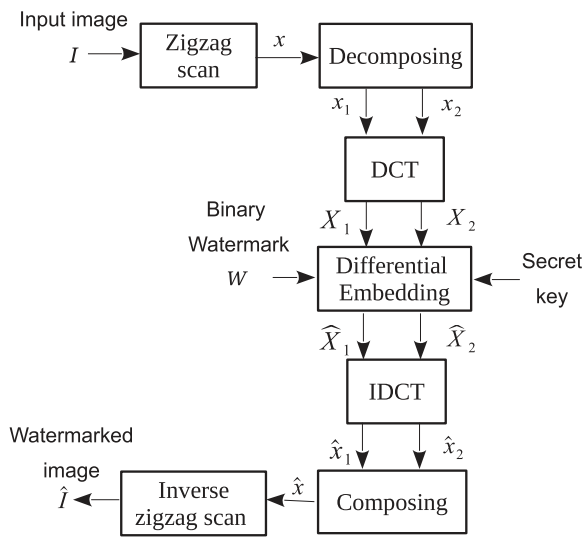

Fig. 7 The embedding procedure of the DCT-only method

the inverse of the zigzag scan operation used in step 2.

- **Step 9**: Construct the watermarked image $\hat{I}$ by performing the inverse wavelet transform of the modified approximation coefficients $\widehat{LL}$ and the sets of original detail coefficients (HL, LH, and HH sub-bands).

Note 1: The parameters a and b should be chosen to satisfy the following conditions:

- $a > 0$: the DC-components of the transformed sub-vectors X_1 and X_2 must remain unchanged in order to preserve the quality of the watermarked image;
- $b - a \geq L$: the insertion band have to be wide enough to insert all the watermark's bits;
- $b \leq \frac{N}{2}$: the watermarking is done in the hight energy band of X_1 and X_2 in order to guarantee the robustness of the method.

Note 2: While the normal differential embedding would be as follows: $\hat{X}_1 = X_1 + \alpha W$ and $\hat{X}_2 = X_2 - \alpha W$ (by omitting the insertion locations), the fact that the transformed sub-vectors X_1 and X_2 are highly correlated (as shown in Fig. 5) allow as to assume in Eqs. 5 and 6, that $X_1 \approx X_2 \approx \frac{1}{2}[X_1 + X_2]$. This will ensure that X_1 and X_2 are equally contributing in the new modified ones $\hat{X}_1$ and $\hat{X}_2$ so that the resulting distortion on the watermarked image will be minimal. Also, it is obvious that the difference between $\hat{X}_1$ and $\hat{X}_2$ will give an amplified (by 2) amount of the inserted watermark sequence (αW) which is the key feature of this differential embedding technique.

2.2 The extraction process

The watermark extraction process follows the same steps as the embedding process until step 5 where the extraction is taking place as shown in Fig. 6.

If the input image is the watermarked one, and by analogy with the embedding process, step 4 of the extraction process will give the two sub-vectors $\hat{X}_1$ and $\hat{X}_2$ in Eqs. 5 and 6, respectively. Consequently, the difference between them has a proportional relationship with the watermark sequence W:

$$\triangle_X(i) = \hat{X}_1(i') - \hat{X}_2(i') = 2\alpha W(i) \tag{13}$$

with $i = 1, \ldots, L$, and i' are the random locations where the watermark bits are embedded. These locations are determined simply by recreating the vector r (Eq. 7) using the user-selected secret key and the random permutation function (Eq. 8). Finally, and since the difference $\triangle_X(i)$

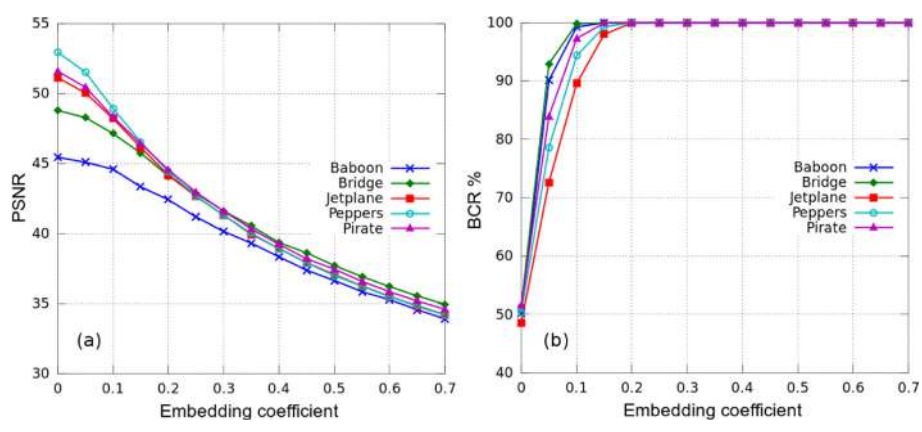

Fig. 8 PSNR of watermarked images versus the gain factor α (**a**). BCR of the extracted watermark versus the gain factor α after JPEG lossy compression ($Q = 40$) (**b**)

Fig. 9 The original images of baboon, bridge, jetplane, peppers, and pirate (*top*), and the their watermarked versions (*bottom*) with PSNR values of 42.64, 43.85, 44.73, 44.80, and 44.45, respectively

might differ from $+1/-1$ values, we apply a hard limitation function on it in order to recover the original bits of the watermark:

$$\tilde{W}(i) = \begin{cases} 1 & \text{if} \quad \triangle_X(i) \geq 0 \\ -1 & \text{otherwise} \end{cases} \tag{14}$$

If the watermarked image has been attacked, the proposed method is able to extract the watermark and the quality of extraction closely depends on the severity of the attack as shown in the experiments.

Notice that no threshold setting is needed at the extraction stage, which represents a great advantage compared with a lot of schemes in literature [9, 10]. Also, this watermarking approach is analogous to the technique of *Differential Signaling*, a method of transmitting information electrically by means of two complementary signals [20]. At the end of the connection, the receiver reads the difference between the two signals to recover the original information.

3 The DCT-only method

To justify the utility of combining DWT and DCT domains, we propose here a reduced version of our method based only on the DCT domain. Since we applied the zigzag scanning on the matrix of approximation coefficients of DWT (Section 2.1) to obtain the vector x, we choose here to apply it on the whole image (without using DWT). The flowchart of the embedding process of the DCT-only method is given in Fig. 7.

In this process, the operations are the same as described in the embedding process of the DWT-DCT method (Section 2.1). Notice that all the vectors in Fig. 7 are four times the size of the corresponding vectors in the DWT-DCT method. The extraction process will be the same as in Fig. 6 except that the DWT step is not needed in this case.

4 Experiment results

In this section, several experiments are conducted to evaluate the performance of the proposed watermarking scheme. The size of original cover images (baboon, bridge, jetplane, peppers, and pirate) is 512×512 pixels[1]. The watermark is a pseudo-random binary sequence of size 256 bits, which is a usual payload [21]. To evaluate the quality of the watermarked image, the peak signal to noise ratio (PSNR) is used [10]. To evaluate the quality of extracted watermark, the bit-correct ratio (BCR) is

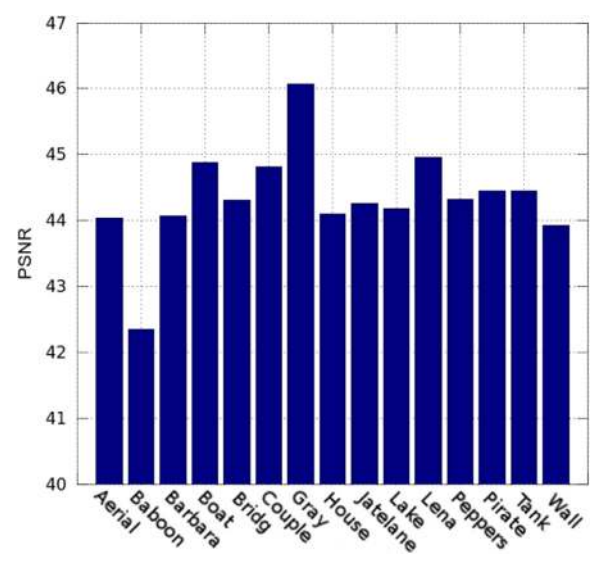

Fig. 10 PSNR of 15 watermarked images

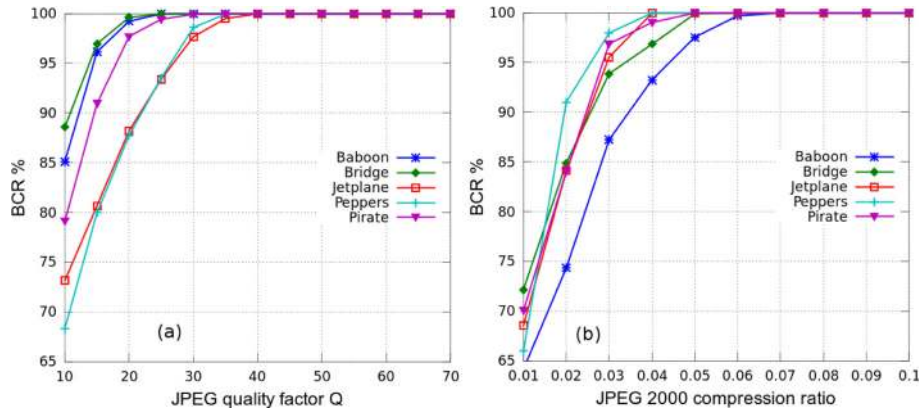

Fig. 11 Robustness against compression attacks. **a** JPEG lossy. **b** JPEG2000

adopted to measure the similarity between the original watermark W and the extracted watermark $\tilde{W}$. The use of this measure has become common recently [22], as it allows for a more detailed scale of values and is defined as the ratio of correct extracted bits to the total number of embedded bits [22]:

$$\mathrm{BCR} = \frac{1}{L}\sum_{k=0}^{L-1}\overline{W(k) \oplus \tilde{W(k)}} \times 100\,\% \tag{15}$$

where $\oplus$ is the XOR operator. If the watermark is extracted without error the BCR value will be 100 %.

4.1 Gain factor selection

In order to select the suitable values of the gain factor α in Eqs. 5 and 6 that fulfill both the invisibility and the robustness requirements of the watermarking, we plot with respect to α the PSNR of the watermarked images (Fig. 8a) and the BCR of the extracted watermarks (Fig. 8b) after a standard image attack (JPEG lossy with quality factor equals to 40).

It is apparent from Fig. 8 that higher α values make lower PSNR of the watermarked images, but the similarity (BCR %) of original watermark and the extracted watermark gets better for higher values of α. The best trade-off between visual quality and watermark robustness is achieved for the values of α in range from 0.2 to 0.3 where the PSNR values are greater than 40 dB and the BCR values are almost 100 % for all test images. In the rest of our experiments, we will set $\alpha = 0.2$ as the default gain factor value.

Figure 9 shows the perceptual difference between the original test images and their watermarked versions and the corresponding PSNR measures.

From Fig. 10, we can see that PSNR of 15 watermarked images is greater than 42 dB which ensures the invisibility requirement. Notice that the watermark is extracted from all test images with no error (BCR = 100 %).

4.2 Robustness tests

4.2.1 Robustness against image compression

The BCR values of the extracted watermarks under JPEG lossy and JPEG2000 compression attacks are shown in Fig. 11. For JPEG lossy compression, the quality factor (Q) is varied from 10 to 70, whereas for JPEG2000 attacks, the compression ratio r [23] is varied from 0.01 to 0.1.

We can see from Fig. 11a that the watermark is completely recovered under high strength JPEG lossy attacks (BCR = 100 for $Q \geq 40$) for all test images.

Fig. 12 Attacked images with LSB removal (6 bits), JPEG lossy ($Q = 20$), Gaussian filter (5×5), salt and pepper noise (var = 0.02), and gamma correction (gamma = 3), respectively. The BCR value is greater than 99 % for all these attacks

Table 1 BCR values of the proposed DWT-DCT technique under noise addition attacks

Attack	Image				
	Baboon	Bridge	Jetplane	Peppers	Pirate
Gaussian noise (var = 0.005)	98.8	99.1	98.5	98.9	98.3
Gaussian noise (var = 0.01)	93.5	93.4	93.7	93.6	94.1
Salt and pepper noise (var = 0.01)	99.9	99.7	99.7	99.4	99.8
Salt and pepper noise (var = 0.02)	98.1	97.7	97.2	97.1	97.5
Speckle noise (var = 0.01)	99.9	100	98.4	100	100
Speckle noise (var = 0.02)	98.2	98.4	93.5	98.8	99.2

Table 3 BCR values of the proposed DWT-DCT technique under other image-processing attacks

Attack	Image				
	Baboon	Bridge	Jetplane	Peppers	Pirate
Bit-plane removal (5 bits)	100	99.7	99.2	100	100
Bit-plane removal (6 bits)	98.0	92.4	96.7	98.4	96.5
Gamma correction (0.5)	100	100	100	100	100
Gamma correction (1.5)	100	100	100	100	100
Histogram equalization	100	100	99.5	100	100
Laplacian sharpening	100	100	100	100	100

The proposed method is also robust for the practical JPEG2000 compression range of levels, i.e., $r \geq 0.04$ (Fig. 12b) except for the textured images of Baboon and Bridge where it exhibits a lower robustness. This because, JPEG2000 compression does not necessarily provide an image of good quality in texture features [24].

4.2.2 Robustness against image processing attacks

In the following, we evaluate the proposed method against noise addition, low pass filtering, image enhancement, etc. Table 1 shows the BCR values of the extracted watermarks under noise addition attacks. For the three types of noises (Gaussian, salt and pepper, and speckle), we can observe that the proposed method is fairly robust against noises with medium variances, whereas for high variance noises the method presents acceptable performance since the BCR values is greater than 93 % for the majority of experiments.

Tables 2 and 3 demonstrate that the proposed method is robust against low-pass filtering, bit-plane removal, gamma correction, histogram equalization, and Laplacian sharpening attacks. Notice that in bit-plane removal attack, the least significant bits of the watermarked image are replaced with zeros. All these experiments show that the proposed method is robust against common image-processing attacks.

Figure 12 shows the visual impact of some attacks on different images. The watermark is extracted with BCR value greater than 99 % which confirms the preceding results.

4.2.3 Robustness against geometrical attacks

The next experiments show the robustness against some geometrical attacks on the test images.

Table 4 and Fig. 13 demonstrate that the proposed method is relatively robust against geometrical attacks. In particular, it performs well for cropping and resizing attacks but exhibits weak robustness against rotation attacks.

Table 2 BCR values of the proposed DWT-DCT technique under low-pass filtering attacks

Attack	Image				
	Baboon	Bridge	Jetplane	Peppers	Pirate
Average filter (3×3)	99.7	100	100	100	100
Gaussian filter (5×5) var = 1.5	90.4	91.2	93.3	88.8	92.5
Gaussian filter (5×5) var = 1	99.8	99.9	99.9	99.6	100
Median filter (3×3)	97.9	99.6	99.9	99.8	100
Wiener filter (3×3)	99.6	99.9	99.9	99.9	99.9

Table 4 BCR values of the proposed DWT-DCT technique under geometrical attacks

Attack	Image				
	Baboon	Bridge	Jetplane	Peppers	Pirate
Resizing (512 → 256 → 512)	98.6	99.7	100	100	100
Resizing (512 → 200 → 512)	77.1	84.4	96.4	97.3	93.8
Rotation (0.25°)	78.3	87.6	97.7	99.3	97.3
Rotation (0.5°)	54.3	56.1	56.4	56.1	57.4
Surrounding crop (15 %)	97.4	99.6	97.6	99.5	99.8
Surrounding crop (25 %)	94.2	97.3	97.2	99.2	99.2

Fig. 13 Robustness of the DWT-DCT technique against different types of cropping. The BCR values is 100 % for these attacks

4.2.4 Robustness against watermark suppression attack

In these experiments, we suppose that the an informed attacker have partial knowledge of the embedding process and he tries to perform a successful attack that produces a smaller amount of perceptible distortion compared to its blind counterparts. In particular, we suppose that the attacker tries to obliterate the inserted watermark by erasing a portion of the two carrying sub-vectors $\hat{X}_1$ and $\hat{X}_2$ (Eqs. 5 and 6). So the attacker puts the vectors $X_1(n) = 0$ and $X_2(n)$ to 0 for $n = 1, 2, \ldots, K$. ($n \neq 0$ in order to keep the DC value intact). The results of attacked images of peppers and the corresponding BCR values for different value of k are given in Fig. 14. We can see that the watermark (or a portion of it) can be successfully extracted for this type of attacks. However, once the suppression of the watermark exceeds a certain level ($K > 512$), the image becomes no longer usable because of the high perceptible distortions.

4.3 Comparison with other methods

In this subsection, we conduct several experiments to compare the performance of the proposed DWT-DCT method with two other blind watermarking approaches ([13] and [25]) and also with the reduced DCT-only method.

The approach in [25] proposed a block-based significant difference quantization watermarking. Every seven wavelet coefficients in one sub-band are grouped into a block and the watermark bit is embedded into a block by quantizing the difference between two maximum wavelet coefficients. Notice that the embedding parameters in each method are adjusted to produce a watermarked image (Lena) of PSNR equal to 44 dB. The results of comparison are listed in Tables 5, 6, and 7.

From the results in Tables 5, 6, and 7, we notice the following:

- The proposed DWT-DCT method outperforms the reduced DCT-only method for JPEG compression, low-pass filtering, resizing, and rotation attacks. For the rest of attacks, both techniques perform equally well. Consequently, the combination of the two transforms (DWT and DCT) is more practically helpful than the use of one domain only (DCT) especially if the watermarked images are intended to undergo these types of attacks.
- For JPEG compression, only the method in [25] performs slightly better than the proposed DWT-DCT method. This is because the fact that wavelet quantization techniques are generally robust against image compression attacks [25].
- For the rest of attacks, the proposed DWT-DCT method is more robust than the two methods in [13] and [25] especially for bit-plane removal, gamma correction, noise addition, and for all geometrical attacks.

Fig. 14 Robustness against watermark suppression attack for the image of peppers. From *left* to *right*: the values of K are 128, 256, 512, and 1024 and the corresponding values of BCR are 100, 99.6, 98.8, and 91.8, respectively

Table 5 Comparison of robustness (BCR) against image compression attacks between Feng et al. [13], Lin et al. [25], the DCT-only, and the DWT-DCT methods

Attack	Method			
	Feng et al. [13]	Lin et al. [25]	DCT-only	DWT-DCT
JPEG 2000 ($R = 0.02$)	79.8	97.2	86.8	90.2
JPEG 2000 ($R = 0.03$)	92.2	98.8	100	99.6
JPEG 2000 ($R = 0.04$)	98.4	100	100	100
JPEG lossy ($Q = 40$)	89.2	100	74.9	100
JPEG lossy ($Q = 30$)	78.4	98.4	68.7	99.4
JPEG lossy ($Q = 20$)	69.8	94.5	61.4	88.8

From the previous results, we may conclude that, overall, the proposed method has a better performance than the compared watermarking schemes ([13, 25]) and that the combination of the DWT and DCT domains is more advantageous than the use of only one frequency domain.

5 Conclusions

In this paper, a robust, yet simple watermarking scheme based on the combination of DWT and DCT domains is presented. In the embedding process, a differential technique is performed on two transformed sub-vectors so that the extraction of the watermark is achieved using only the difference of the corresponding watermarked sub-vectors.

Table 6 Comparison of robustness (BCR) against image processing attacks between Feng et al. [13], Lin et al. [25], the DCT-only, and the DWT-DCT methods

Attack	Method			
	Feng et al. [13]	Lin et al. [25]	DCT-only	DWT-DCT
Bit-plane removal (5 bits)	96.3	85.9	100	100
Gamma correction (3)	99.2	76.1	100	100
Gaussian noise (0.01)	87.5	79.5	96.3	94.9
Histogram equalization	99.3	94.5	100	100
Laplacian sharpening	100	91.4	100	100
Median filter (3×3)	97.1	99.2	41.6	100
Gaussian filter (5×5)	98.8	94.5	83.4	100
Salt and pepper noise (0.02)	93.3	85.9	99.1	98.3

Table 7 Comparison of robustness (BCR) against geometrical attacks between Feng et al. [13], Lin et al. [25], the DCT-only, and the DWT-DCT methods

Attack	Method			
	Feng et al. [13]	Lin et al. [25]	DCT-only	DWT-DCT
Resizing (512 → 200 → 512)	98.9	94.1	65.6	100
Rotation (0.25°)	90.6	88.2	65.5	99.4
Top left quarter crop	88.3	85.1	100	99.1
Surrounding crop (25 %)	82.2	82.0	99.7	99.2

Overall, the experimental results demonstrate that our scheme provides excellent robustness against multiple image attacks such as bit-plan removal, cropping, JPEG compression, histogram equalization, low-pass filtering, and noise adding attacks. Besides, the quality of the watermarked image is satisfactory in terms of imperceptibility as the PSNR per watermarked image is over 42 dB.

We have also investigated the utility of the combination of the DWT and DCT transforms through the proposition of a relaxed version of our method based only on the DCT transform. In comparison, the DWT-DCT method is more robust than the DCT-only method for a set of attacks such as JPEG compression and low-pass filtering. The results of experiments have showed also that the proposed (DWT-DCT) method has stronger robustness in comparison with two existing watermarking schemes.

As a future work, we plan to extend the proposed approach to video watermarking domain. As the embedding and the extracting processes are of low complexity and do not require any specific features of the input image, the extension to video watermarking will be straightforward. Along with that, an automatic technique for the selection of the gain factor value needs to be developed to have better control on both imperceptibility and robustness of the scheme.

Endnote

[1] All test images are obtained from the USC-SIPI Image Database: http://sipi.usc.edu/database/.

Competing interests

The authors declare that they have no competing interests.

Received: 9 December 2014 Accepted: 8 June 2015
Published online: 03 July 2015

References

1. VM Potdar, S Han, E Chang, in *International Conference on Industrial Informatics*. A Survey of Digital Image Watermarking Techniques, (2005), pp. 709–716. doi:10.1109/INDIN.2005.1560462
2. I Cox, M Miller, J Bloom, J Fridrich, T Kalker, *Digital Watermarking and Steganography*, 2nd edn. (Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008)
3. M Abdullatif, AM Zeki, J Chebil, TS Gunawan, in *International Colloquium on Signal Processing and Its Applications*. Properties of Digital Image Watermarking (IEEE KL, Malaysia, 2013), pp. 235–240. doi:10.1109/CSPA.2013.6530048
4. P Moulin, JA O'Sullivan, Information-theoretic analysis of information hiding. IEEE T. Inform. Theory. **49**, 563–593 (2003). doi:10.1109/TIT.2002.808134
5. CM Pun, in *International Conference on Signal Processing*. A Novel DFT-based Digital Watermarking System for Images, vol. 2, (2006), pp. 16–20. doi:10.1109/ICOSP.2006.345581
6. WC Chu, DCT-based image watermarking using subsampling. IEEE T. Multimedia. **5**, 34–38 (2003). doi:10.1109/TMM.2003.808816
7. CV Serdean, MK Ibrahim, A Moemeni, MM Al-Akaidi, Wavelet and multiwavelet watermarking. IET Image Process. **48**, 223–230 (2007). doi:10.1049/iet-ipr:20060214
8. MR Keyvanpour, FM Bayat, Robust dynamic block-based image watermarking in DWT domain. Procedia CS. **3**, 238–242 (2011). doi:10.1016/j.procs.2010.12.040
9. X Kang, J Huang, YQ Shi, Y Lin, A DWT-DFT composite watermarking scheme robust to both affine transform and jpeg compression. IEEE T. Circ. Syst. Vid. **13**, 776–786 (2003). doi:10.1109/TCSVT.2003.815957
10. Y Zhao, P Campisi, D Kundur, Dual domain watermarking for authentication and compression of cultural heritage images. IEEE T. Image Process. **13**, 430–448 (2004). doi:10.1109/TIP.2003.821552
11. A Al-Haj, Combined DWT-DCT digital image watermarking. J. Comput. Sci. **3**, 740–746 (2007). doi:10.3844/jcssp.2007.740.746
12. S Zhu, J Liu, in *Lect. Notes Comput. Sc*. A Novel Adaptive Watermarking Scheme Based on Human Visual System and Particle Swarm Optimization, vol. 5451, (2009), pp. 136–146. doi:10.1007/978-3-642-00843-6_13
13. LP Feng, LB Zheng, P Cao, in *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*. A DWT-DCT Based Blind Watermarking Algorithm for Copyright Protection, vol. 7, (2010), pp. 455–458. doi:10.1109/ICCSIT.2010.5565101
14. RH Laskar, M Choudhury, K Chakraborty, S Chakraborty, in *Computer Networks and Intelligent Computing. Communications in Computer and Information Science*. A Joint DWT-DCT Based Robust Digital Watermarking Algorithm for Ownership Verification of Digital Images, vol. 157 (Springer Berlin, Germany, 2011), pp. 482–491. doi:10.1007/978-3-642-22786-8_61
15. MJ Tsai, HY Hung, in *24th International Conference on Distributed Computing Systems Workshops*. DCT and DWT Based Image Watermarking Using Sub Sampling (China, 2004), pp. 184–189. doi:10.1109/ICDCSW.2004.1284029
16. AK Singh, M Dave, A Mohan, Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT–DCT–SVD Domain. Natl. Acad. Sci. Lett. **37**, 351–358 (2014). doi:0.1007/s40009-014-0241-8
17. PW Lin, YH Chen, CC Chang, JS Lee, Contrast-adaptive removable visible watermarking (CARVW) mechanism. Image and Vision Computing. **31**, 311–321 (2013). doi:10.1016/j.imavis.2013.02.002
18. W Lu, W Sun, H Lu, Novel robust image watermarking based on subsampling and DWT. Multimedia Tools and Applications. **60**, 31–46 (2012). doi:10.1007/s11042-011-0794-1
19. G Bhatnaga, QM Jonathan Wu, A new robust and efficient multiple watermarking scheme. Multimed. Tools Appl. (2013). doi:10.1007/s11042-013-1681-8
20. H Johnson, M Graham, *High Speed Signal Propagation: Advanced Black Magic*. (Prentice Hall, 2003)
21. F Yaghmaee, M Jamzad, Estimating watermarking capacity in gray scale images based on image complexity. EURASIP J. Adv. Signal Process. (2010). doi:10.1155/2010/851920
22. HC Huang, SC Chu, JS Pan, CY Huang, BY Liao, Tabu search based multi-watermarks embedding algorithm with multiple description coding. Inf. Sci. **181**, 3379–3396 (2011). doi:10.1016/j.ins.2011.04.007
23. G Qadir, Z Xi, ATS Ho, in *Optics, Photonics, and Digital Technologies for Multimedia Applications. SPIE Proceedings*. Estimating jpeg2000 compression for image forensics using Benford's law, vol. 7723 (Brussels, Belgium, 2010). doi:10.1117/12.855085
24. K Roimela, T Aarnio, J Itäranta, in *Proceedings of the 2008 Symposium on Interactive 3D Graphics and Games. I3D '08*. Efficient high dynamic range texture compression (ACM New York, NY, USA, 2008), pp. 207–214. doi:10.1145/1342250.1342282. http://doi.acm.org/10.1145/1342250.1342282
25. WH Lin, SJ Horng, TW Kao, P Fan, CL Lee, Y Pan, An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE Trans. on Multim. **10**, 746–757 (2008). doi:10.1109/ TMM.2008.922795