

Research Article

A Robust Watermarking Scheme Based on the Mean Modulation of DWT Coefficients

Zied Kricha ^{1,2}, Anis Kricha,^{3,4} and Anis Sakly⁵

¹National School of Engineers of Sousse, University of Sousse, Erriadh City, 4023, Tunisia

²CSR Group with the Electronic and Microelectronic Lab, National School of Engineers of Monastir, University of Monastir, Ibn El Jazzar Avenue, 5035, Tunisia

³LATIS Lab, National School of Engineers of Sousse, University of Sousse, Erriadh City, 4023, Tunisia

⁴National School of Engineers of Monastir, University of Monastir, Ibn El Jazzar Avenue, 5035, Tunisia

⁵ESIR Research Unit, National School of Engineers of Monastir, University of Monastir, Ibn El Jazzar Avenue, 5035, Tunisia

Correspondence should be addressed to Zied Kricha; kricha.zied@gmail.com

Received 4 May 2018; Revised 29 October 2018; Accepted 21 November 2018; Published 6 December 2018

Academic Editor: Emanuele Maiorana

Copyright © 2018 Zied Kricha et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In an endeavor to deal with image copyright infringement, robust watermarking approaches are commonly used. However, most of the existing approaches either present a limited robustness or rely on highly computational algorithms, thereby limiting the efficiency of these solutions. In this paper, a novel blind and robust watermarking method is presented. First, the vertical and horizontal subbands coefficients, resulting from the wavelet transformation, are scrambled using a chaotic sequence and then gathered into individual blocks. Next, the mean value of each block is modulated according to watermark bit. At the extraction stage, based on the sign of the blocks' mean, a blind watermark extractor is suggested. The imperceptibility, security, complexity, and robustness of the proposed approach have been evaluated and compared with state of the art solutions. Experimental results prove that the proposed approach successfully satisfies the watermarking requirement and outperforms existing methods against both geometric and signal processing attacks.

1. Introduction

We all remember directing a banknote toward a source of light to verify its authenticity. The presence of a predefined pattern, number, or portrait, technically called watermark, determines whether the banknote is fake or not. Watermarking is an old technique used to prevent counterfeiting of several official paper documents. Nowadays, physical form of paper is not the only valuable thing worth securing, whereas images, audio tracks, and video sequences present a new form of money, that is vulnerable to unauthorized distribution and modification. In an effort to address these issues, watermarking concept was again adopted, but this time with the prefix “digital” for referring to digital objects. Digital watermarking is the act of incorporating supplemental information into multimedia material (still images, audio, or video) in such a manner that it does not alter the delivered material and yet still readily exploited by the watermark detector, even after

some undesirable operations. An overview of the literature reveals a broad range of application domains including encryption [1], copyright protection [2], integrity verification [3], content restoration [4], and documentation [5].

The main focus of this paper is to design a robust watermarking scheme for image copyright protection. The first watermarking schemes in this regard targeted the least significant bit (LSB) of pixels' brightness [6]. Despite their simplicity of realization, LSB based schemes suffer from a high sensitivity to noise, which prompted researchers to look for new alternatives. In fact, researchers have targeted different parts of the watermarking process; the generation of carrier elements from the raw representation (e.g., pixels values) [7, 8], the choice of an embedding method, summarized by the embedding equation that describes how the watermarked elements are generated from the original coefficients [9, 10], and finally the choice of a suitable watermark detector [11].

The two main used techniques for watermark embedding are the spread spectrum (SS) [12] and the quantization (QIM) [10] based techniques. These techniques have been subject to much amelioration such as the spread transform dither modulation [13] and the progressive quantization [14] for QIM-based-techniques; and the improved SS [9], the multiplicative SS (MSS) [15], and the improved MSS for SS-based-techniques [16].

The digital watermark may be inserted either in the raw representation of the image, where each watermark bit is inserted straight into pixel's brightness, or after a preprocessing phase involving the generation of a new domain or/and the selection of an appropriate component on which the embedding algorithm will be applied.

The straightforward option, though it is not the robusiter, is to insert the watermark in the spatial domain. A preliminary work in this trend is presented in [17], where the watermark is repeatedly inserted in a subtractive or additive way depending on the pixels' characteristics. To consolidate the robustness of the DC coefficients with the rapidity of direct pixels manipulation, Su et al. [18] proposed to compute the DC without going through the DCT transformation. Although this method is computationally lighter than the conventional insertion in transform domain, it provides fewer choices, and it is limited, so far, to the DC coefficients.

In contrast to the spatial domain, transform ones offer more flexibility. For instance, in the DCT domain, the watermark has been embedded into different positions, such as the DC [19] or the AC frequency [20]. Similarly, in the Discrete Wavelet Transform (DWT), researchers opted for different subbands and different wavelet families. In [21], the watermark is embedded into the HL_3 subband of the *Haar* wavelet decomposition and into the LL_5 subband of the integer DWT in [22]. Other employed transformations include the gyrator domain [1], the contourlet [23], and the Hessenberg [24] transforms.

When most of schemes have been designed to embed the watermark into the amplitude of coefficients, either in the spatial or frequency domain, some academics have chosen to create or form a new carrier using various representations of these coefficients. Inspired by the works realized in communication theory, specifically the modulation of the phase instead of the amplitude, Ourique et al. [25] proposed to watermark the angle constituted by the host vector with respect to a hyperspherical coordinate system.

Recently, many researchers have tended to embed the watermark into a robust feature obtained from a set of coefficients, such as the coefficient difference computed between the two largest wavelet coefficients belonging to the same group [7], or the difference between adjacent coefficients of the same DWT subbands [8]. In [26, 27], the watermark is embedded into the image's significant elements. In [27], the nonsampled Shearlet transform of images significant region is calculated, and then the watermark is embedded in the high-pass subband with the highest energy. The human visual system can barely notice the modifications of high edge concentration zones. To benefit from this weakness, the authors of [26] proposed to adjust the watermark strength according to the blocks complexity. The embedding stage

consists in the modification of two DCT coefficients from each block. At the extraction phase, the difference between these coefficients specifies the value of the watermark bit. In [28], Lili et al. took advantage of the LL subband's robustness to provide blindness to the additive SS algorithm, where the HH subband is replaced by the quantized and watermarked LL subband.

The bottom line of the literature review reveals that the watermarking problem persists and the dilemma remains unsolved. Most of the existing schemes either manifest a weak robustness or make recourse to overcomputational schemes through a cascade of transformations [14, 29, 30], metaheuristic algorithms [31], or both [32, 33].

The main objective of this paper is to investigate and implement an efficient watermarking scheme for grayscale images. This objective is achieved by using a single transformation (DWT) to localize the appropriate frequencies, a block mean as a representation of the watermark carrier, a chaotic encryption for security, and a mean modulation for embedding.

To the best of our knowledge, the closest work to ours is perhaps that of [34], in which the authors embedded the watermark in the mean value of DWT coefficients. However the difference between the two approaches is threefold. Firstly, the two papers are dealing with different cover media; in [34] the host signal is an auditory signal while this paper addresses robust image watermarking problem. Secondly, the mean value in [34] is computed between adjacent coefficients obtained from the same subband, while in our work it is computed from gathered coefficients from different subbands. Thirdly, the embedding method is different, where in [34] the mean value is moved to the nearest integer multiple of the used quantization step. However, in this work the watermark is embedded by changing the sign of the mean value.

The rest of this paper is organized as follows. In Section 2, we introduced the advantages of the used watermark carrier. Section 3 describes how the watermark is inserted and detected. The performances of our scheme are evaluated and discussed in Section 4. Finally, the conclusions are stated in Section 5.

2. Watermark Carrier Selection

As discussed in the previous section, the selection of a watermark carrier involves the choice of a transform domain alongside with an adequate representation.

2.1. Transform Domain. The wavelet transformation (WT) is a mathematical tool used to analyze a discrete or continuous signal by extracting its frequency components and localize them in time. Hence, it allows access to important information unattainable in the original representation. The WT is widely used in multidisciplinary fields such as astronomy, economy, earthquake prediction, signal processing, and watermarking. Although developed on the basis of the Fourier transform, the WT is more effective in terms of computational complexity and frequency localization.

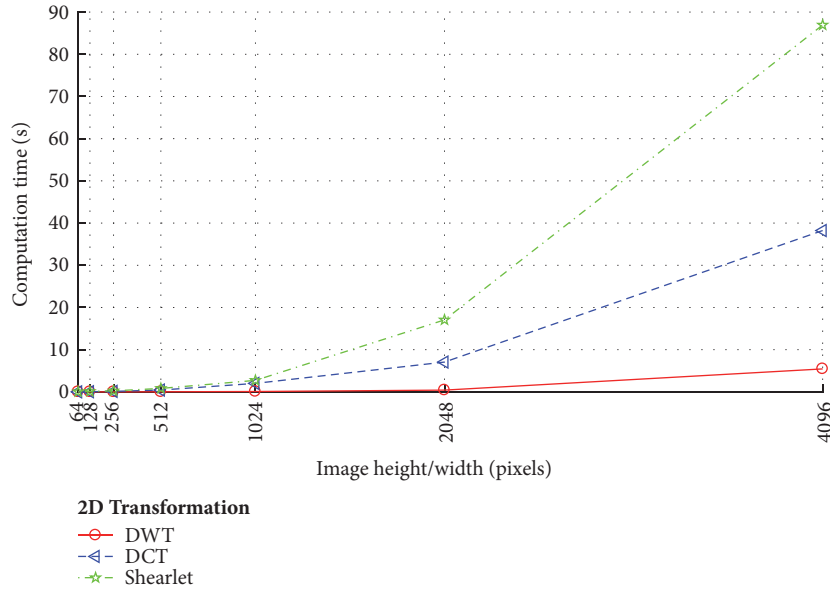


FIGURE 1: Computational time evolution with respect to the image dimension of some 2D transformations.

In order to prove the complexity advantage of the DWT over other transformations, the computational time of the DWT (1 level), DCT (8×8 blocks), and the Shearlet transform are examined using different image sizes (Figure 1). These transformations are employed in [7, 28, 35], [13, 20, 36], and [27] respectively. The advantage of the DWT over other transformations is clear for large image sizes and especially over the DCT, which is the most time consuming among the three evaluated transformations.

Due to the above advantages, we adopted the DWT transformation in our scheme. When applied to an image, the DWT is achieved by filtering separately the rows and columns of the image. Each individual image transformation produces four separable subbands: one coarse subimage locating the low frequencies (*LL*), and three locating the horizontal (*HL*), vertical (*LH*), and diagonal (*LL*) details (high frequencies). The WT may be repeated, as appropriate, by filtering again the low frequency subband. Each individual operation stage produce a resolution level, and each higher level yields to a better frequency localization, but a shrinkage in the subband size. From the perspective of imperceptibility, the *LL* subband is inappropriate for watermark insertion. The approximation coefficients represent the low frequencies that reflect significant information about an image. Thus, the manipulation of these coefficients provokes quality degradation. On the other hand, the modification of the *HH* coefficients may go unnoticed, but the watermark may be easily removed by image processing tasks such as lossy compression. The remaining subbands (*HL* and *LH*) serve as a good candidate for watermark embedding. They are midfrequency subbands; thus they are less noticeable and more robust than the *LL* and *HH* subbands, respectively.

2.2. Carrier Selection. Regardless of the insertion method, there are always two ways to embed a watermark; either to

insert one bit in a single coefficient or one bit in multiple coefficients. The latter solution leads to some important advantages of both robustness and imperceptibility [36]. In fact, a good watermark carrier has to guarantee two main properties: a high robustness combined with a low perceptibility. From a carrier's point of view, these properties are manifested by a low distortion after attacks and an imperceptible change after embedding the watermark. The blocks' mean values (BMV) of *HL* and *LH* subbands satisfy the above requirements; it is computed from multiple coefficients, and it manifests a high robustness and imperceptibility. To prove this claim, we analyze the variation of BMVs through the cumulative distribution function (CDF), where each block is constructed by gathering eight coefficients from unrepeated random positions. The insertion of a watermark bit into a BMV can only be accomplished through the modification of its block-coefficients. Hence, to emulate the insertion, we propose to modify all the coefficients of each block by a fixed value (negative or positive).

First, we investigate the quality of the resulting image. The CDF in Figure 3(b) shows the large variations of the BMVs expressed in terms of percentage; the variation reaches up to 2 000%, where 58% of the BMVs are modified between 100% and 950% from their original values. Despite this large variation, the modified image (Figure 2(b)) remains highly similar to the original one (Figure 2(a)).

Concerning the robustness, Figures 3(c) and 3(d) depict the variation of BMVs, always in terms of percentage, after JPEG compression and median filtering, respectively. Here, we can observe the limited variation, which implies a high robustness. In fact, in 72% of the cases, the variation is less than 10% after compression and less than 20% in 73% of the times after filtering operations. In both cases the variation is less than 30% in 83% of the BMVs.



FIGURE 2: Lena image (a) original and (b) after modification of all the HL_1 and LH_1 coefficients.

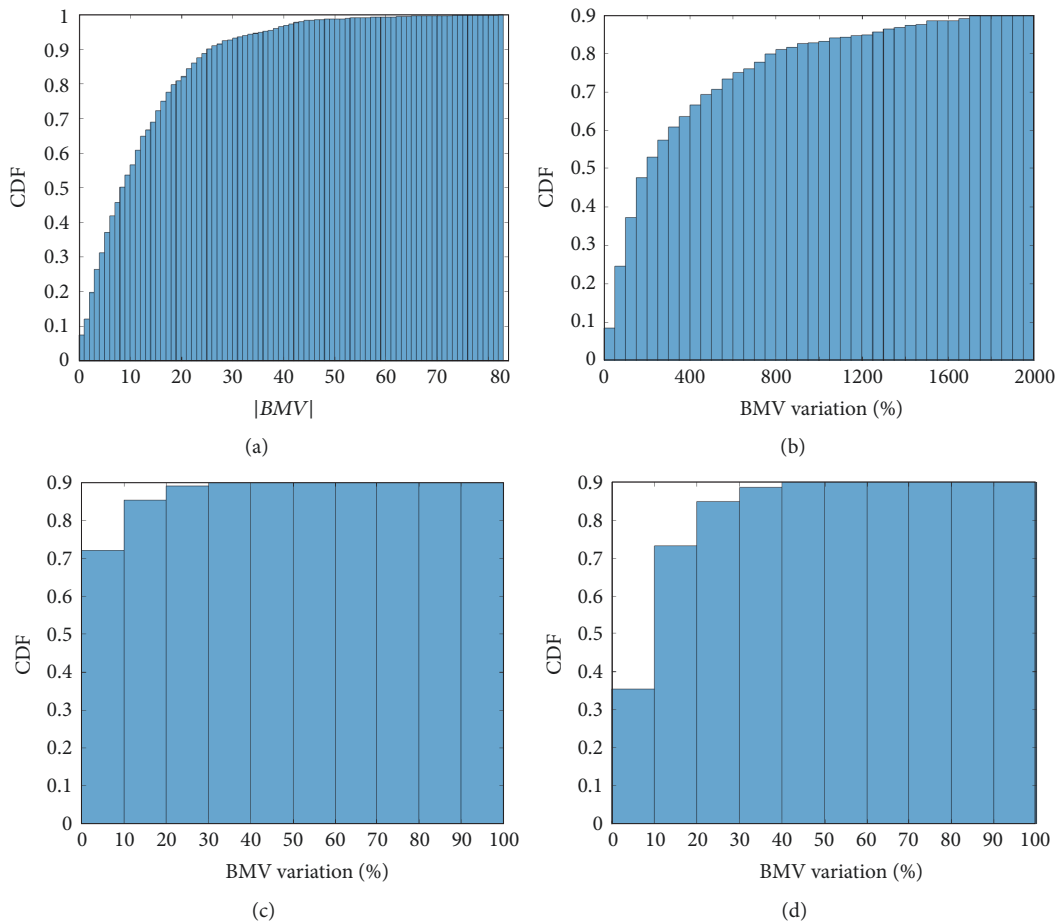


FIGURE 3: Absolute value of Cumulative histogram of (a) original BMVs, (b) difference between the original BMVs and the altered ones ((a) and (b)), (c) difference after JPEG(30) compression, and (d) difference after median filtering (3×3).

It is worth noting that despite the robustness and imperceptibility of the BMVs, the final results will also depend on the insertion and detection method described in the next section.

3. The Proposed Scheme

This section describes the insertion and extraction processes of a binary watermark $M = \{b_1, b_2, \dots, b_m\}$, in a grayscale

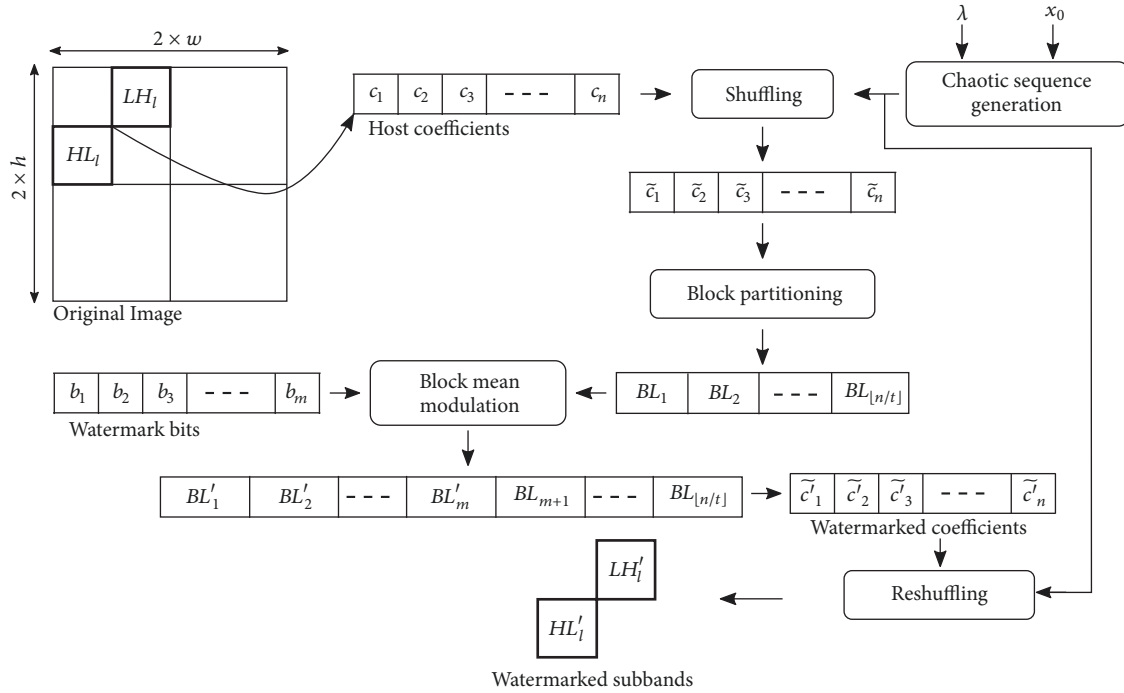


FIGURE 4: Block diagram of the watermark embedding scheme.

image I with $2 \times h$ height and $2 \times w$ width. At this point, the embedding parameters are not specified but kept generalized to point out the flexibility of the scheme. At first, the original image goes through l levels of DWT in order to manifest the different frequencies of the image. For the reasons presented in Section 2, the LH_l and the HL_l subbands are selected for embedding. Let $LH_l = \{LH(i, j)\}$ and $HL_l = \{HL(i, j)\}$, be the full set of carrier coefficients, where $i \in [1, w/2^{l-1}]$, and $j \in [1, h/2^{l-1}]$. The coefficients of the two subbands are then concatenated into a single vector $C = \{c_k\}$, where $k \in [1, n]$ and $n = h \times w/2^{2l-3}$. Next, the carrier vector C is shuffled using a chaotic sequence generated using the logistic map, and each watermark bit is embedded by modulating the mean value of a set of coefficients. The complete block diagram of the embedding process is given in Figure 4. The three main stages involved in the watermarking process (chaotic sequence generation, coefficients shuffling, and mean block modulation) are detailed in the rest of this section.

3.1. Chaotic Sequence Generation. Chaotic maps are dynamic systems defined by a mathematical function ($x_{n+1} = f(x_n)$) that model a chaotic behavior. In practice, a variety of chaotic systems may be utilized (e.g. Baker's map, circle map, duffing map, logistic map, etc.). The implementation of the latter is one of the simplest thanks to its polynomial mapping degree, though it's high dynamic complexity. These features allowed the logistic map to attract a lot of attention in the information security disciplines such as cryptography and watermarking.

The logistic map may be described by the following recurrence relation:

$$x_{n+1} = f(x_n) = \lambda(x_n - x_n^2) \quad (1)$$

The chaotic sequence x_n generated by the function f after n iterations is determined by its input parameters λ and x_0 , where x_0 is the initial value of the sequence and λ is the control parameters. In practice x_0 is choosing between $[0, 1]$ and λ lies between 3.569955672 and 4. These ranges guarantee a chaotic sequence with a high randomness in the output, where the slightest difference in the initial parameters (x_0 and λ) will lead to uncorrelated sequences over time.

3.2. Shuffling. In the shuffling phase, the elements of the vector C are assigned to new positions according the generated chaotic sequence. The objective of this shuffling is double-fold. Firstly, it aims to improve the security of the scheme; the t coefficients forming each block (BL) are randomly selected, thereby making it difficult for a third party to extract the watermark or selectively attack the host coefficients to destroy the watermark without the permutation sequence. Secondly, the shuffling dispels the correlation between adjacent coefficients. In fact, adjacent coefficients tend to be of the same sign, leading to MVBs distant from zero. In contrast, the MVBs of scattered coefficients are gathered around the zero value, which will serve us to minimize the embedding strength and hence the perceptibility of the watermark.

The logistic map defined by (1) is employed to produce a pseudo-random key containing the new positions for each coefficient.

Let $\{x_n\} = (x_1, x_2, x_3, \dots, x_n)$ be the chaotic sequence generated by means of the logistic map using the secret key $SK = \{x_0, \lambda\}$, where n is the number of iterations that is equal to the total number of coefficients in LH_l and HL_l . The x_n coefficients are then sorted in a ascending

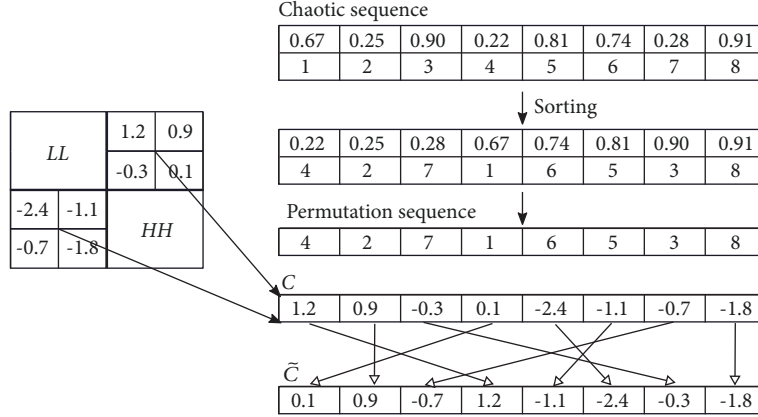


FIGURE 5: Shuffling of DWT diagonal subbands using a chaotic sequence of eight real numbers.

order $(x_{s_1}, x_{s_2}, x_{s_3}, \dots, x_{s_n})$, and so the permutation sequence $(s_1, s_2, s_3, \dots, s_n)$ is obtained.

The example shown in Figure 5 illustrates a concrete example for the shuffling operation. In this example, n is equal to eight, the vector C is the concatenation of the diagonal DWT coefficients, and \tilde{C} is the shuffled version of C .

3.3. Block Mean Modulation. The first step in the block modulation phase is the partitioning of the confused host coefficients \tilde{c}_i into independent blocks. This operation is realized by gathering each t adjacent coefficients into a single block BL_i as given by (2), where i is the index of the block and \parallel is the concatenation symbol. The total number of generated blocks BL should be larger or equal than the binary watermark message length. In other words, $\lfloor n/t \rfloor \geq m$ such as $t \in \mathbb{N}^*$.

$$BL_i = \parallel_{j=t(i-1)+1}^{ixt} \tilde{c}_j = \{\tilde{c}_{it-t+1}, \tilde{c}_{it-t+2}, \dots, \tilde{c}_{it}\} \quad (2)$$

To embed a robust watermark, we consider the quantization technique, which modulates the carrier hosts to P nonoverlapping sets, where P represents the possible embedded words. In this work, the watermark is a binary message, hence the carrier will be modulated to two different sets ($p = 2$), each associated to a watermark bit. The robustness of the quantization-based insertion method depends on the distance between the two sets. On the other hand, widening the gap will lead to mediocre results in terms of visual quality. To work around this issue, Chen et al. [10] proposed to increase the element of each set, and it is up to the embedding algorithm to choose the appropriate quantizer among the available ones. However, as illustrated in Figure 3(a), most of the BMVs are concentrated around the zero, where in 80% of the BMVs are in the range $[-20, 20]$. Thus, we propose to modulate the blocks' mean values by a positive or negative number according to the embedded bit. Let \overline{BL}_i be the mean value of the block i defined by

$$\overline{BL}_i = \frac{1}{t} \sum_{j=t(i-1)+1}^{ixt} \tilde{c}_j \quad (3)$$

The modulation of \overline{BL}_i goes by firstly nullifying the mean value by spreading its value equally to all block's coefficients, then adding or subtracting a threshold T according to the embedded bit b . The equation of modulation is given by (4), where \tilde{c}_k is a coefficient belonging to the block i (BL_i).

$$\tilde{c}'_k = \begin{cases} \tilde{c}_k - \frac{\overline{BL}_i}{t} - T, & \text{if } b = 0. \\ \tilde{c}_k - \frac{\overline{BL}_i}{t} + T, & \text{otherwise.} \end{cases} \quad (4)$$

Once all the watermark bits are inserted, the watermarked coefficients are rearranged into their initial positions using the same key SK. Finally, the inverse DWT is performed to obtain the watermarked image.

3.4. Watermark Extraction. In the watermark extraction phase, the watermarked image is firstly transformed in the frequency domain, as in the embedding, and the same key SK is used to constitute different blocks. The decision upon the embedded bit is judged according to the block's mean value of the attacked watermarked block \overline{BL}_i

$$b = \begin{cases} 1, & \text{if } \overline{BL}_i > 0. \\ 0, & \text{otherwise.} \end{cases} \quad (5)$$

4. Experimental Results

This section is dedicated to evaluate the performance of the suggested watermarking framework. A variety of 8-bit depth ($d = 8$) grayscale standard benchmark images, with a resolution of 512×512 pixels ($w = h = 256$), have been subjects of assessment. The used image database includes Lena, Baboon, Peppers, and Tank. These images present a variety of image properties (e.g., mixture of dark and light area, alongside with highly textures regions (hair) in the Lena image), which refutes the idea of tying the performance of the scheme to some image properties.

The performance of the suggested method is experimentally examined from different aspects. Firstly, the relation

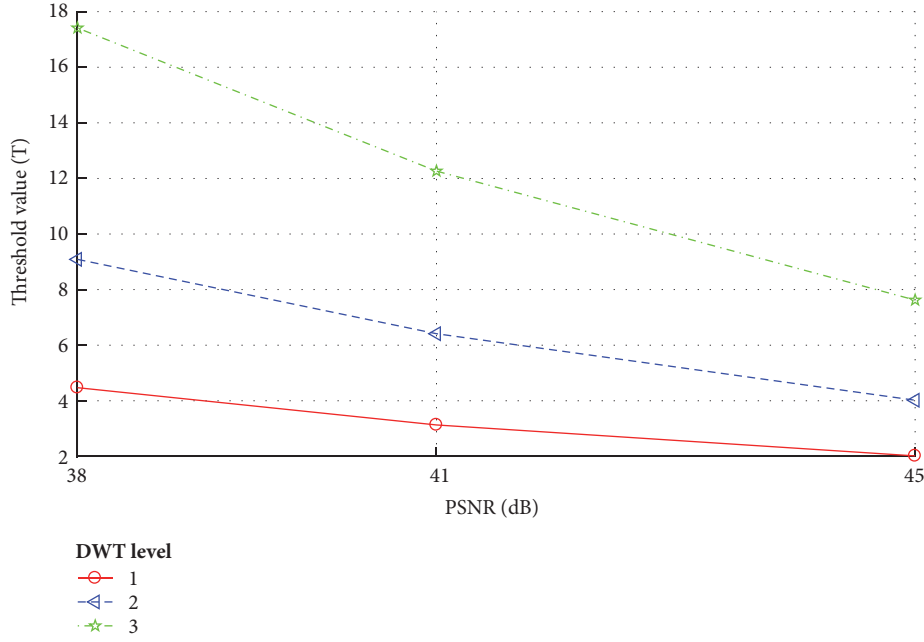


FIGURE 6: Relation of threshold value (T) and the PSNR at different DWT levels.

between the capacity and the imperceptibility is evaluated using different insertion parameters. Next, the evolution of complexity according to the host image size is monitored. Afterwards, the robustness is validated in two ways: initially the robustness against different levels of attacks is examined and then a comparative study with similar works is presented. Finally, the security of the scheme is verified.

4.1. Imperceptibility. The imperceptibility feature reflects the fidelity of the watermarked image toward the original one. Several metrics can be used to quantify the noticeable difference between two images, involving subjective and objective metrics. In this work we employed the Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index Measure (SSIM) given by (6) and (7), respectively.

$$\text{PSNR}(\mathbf{I}, \mathbf{I}^*) = 10 \log_{10} \left(\frac{(2^d - 1)^2 \times w \times h}{\sum_{i=1}^w \sum_{j=1}^h (\mathbf{I}_{ij} - \mathbf{I}_{ij}^*)^2} \right) \quad (6)$$

$$\text{SSIM}(\mathbf{I}, \mathbf{I}^*) = \frac{(2\mu_{\mathbf{I}}\mu_{\mathbf{I}^*} + S_1)(2\theta_{\mathbf{I}\mathbf{I}^*} + S_2)}{(\mu_{\mathbf{I}}^2 + \mu_{\mathbf{I}^*}^2 + S_1)(\theta_{\mathbf{I}}^2 + \theta_{\mathbf{I}^*}^2 + S_2)} \quad (7)$$

where $\theta_{\mathbf{I}}$ and $\mu_{\mathbf{I}}$ are, respectively, the mean intensity and the standard deviation of the original image \mathbf{I} and $\sigma_{\mathbf{I}\mathbf{I}^*}$ is the sample cross-correlation between \mathbf{I} and \mathbf{I}^* . The constants S_1 and S_2 are defined as $S_1 = (k_1(2^d - 1))^2$ and $S_2 = (k_2(2^d - 1))^2$, where $k_1, k_2 \ll 1$.

4.2. Capacity. The maximum capacity of the proposed scheme depends on three variables: the image dimension (w

and h), the wavelet level (l), and the block length (t). Hence we can express the maximum capacity using


















































































$$\text{Max capacity} = \left\lfloor \frac{w \times h}{t \times 2^{2l-3}} \right\rfloor \quad (8)$$

For a better understanding of the relation between the capacity and imperceptibility, we embedded a variable message size ($m \in \{256, 512, 1024\}$) at different levels of decomposition ($l \in \{1, 2, 3\}$) into three different images namely Lena, Couple, and Baboon. For each watermarking operation, the blocks' size t is maximized so that all coefficients are involved in the watermarking process (e.g., $l = 2$ and $t = 32$ for $m = 1024$). The threshold T is manually chosen to reach a PSNR value of 38, 41, and 45 dB. The parameters of insertion (T, t, l, m), the objective measurements (PSNR and SSIM), and the watermarked images are all listed in Table 1.

The first observation that we draw from Table 1 is that for a given PSNR, the threshold T is converging toward the same value regardless the host image or the watermark size. This amounts to saying that we can anticipate the T value according to the level of transformation and the targeted PSNR. Figure 6 illustrates the relation between these parameters, where T is obtained by averaging all the values for a specific level and PSNR. Secondly, it is shown from Table 1 that at 45 dB, the distortion due to the watermark insertion is invisible whatever the size of the message and the level of decomposition. However, for watermarked images with a PSNR of 38 and 41 dB, the imperceptibility is conditioned upon the level l ; the higher l is, the lower the quality is going to be.

4.3. Complexity. The computational cost of the watermark embedding and extraction is an important aspect that may

TABLE 1: Quality of watermarked images using different insertion parameters (l, T, m).

Message size	Transformation level	Watermarked Lena images			Watermarked Couple images			Watermarked Baboon images		
256	l=1									
	T	4.47	3.12	2.02	4.48	3.13	2.01	4.47	3.13	2.02
	PSNR	37.9943	40.999	44.9961	37.9902	40.9901	44.9993	37.9998	40.9945	44.9965
	SSIM	0.9231	0.9594	0.98329	0.95005	0.97394	0.98938	0.97439	0.98681	0.99468
	l=2									
	T	9.09	6.39	4.01	9.09	6.43	4.02	9.08	6.41	4.01
	PSNR	37.9967	40.9958	44.9995	37.998	40.9941	44.9901	37.9971	40.997	44.9963
	SSIM	0.92872	0.96245	0.9846	0.95373	0.97585	0.99015	0.97628	0.98778	0.99507
	l=3									
T	17.38	12.28	7.64	17.45	12.25	7.61	17.48	12.2	7.59	
PSNR	37.9927	40.996	44.9935	37.9952	40.9955	44.9958	37.9923	40.9987	44.9991	
SSIM	0.955	0.97657	0.99024	0.97074	0.98497	0.99379	0.985	0.9924	0.99687	
512	l=1									
	T	4.47	3.13	2.02	4.47	3.13	2.01	4.46	3.13	2.01
	PSNR	37.9983	40.9968	44.996	37.9973	40.9991	44.9984	37.9992	40.9955	44.9952
	SSIM	0.92319	0.9594	0.98329	0.95006	0.97397	0.98936	0.97443	0.98681	0.99467
	l=2									
	T	9.09	6.41	4.01	9.10	6.42	4.02	9.05	6.40	4.02
	PSNR	37.9985	40.9908	44.9998	37.9937	40.9946	44.9943	37.9965	40.9984	44.9921
	SSIM	0.9288	0.96241	0.98457	0.95359	0.97585	0.99017	0.97633	0.98777	0.99505
	l=3									
T	17.45	12.28	7.62	17.48	12.26	7.64	17.30	12.25	7.61	
PSNR	37.9979	40.9913	44.995	37.9982	40.999	44.9945	37.9974	40.9998	44.9975	
SSIM	0.95478	0.97642	0.99026	0.97061	0.98499	0.99377	0.98524	0.99239	0.99688	
1024	l=1									
	T	4.47	3.13	2.02	4.47	3.13	2.02	4.47	3.13	2.01
	PSNR	37.9984	40.9978	44.9951	37.9984	40.9933	44.9922	37.9969	40.9984	44.998
	SSIM	0.92325	0.9594	0.98329	0.95014	0.9739	0.98937	0.97441	0.98683	0.99467
	l=2									
	T	9.082	6.4117	4.0237	9.10	6.42	4.02	9.08	6.40	4.02
	PSNR	37.9969	40.9961	44.999	37.9905	40.9962	44.9975	37.997	40.9995	44.9942
	SSIM	0.92885	0.96245	0.98456	0.95357	0.9759	0.99016	0.97628	0.98782	0.99506
	l=3									
T	17.40	12.26	7.60	17.44	12.30	7.64	17.35	12.23	7.62	
PSNR	37.9972	40.9987	44.9957	37.9993	40.9988	44.9974	37.9965	40.9997	44.999	
SSIM	0.95549	0.97656	0.99029	0.97078	0.98484	0.99375	0.98521	0.99244	0.99686	

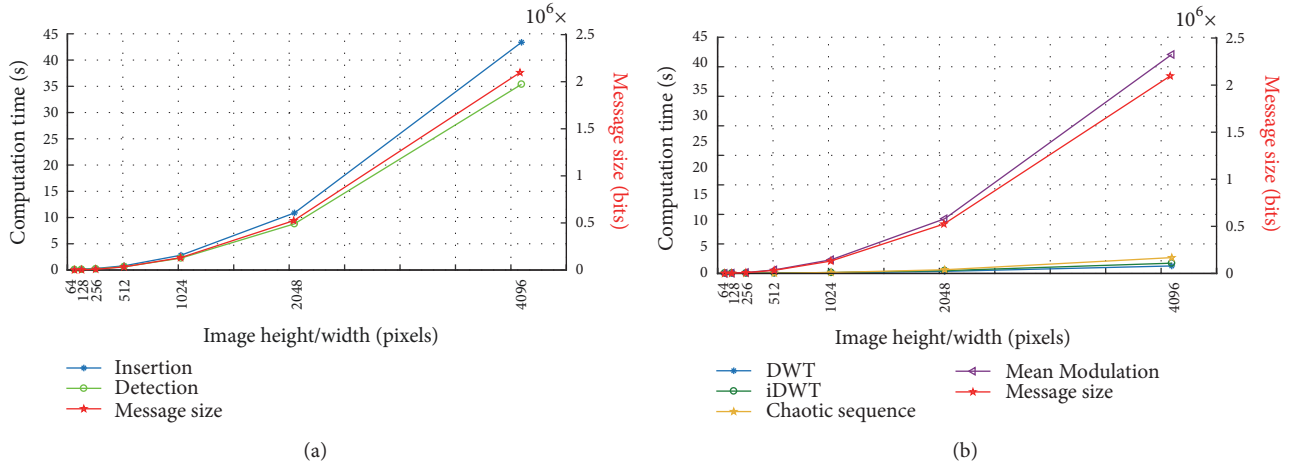


FIGURE 7: Computational time of (a) overall insertion and detection and (b) details of the embedding stage.

restrict or expand the use of a given watermarking scheme. In the literature, most of schemes are evaluated in a standard image with a size of 512×512 pixels, and there is no perspective of the computational cost trend when the image goes bigger, which is more realistic. Hence, we propose to vary the size of the image beginning with 64×64 pixels and ending with 4096×4096 pixels, by doubling the height and width after each insertion. For the sake of simplicity, the watermark was embedded after one level of DWT ($l = 1$), with a fixed block size ($t = 4$) and a maximum watermark size as defined by (8).

Figure 7(a) depicts the execution time evolution of the overall embedding and detection, alongside with the variation of the watermark size (red), as a function of the image size. The details of the embedding phase are shown in Figure 7(b). The most important remark to be made from Figure 7 is that the computational time evolves broadly in line with the watermark size (red curve), to find out the complexity of our scheme in comparison with other state-of-the-art methods.

4.4. Robustness. In the following, we investigate the robustness of the suggested watermarking approach under several types of attacks. The robustness is quantified using the Bit Error Rate (BER) and the Normalized Correlation (NC) metrics.

4.4.1. Evaluated Attacks. Since the proposed scheme is designed to be robust, the embedded message should last, or at least a significant part of it, after image processing operations. From watermark perspective all image processing operations, whatever performed on goodwill or not is considered as attacks. The involved attacks in the evaluation tests are classified into three groups:

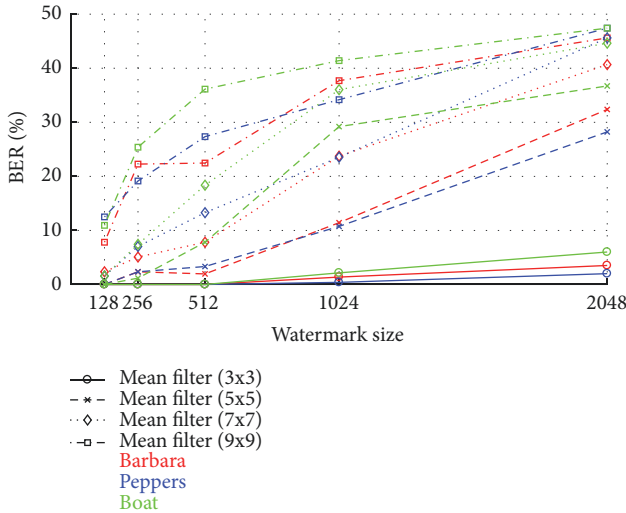
- (i) Compression attacks: usually images are not stored in a raw format, but after a compression operation that aims to reduce the required storage space. JPEG algorithm is one of the most used compression

algorithms. However, JPEG is a lossy algorithm that causes some quality degradation, inversely commensurate with the compression quality factor. Hence, we tested the robustness of our algorithm under different JPEG quality factors ranging from 10 to 90.

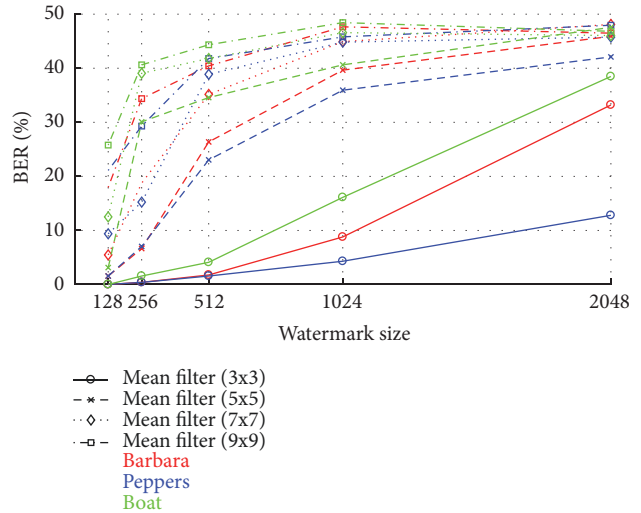
- (ii) Image processing attacks: used to imitate a noise contaminating the image during transmission such as salt and peppers, or to improve the image's quality by eliminating a noise or enhancing some properties. The used attacks are listed as follows: scaling, median filtering, sharpening, Gaussian filtering, average filtering, Gaussian noise, salt and pepper noise contamination, histogram equalization, and additive white Gaussian noise (AWGN).
- (iii) Geometric attacks: used to correct geometric distortions such camera orientation (rotation), or images' alignment (cropping). The used attacks are listed as follows: image cropping and resizing and rotation.

Since the DWT coefficients are not geometrically invariant, a manual synchronization of the image's dimension and orientation was realized prior to the extraction.

4.4.2. Performance Evaluation. Here we test the robustness of our scheme on three different images: Boat, Peppers and Barbara. Each time, we varied the embedded message between 128 bits and 2048 bits. The embedding threshold T is manually tuned to provide a watermarked image with a PSNR value of 40 dB and 45 dB. The robustness is expressed in terms of BER (%) after mean filter (Figure 8), JPEG compression (Figure 9), median filter (Figure 10) and gamma correction, Poisson noise, histogram equalization, and image unsharpening (Figure 11). Figures 8–11 show that the robustness performance slightly differs between images. For a small message length (between 128 and 256 bits) and a PSNR value of 40 dB, the BER does not exceed 20% for most of attacks. However the larger the message size is or the stronger the attack is, the higher the BER will be.

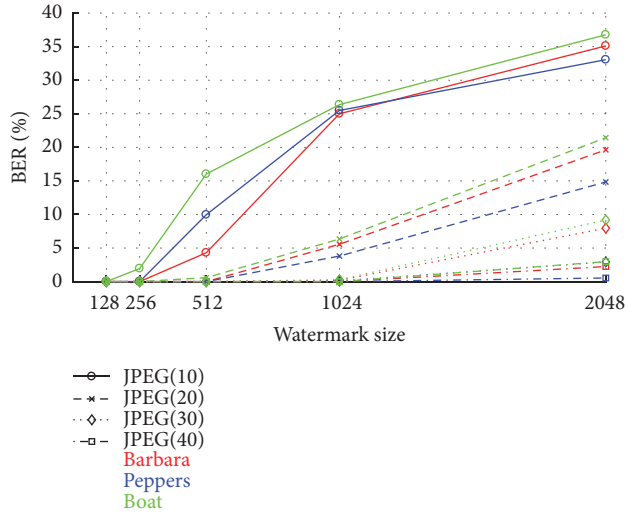


(a)

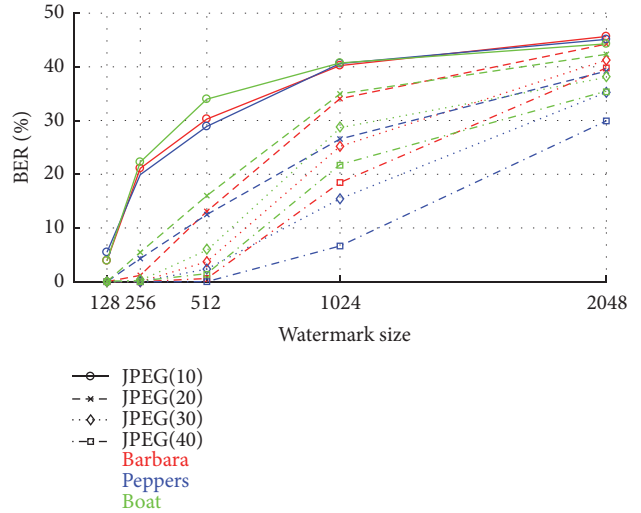


(b)

FIGURE 8: BER(%) after mean filter attacks using different message lengths at different PSNR values (a) 40 dB and (b) 45 dB.



(a)



(b)

FIGURE 9: BER(%) after JPEG compression using different message lengths at different PSNR values (a) 40 dB and (b) 45 dB.

4.4.3. *Comparative Study.* To prove the superiority and the robustness advantages of our scheme a comparative study with state of the art works is indispensable. In fact, we compared the robustness of our scheme with six robust watermarking schemes [26, 27, 35, 37–39]. In order to carry out a fair comparison, the same insertion parameters (PSNR, watermark size) and attacks are used in this comparison. The PSNRs value of different images and their corresponding values in the comparative schemes are illustrated in Figure 12. It is worth mentioning that the insertion parameters (l, t, T) were empirically chosen to produce the same PSNR alongside with an acceptable visual quality.

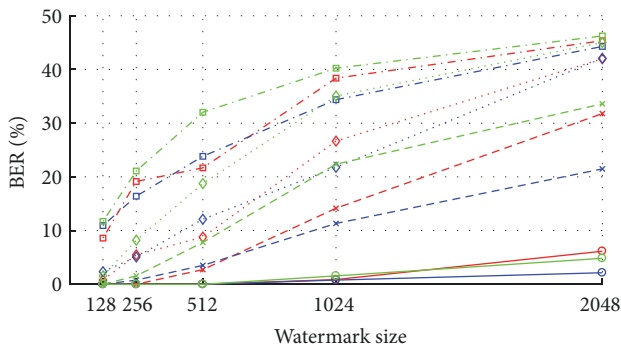
The robustness results are presented in Tables 2–5, in terms of either BER or NC depending on how they appear in the reference papers, and the superior results are marked in bold number.

Based on the simulation results given in Tables 2–5, it can be found that our approach outperforms similar schemes on 71.94% of the time. Equal results are obtained on 23.43% of the time, and our scheme underperforms on 4.62% of the cases.

4.5. *Security.* The robustness of a watermarking scheme is not sufficient to judge a scheme as reliable. As discussed in the first section, robust watermarking is used to secure images. Hence, the security is necessary. First, the watermark should be immune against illegal extraction, even when the embedding procedure is exposed. Second, the watermark detector should not report the existence of the watermark when none is embedded. To evaluate these two risks, we extract the watermark from a watermarked image using

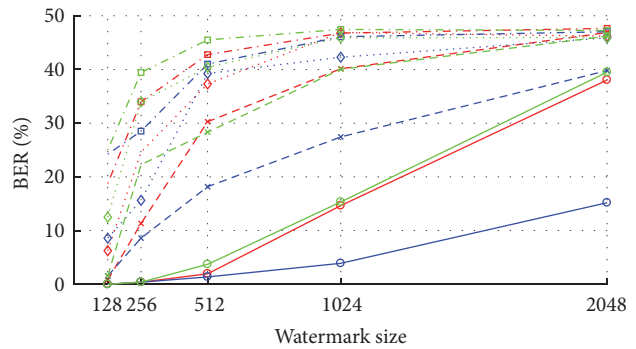
TABLE 2: BER comparison with [27] and [37] using a message length of 128 bits.

Benchmark image	Couple			Barbara			Mandrill		
watermarking method	[27]	[37]	Proposed	[27]	[37]	Proposed	[27]	[37]	Proposed
JPEG (30)	0,0781	0,0703	0	0,0938	0,0859	0	0,0938	0,0859	0
JPEG (40)	0,0625	0,0625	0	0,0781	0,0781	0	0,0781	0,0781	0
JPEG (50)	0,0547	0,0547	0	0,0625	0,0703	0	0,0625	0,0625	0
JPEG (60)	0,0391	0,0469	0	0,0391	0,0547	0	0,0469	0,0547	0
JPEG (70)	0,0313	0,0391	0	0,0301	0,0469	0	0,0313	0,0391	0
Median filtering (3 × 3)	0,0625	0,0938	0	0,0703	0,1016	0	0,0625	0,0859	0
Median filtering (5 × 5)	0,0781	0,1094	0	0,0781	0,1094	0,0234	0,0781	0,0938	0,0234
Median filtering (7 × 7)	0,0859	0,1171	0,0078	0,0859	0,1250	0,0625	0,0859	0,1094	0,0781
Median filtering (9 × 9)	0,0938	0,1328	0,0625	0,1016	0,1406	0,1718	0,0938	0,1250	0,1796
AWGN (15)	0,0234	0,0547	0	0,0078	0,0469	0	0,0156	0,0547	0
AWGN (20)	0,0313	0,0703	0	0,0156	0,0625	0	0,0312	0,0547	0
AWGN (25)	0,0313	0,1016	0	0,0313	0,0781	0	0,0469	0,0859	0
AWGN (30)	0,0391	0,1328	0	0,0391	0,1094	0	0,0781	0,1170	0
Salt & Peppers (0,01)	0,0234	0,0547	0	0,0156	0,0547	0	0,0391	0,0547	0
Salt & Peppers (0,02)	0,0313	0,0625	0	0,0156	0,0547	0	0,0547	0,0781	0
Salt & Peppers (0,04)	0,0391	0,0781	0	0,0313	0,0781	0,0078	0,0625	0,1094	0,0078
Salt & Peppers (0,05)	0,0469	0,0781	0	0,0391	0,0859	0,0078	0,0781	0,1171	0,0468
Scaling (0,8)	0,0391	0,0391	0	0,0313	0,0234	0	0,0391	0,0469	0
Scaling (0,9)	0,0234	0,0313	0	0,0234	0,0234	0	0,0391	0,0391	0
Scaling (1,1)	0,0313	0,0391	0	0,0313	0,0313	0	0,0156	0,0234	0,0234
Scaling (1,5)	0,0391	0,0469	0	0,0391	0,0391	0	0,0313	0,0313	0
Scaling (1,2)	0,0547	0,0547	0	0,0313	0,0547	0	0,0313	0,0547	0
Rotation (-10°)	0,0703	0,0859	0,0078	0,0625	0,0781	0,0390	0,0469	0,0469	0,0312
Rotation (-5°)	0,0625	0,0781	0,0078	0,0547	0,0547	0,0156	0,0313	0,0313	0,0078
Rotation (-1°)	0,0469	0,0703	0,0078	0,0234	0,0313	0	0,0156	0,0234	0,0156
Rotation (1°)	0,0391	0,0625	0,0156	0,0234	0,0234	0	0,0078	0,0234	0,0156
Rotation (5°)	0,0547	0,0781	0,0156	0,0391	0,0469	0,0078	0,0234	0,0313	0,0234
Rotation (10°)	0,0625	0,0938	0,0078	0,0547	0,0703	0,0390	0,0391	0,0391	0,0156



○ Median filter (3x3)
 × Median filter (5x5)
 ◇ Median filter (7x7)
 □ Median filter (9x9)
 Barbara
 Peppers
 Boat

(a)



○ Median filter (3x3)
 × Median filter (5x5)
 ◇ Median filter (7x7)
 □ Median filter (9x9)
 Barbara
 Peppers
 Boat

(b)

FIGURE 10: BER(%) after median filter attacks using different message lengths at different PSNR values (a) 40 dB and (b) 45 dB.

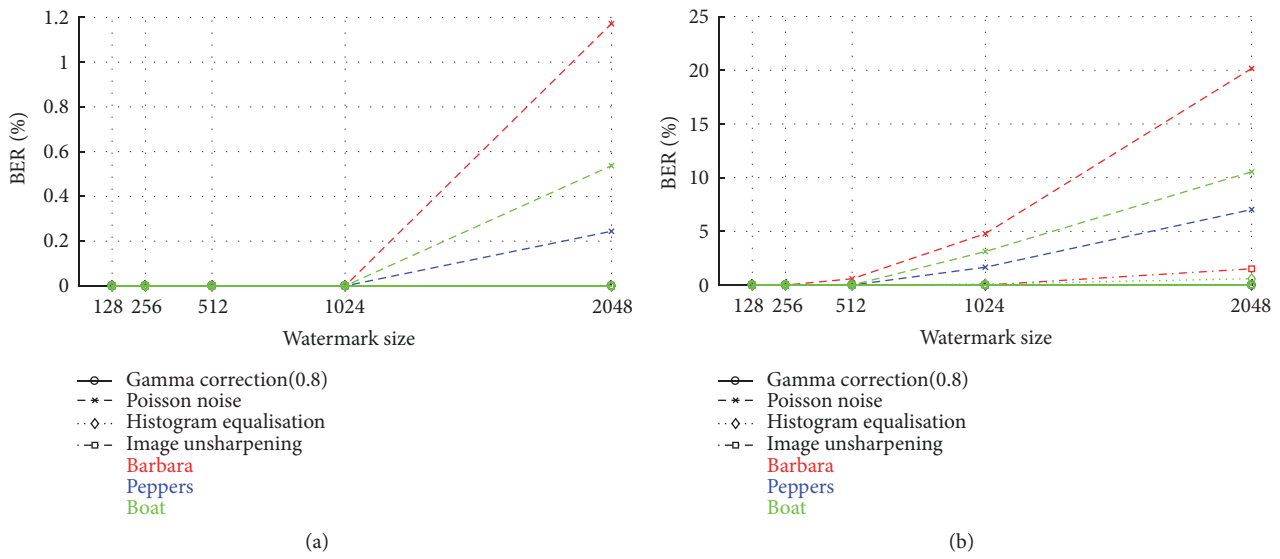


FIGURE 11: BER(%) after various attacks using different message lengths at different PSNR values (a) 40 dB and (b) 45 dB.

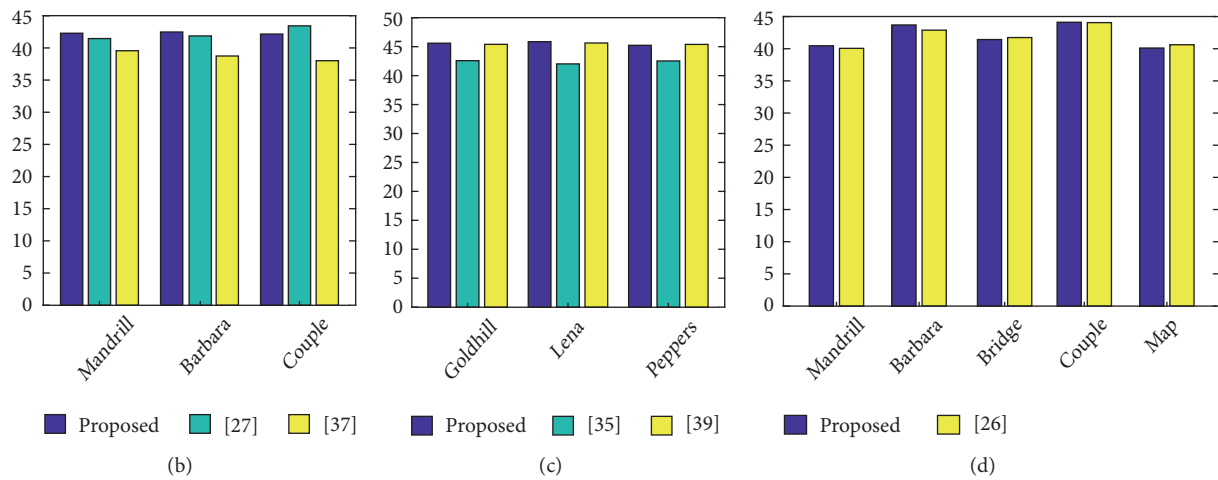
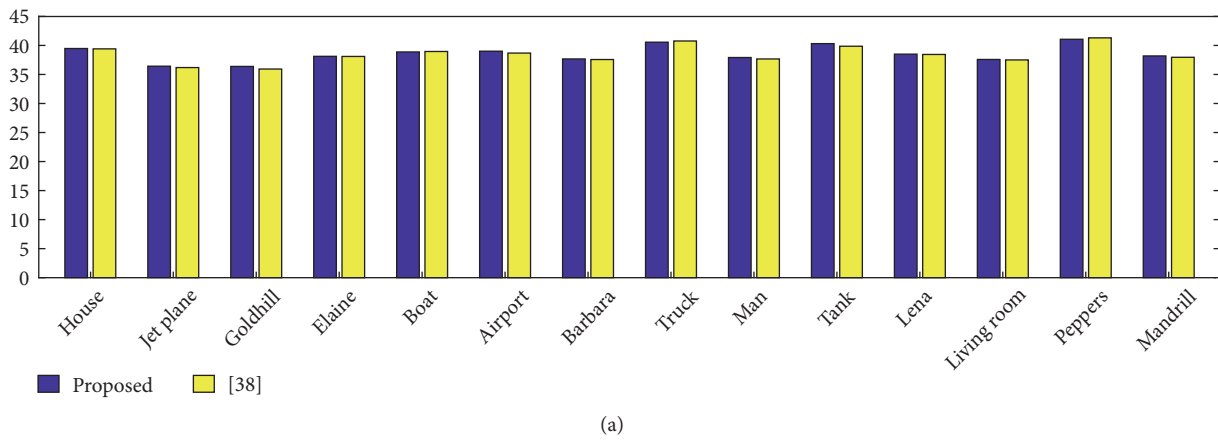


FIGURE 12: PSNR values of different experimentations: (a) Table 3, (b) Table 2, (c) Table 4, and (d) Table 5.

TABLE 4: NC comparison with [35] and [39] using a message length of 512 bits.

Benchmark image	Lena			Goldhill			Peppers		
	[35]	[39]	Proposed	[35]	[39]	Proposed	[35]	[39]	Proposed
watermarking method	[35]	[39]	Proposed	[35]	[39]	Proposed	[35]	[39]	Proposed
Median filtering (3×3)	0,9000	0,9300	0,9770	0,8500	0,9000	0,9725	0,9200	0,9200	0,9713
Median filtering (5×5)	0,7600	0,5700	0,8199	0,6600	0,4600	0,7296	0,7500	0,6200	0,7782
Resize (0,5)	0,8800	0,9700	0,9730	0,8400	0,9400	0,9667	0,8800	0,9500	0,9696
Cropping (25%)	0,6600	0,8800	0,9374	0,6500	0,8200	0,9232	0,6400	0,7600	0,9493
Image sharpening	0,9700	0,4700	1	0,9500	0,5400	1	0,9600	0,4600	1
Gaussian filter	0,8800	0,9900	1	0,9300	0,9900	1	0,9200	0,9800	1

TABLE 5: BER(%) comparison with [26] using a message length of 128 bits.

Attack	Method	Barbara	Mandrill	Map	Couple	Bridge
JPEG (10)	[26]	5,4700	5,47	6,25	21,8800	14,0600
	Proposed	0,0078	0	0	0,1250	0,0078
JPEG (20)	[26]	0,7800	2,34	0	5,4700	3,1300
	Proposed	0	0	0	0,0078	0,0078
JPEG (30)	[26]	0	0	0	3,9100	0,7800
	Proposed	0	0	0	0	0
JPEG (40)	[26]	0	0	0	2,3400	0
	Proposed	0	0	0	0	0
JPEG (50)	[26]	0	0	0	0	0
	Proposed	0	0	0	0	0
JPEG (60)	[26]	0	0	0	0	0
	Proposed	0	0	0	0	0
JPEG (70)	[26]	0	0	0	0	0
	Proposed	0	0	0	0	0
JPEG (80)	[26]	0	0	0	0	0
	Proposed	0	0	0	0	0
JPEG (90)	[26]	0	0	0	0	0
	Proposed	0	0	0	0	0
Scaling (0,75)	[26]	0	0	0	0	0
	Proposed	0	0	0	0	0
Scaling (0,8)	[26]	0	1,50	0	0	0
	Proposed	0	0	0	0,0078	0
Scaling (0,9)	[26]	0	0	0	0	0
	Proposed	0	0	0	0	0
Scaling (1,1)	[26]	0	2,34	0,78	0	1,5600
	Proposed	0	0	0	0,0312	0,0078
Scaling (1,5)	[26]	0	0	0	0	0
	Proposed	0	0	0	0	0
Scaling (2)	[26]	0	0	0	0	0
	Proposed	0	0	0	0	0

different keys, and extract a watermark from a nonwatermarked image respectively. In the two cases, the maximum correlation obtained has not exceeded the value 0.59, which points out a negative presence.

5. Conclusion

The mean value of DWT's vertical and horizontal subbands coefficients is highly robust and imperceptible. In fact, these

two advantages were exploited in the design of a robust and blind watermarking approach. The embedding method consisted in modulating the BMV in accordance with the quantization technique. The use of a single transformation domain alongside with a simple embedding technique makes from the proposed algorithm computationally undemanding. At the extraction phase the watermark bits were identified by the BMV position with respect to the zero value. Unlike some existing schemes, the extraction rules did not require to

be adjusted to the applied attacks to fulfill a high robustness. In fact the inserted watermark was capable to withstand with no error after JPEG compression up to a quality factor of 30, Gaussian filter, and other attacks.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] S. Liansheng, Z. Bei, W. Zhanmin, and T. Ailing, "An optical color image watermarking scheme by using compressive sensing with human visual characteristics in gyrator domain," *Optics and Lasers in Engineering*, vol. 92, pp. 85–93, 2017.
- [2] D. Shukla and M. Sharma, "A Novel Scene-Based Video Watermarking Scheme for Copyright Protection," *Journal of Intelligent Systems*, vol. 27, no. 1, pp. 47–66, 2018.
- [3] A. Tiwari and M. Sharma, "An efficient vector quantization based watermarking method for image integrity authentication," *Advances in Intelligent Systems and Computing*, vol. 519, pp. 215–225, 2018.
- [4] S. Bravo-Solorio, F. Calderon, C.-T. Li, and A. K. Nandi, "Fast fragile watermark embedding and iterative mechanism with high self-restoration performance," *Digital Signal Processing*, vol. 73, pp. 83–92, 2018.
- [5] A. Ghardallou, A. Kricha, A. Sakly, and A. Mtibaa, "Adaptive block sized reversible watermarking scheme based on integer transform," in *Proceedings of the 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering, STA 2016*, pp. 347–351, Tunisia, December 2016.
- [6] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proceedings of the IEEE International Conference Image Processing (ICIP '94)*, vol. 2, pp. 86–90, Austin, Tex, USA, November 1994.
- [7] W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," *IEEE Transactions on Multimedia*, vol. 10, no. 5, pp. 746–757, 2008.
- [8] S. Bhattacharyya and G. Sanyal, "A Robust Image Steganography using DWT Difference Modulation (DWTDM)," *International Journal of Computer Network and Information Security*, vol. 4, no. 7, pp. 27–40, 2012.
- [9] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: a new modulation technique for robust watermarking," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 898–905, 2003.
- [10] B. Chen and G. W. Wornell, "Provably robust digital watermarking," in *Proceedings of the 1999 Multimedia Systems and Applications II*, pp. 43–54, September 1999.
- [11] Z. Kricha, A. Kricha, and A. Sakly, "Accommodative extractor for QIM-based watermarking schemes," *IET Image Processing*, 2018.
- [12] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure, imperceptible yet perceptually salient, spread spectrum watermark for multimedia," in *Proceedings of the 1996 Southcon Conference*, pp. 192–197, June 1996.
- [13] X. Li, J. Liu, J. Sun, Z. Sun, H. Hu, and L. Zhang, "Improved spread transform dither modulation-based watermark algorithm based on step projection," in *Proceedings of the 2010 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, pp. 1–5, Shanghai, China, March 2010.
- [14] H.-T. Hu and L.-Y. Hsu, "Exploring DWT-SVD-DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression," *Computers and Electrical Engineering*, vol. 41, pp. 52–63, 2015.
- [15] J. Cannons and P. Moulin, "Design and statistical analysis of a hash-aided image watermarking system," *IEEE Transactions on Image Processing*, vol. 13, no. 10, pp. 1393–1408, 2004.
- [16] A. Valizadeh and Z. J. Wang, "An improved multiplicative spread spectrum embedding scheme for data hiding," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1127–1143, 2012.
- [17] M. Kutter, D. Frederic, and F. B. Jordan, *Digital signature of color images using amplitude modulation*, 1997.
- [18] Q. Su and B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft Computing*, vol. 22, no. 1, pp. 91–106, 2018.
- [19] Z. Yanling, Z. Xiaoshi, L. Na et al., "A Digital Image Watermark Algorithm Based on DC Coefficients Quantization," in *Proceedings of the 2006 6th World Congress on Intelligent Control and Automation*, pp. 9734–9738, Dalian, China, 2006.
- [20] R. M. Zhao, H. Lian, H. W. Pang, and B. N. Hu, "A Watermarking Algorithm by Modifying AC Coefficients in DCT Domain," in *Proceedings of the 2008 International Symposium on Information Science and Engineering (ISISE)*, pp. 159–162, Shanghai, China, December 2008.
- [21] B. L. Gunjal and R. R. Manthalkar, "Discrete Wavelet Transform based strongly robust watermarking scheme for information hiding in digital images," in *Proceedings of the 3rd International Conference on Emerging Trends in Engineering and Technology, ICETET 2010*, pp. 124–129, India, November 2010.
- [22] H. Shi and F. Lv, "A Blind Digital Watermark Technique for Color Image Based on Integer Wavelet Transform," in *Proceedings of the 2010 International Conference on Biomedical Engineering and Computer Science (ICBECS)*, pp. 1–4, Wuhan, China, April 2010.
- [23] S. Ranjbar, F. Zargari, and M. Ghanbari, "A highly robust two-stage Contourlet-based digital image watermarking method," *Signal Processing: Image Communication*, vol. 28, no. 10, pp. 1526–1536, 2013.
- [24] Q. Su and B. Chen, "A novel blind color image watermarking using upper Hessenberg matrix," *AEÜ - International Journal of Electronics and Communications*, vol. 78, pp. 64–71, 2017.
- [25] F. Ourique, V. Licks, R. Jordan, and F. Pérez-González, "Angle QIM: a novel watermark embedding scheme robust against amplitude scaling distortions," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '05)*, pp. 797–800, March 2005.
- [26] H. R. Fazlali, S. Samavi, N. Karimi, and S. Shirani, "Adaptive blind image watermarking using edge pixel concentration," *Multimedia Tools and Applications*, vol. 76, no. 2, pp. 3105–3120, 2017.
- [27] X.-Y. Wang, Y.-N. Liu, H. Xu, A.-L. Wang, and H.-Y. Yang, "Blind optimum detector for robust image watermarking in

- nonsampled shearlet Domain,” *Information Sciences*, vol. 372, pp. 634–654, 2016.
- [28] X. Liu, C. Lin, and S. Yuan, “Blind Dual Watermarking for Color Images’ Authentication and Copyright Protection,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 5, pp. 1047–1055, 2018.
- [29] . Poonam and S. M. Arora, “A DWT-SVD based Robust Digital Watermarking for Digital Images,” *Procedia Computer Science*, vol. 132, pp. 1441–1448, 2018.
- [30] S. Fazli and M. Moeini, “A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks,” *Optik - International Journal for Light and Electron Optics*, vol. 127, no. 2, pp. 964–972, 2016.
- [31] K. Kuppusamy and K. Thamodaran, “Optimized Image Watermarking Scheme Based On PSO,” *Procedia Engineering*, vol. 38, pp. 493–503, 2012.
- [32] V. S. Rao, R. S. Shekhawat, and V. K. Srivastava, “A dwt-dct-svd based digital image watermarking scheme using particle swarm optimization,” in *Proceedings of the 2012 IEEE Students’ Conference on Electrical, Electronics and Computer Science*, pp. 1–4, 2012.
- [33] T. T. Takore, P. R. Kumar, and G. L. Devi, “A modified blind image watermarking scheme based on DWT, DCT and SVD domain using GA to optimize robustness,” in *Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016*, pp. 2725–2729, India, March 2016.
- [34] H. Hu, S. Lin, and L. Hsu, “Effective blind speech watermarking via adaptive mean modulation and package synchronization in DWT domain,” *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2017, no. 1, 2017.
- [35] W.-H. Lin, Y.-R. Wang, S.-J. Horng, T.-W. Kao, and Y. Pan, “A blind watermarking method using maximum wavelet coefficient quantization,” *Expert Systems with Applications*, vol. 36, no. 9, pp. 11509–11516, 2009.
- [36] X. Li, J. Liu, J. Sun, X. Yang, and W. Liu, “Step-projection-based spread transform dither modulation,” *IET Information Security*, vol. 5, no. 3, pp. 170–180, 2011.
- [37] M. Hamghalam, S. Mirzakuchaki, and M. A. Akhaee, “Geometric modelling of the wavelet coefficients for image watermarking using optimum detector,” *IET Image Processing*, vol. 8, no. 3, pp. 162–172, 2014.
- [38] V. S. Verma, R. K. Jha, and A. Ojha, “Digital watermark extraction using support vector machine with principal component analysis based feature reduction,” *Journal of Visual Communication and Image Representation*, vol. 31, pp. 75–85, 2015.
- [39] C. Li, Z. Zhang, Y. Wang, B. Ma, and D. Huang, “Dither modulation of significant amplitude difference for wavelet based robust watermarking,” *Neurocomputing*, vol. 166, pp. 404–415, 2015.



Hindawi

Submit your manuscripts at
www.hindawi.com

