Chapter

Blind Wavelet-Based Image Watermarking

Abeer D. Algarni and Hanaa A. Abdallah

Abstract

In this chapter, the watermarking technique is blind; blind watermarking does not need any of the original images or any information about it to recover watermark. In this technique the watermark is inserted into the high frequencies. Three-level wavelet transform is applied to the image, and the size of the watermark is equal to the size of the detailed sub-band. Significant coefficients are used to embed the watermark. The proposed technique depends on quantization. The proposed watermarking technique generates images with less degradation.

Keywords: watermarking, discrete wavelet transform, quantization, blind, coefficients, peak signal-to-noise ratio, normalization, correlation

1. Introduction

Watermarking methods operating in the wavelet domain have become attractive because they have inherent robustness against compression if the low-frequency band is selected for watermark embedding, and, additionally, the wavelet transform provides a multiresolution representation of images, which can be exploited to build more efficient watermark detection schemes. The history of watermarking is presented here. Zhu et al. [1] proposed adding a mark, a Gaussian sequence of pseudorandom real numbers, into all the high-pass bands in the wavelet domain. An algorithm developed by Xia et al. [2] utilizes large DWT coefficients of the high- and mid-frequency bands to embed a random Gaussian distributed watermark sequence. Dugad et al. [3] provided a method to embed a Gaussian sequence of pseudorandom real numbers into selected coefficients in all detailed sub-bands with magnitude above a given threshold in a three-level decomposition with Daubechies-8 filters. In general, the watermark embedded in low-pass bands of the wavelet domain is robust to a group of attacks such as low-pass filtering, Gaussian noise, and lossy compression but affects the fidelity of the watermarked image and that in high-pass bands is resistant to another set of attacks such as histogram equalization, intensity adjustment, and gamma correction [4].

2. Blind and non-blind methods

As described before, watermarking methods can be classified according to whether the original data is used in extraction/detection procedure or not. In 1997, Cox et al. [5] proposed a watermarking method where they embed the watermark into the

lower frequency coefficients in the DCT domain. Their method needs the original image and the embedding strength coefficient to detect the presence of the watermark. However, the original source might not be available in several applications. Barni et al. [6] presented a method to overcome the non-blind watermarking problem. They correlate the watermark sequence directly with all coefficients of the received image and then compare the correlation coefficient with some detection threshold. Only, the watermark sequence and the scaling factor are needed in the watermark detection. This approach is widely utilized in the watermarking community. However, it turns out that blind methods are less secure than non-blind methods.

3. Watermarking in transform domains

Watermarking methods can be classified according to whether they use embedding based on additive algorithms or quantization algorithms.

3.1 Additive algorithms

Additive embedding strategies are characterized by the linear modification of the host image and correlative processing in the detection stage. A considerable number of image watermarking methods share this architecture. In most algorithms, the signature data is a sequence of numbers wi of length N that is embedded in a suitable selected subset of the host signal coefficients. The basic and commonly used embedding formulas are defined by the following equations (Eqs. (1) and (2)):

$$V_i^{'} = V_i(1 + k.w_i) \tag{1}$$

$$V_i^{'} = V_i + k.w_i \tag{2}$$

where k is a weighting factor that influences the robustness as well as the visibility and V' is the resulting modified host data coefficients carrying the watermark information. The majority of watermarking systems presented in the literature falls into this class, differing chiefly in the signal design, the embedding, and the retrieval of the watermark content. The extraction process is accomplished by applying the inverse embedding formulas.

The algorithm developed by Dugad et al. [3] makes use of a sequence of pseudorandom Gaussian real numbers, matching the size of the detailed sub-bands of the wavelet domain. The authors performed three-level decomposition with Daubechies-8 filters and selected all coefficients in all detailed sub-bands, whose magnitude is above a given threshold. The equation used for watermark embedding is described in Eq. (3).

For a blind retrieval of the watermark, a statistical detector was proposed based on the following formula:

$$\delta = \frac{\sum_N V_i^* . w_i}{N} \tag{3}$$

where δ is estimated by correlating the watermark sequence w directly with all N coefficients of the received image V^*. A large number of random sequences are tested, but only the sequence that was originally embedded yields the highest

correlation coefficient. Therefore, we can conclude that the image has been watermarked with w. A detection threshold τ can be established to make the detection decision if $\delta\ \tau$. The detection threshold can be derived either experimentally or analytically.

The threshold τ is estimated using Eq. (4):

$$\tau = \frac{\alpha}{2.N}\sum_{i=1}^{N}\left|V_i^*\right| \tag{4}$$

where only the coefficients above the detection threshold are considered.

3.2 Algorithms based on quantization

The quantization schemes perform nonlinear modifications during embedding and detecting the embedded message by quantizing the received samples to map them to the nearest reconstruction point. Quantization is the process of mapping a large possibly infinite set of values to a much smaller set. A quantizer consists of an encoder mapping and a decoder mapping. The range of source values is divided into a number of intervals. The encoder represents each interval with a code word assigned to that interval. The decoder is able to reconstruct a value for every code word produced by the encoder. Scalar quantizes take scalar values as input and output code words, while vector quantizers work with vectors of input sequences or blocks of the source input.

Quantization-based watermarking is a new technique, as a logo is embedded and detected in a blind way. Authors in [6] introduced a scalar quantization watermarking technique, where the watermark is embedded in the middle- and low-frequency bands. The robustness of the algorithm is tested by applying the algorithm to JPEG compression. Only this attack is tested.

Authors in [7, 8] present another quantization-based watermarking algorithm which improves on the Tsai algorithm by incorporating variable quantization and resistance against a wide range of attacks like blurring, noising, sharpening, scaling, cropping, and compression.

The main issue with these quantization-based algorithms is that it only tackles a subset of attacks. For example, Tsai's algorithm is only robust against JPEG compression; however Chen's algorithm does not tackle geometric attacks like rotation. Hence we propose a new algorithm which is robust against cropping, JPEG compression, resizing, rotation, and salt and pepper.

4. Wavelet-based methods

The wavelet transform finds a great popularity in the field of watermarking as it is able to decompose the available images into sub-bands, in which watermarks can be embedded [3, 9]. Taking the cue from the spread spectrum method, we embed the data in transform coefficients chosen in a random order. For extraction of the hidden data, the random sequence must be made available to the extractor. Cox et al. [5] were the first to apply the spread spectrum method to data hiding. Transforms such as the DCT and DWT have been used. The use of the DWT has advantages of speed and robustness against wavelet-based compression. Previously, Dugad's algorithm introduced an additive watermarking technique in the wavelet domain [3]. The proposed technique in this paper uses three-level wavelet

transform using Daubechies filter; the watermark is embedded in the high-frequency domain [9], and it is blind algorithm, and the watermark is detected without using the original image. Also this technique uses only the high value coefficients to insert the watermark. Large wavelet coefficients are referred to edges within an image. So, any degradation in this region won't be noticed by the human viewer. Also it is difficult to remove the watermark without distorting the marked image according to the perceptually significant large magnitude wavelet coefficients. Since watermark verification typically consists of a correlation estimation step, which is extremely sensitive to the relative order in which the watermark coefficients are placed within the image, such changes in the location of the watermarked coefficients were unacceptable. Dugad et al. have proposed a spread spectrum method for digital image watermarking in the wavelet domain, which does not require the original image for watermark detection [3]. This method is based on adding the watermark in selected coefficients with significant image energy in the transform domain in order to ensure non-erasability of the watermark. This method has an advantage over the previous methods, which did not use the original in the detection process and could not selectively add the watermark to the significant coefficients, since the locations of such selected coefficients can change due to image manipulations.

The method proposed by Dugad et al. [3] has overcome the problem of "order sensitivity." It has some advantages such as an improved resistance to attacks on the watermark, an implicit visual masking utilizing the time-frequency localization property of the wavelet transform, and a robust definition for the threshold, which validates the watermark.

The disadvantage of this method is using additive technique in watermarking. In this additive method, the detectors must correlate watermarked image coefficients with the known watermark to know if the image is marked or not. To solve this problem, it is important to correlate a large number of coefficients as possible, but it in turn requires the watermark to be embedded into many image coefficients at the embedding stage. This has the effect of increasing the amount of degradation in the marked image. Another drawback is that the detector can only tell if the watermark is present or absent. It cannot recover the actual watermark. Here, we present a new method to avoid these drawbacks. It is possible to use the advantages of the watermarking scheme by Dugad et al. [3] while avoiding the disadvantages. This can be achieved using the idea of a watermark with the same size as the original image in conjunction with adapted versions of scalar quantization insertion/detection method. The resultant watermarking system will be blind and based on quantization.

A watermark size has to be equal in size to the detailed sub-band in wavelet transform domain, and only significant coefficients will be used to embed watermark. Finally, this new method outperforms the previous method using quantization and a new watermark embedding process, not the additive one. After applying a comparable robustness performance, the watermarked images using our new method give less degradation than Dugad's scheme.

However, only a few of these watermark values are added to the host image. The watermark values are found in fixed locations; thus, the ordering of significant coefficients in the correlation process is not an issue for watermark detection. This gives the technique a value as the correlation process is sensitive to the ordering of significant coefficients, and if there is any change applied to the ordering, it will cause a poor detector response.

In Zolghadrasli's method that is based on the DWT [10], Gaussian noise is used as the watermark. Here the watermark is added to the significant coefficients of each selected sub-band depending on the human visual system (HVS)

characteristics. Any small modifications are performed to improve HVS model. This technique is non-blind as the host image is needed in the watermark extraction.

4.1 Dugad's method

Dugad et al. [3] presented an additive watermarking method operating in the wavelet domain. This method allowed the detection of the watermark without access to the original uncorrupted image.

4.1.1 Embedding algorithm

The embedding algorithm can be summarized in the following steps:

1. From all wavelet coefficients (except the low-pass coefficients in LL band and high-pass coefficients in HH band), the coefficients of magnitude higher than t1 are chosen. This proves that only significant coefficients are used. The wavelet coefficients of magnitude higher than t1 depend upon the smoothness or more details in the image.

2. Then the zero mean and unit variance watermark are generated with a known seed value; the watermark should be equal in size to the input image.

3. The watermark is embedded in each location which has wavelet coefficient with magnitude higher than t1; the watermarked wavelet coefficient is given by Eq. (5):

$$\hat{w}_{ij} = w_{ij} + k\left|w_{ij}\right|x_{ij} \tag{5}$$

where w_{ij} is the wavelet coefficient, k is a scaling parameter, x_{ij} is a watermark value, and is the watermarked wavelet coefficient.

4.1.2 Detection algorithm

1. The watermark is regenerated using the known seed value.

2. All wavelet coefficients (barring the LL and HH components) of magnitude greater than t2 from a possibly corrupted watermarked image are selected. Note that by setting t2 > t1, we find that the robustness is increased, and some wavelet coefficients with magnitudes below t1 may become higher than t1 due to image manipulations.

3. Wavelet coefficients with magnitude higher than t2 are used in the detection process; these detected values are correlated with the watermark values at the same locations. After this correlation process, a yes or no answer will be given as to the presence of the watermark.

5. Non-blind watermarking

Another watermarking method operating upon significant coefficients within the wavelet domain was presented by Miyazaki et al. [9]. This method takes a three-level wavelet transform of the image to be watermarked and inserts the watermark

into the detail coefficients at the coarsest scales (LH3, HL3); the low-pass component LL3 and diagonal details HH3 are excluded.

5.1 Miyazaki's method

Two watermarking algorithms were presented by Miyazaki et al. [9]. Both algorithms were implemented in the wavelet domain, but each targeted a different set of coefficients for insertion. The first of these insertion methods is applied on insignificant coefficients, whereas the second type of insertion is applied on significant coefficients. So, both insertion techniques would be applied to a single image at the same time. However, experimental results proved that the insertion method by applying the significant coefficients was more robust than the insertion method using insignificant coefficients. So, the insertion method utilizing the significant coefficients will be considered.

In this technique three-level wavelet transform is applied to the image, and the watermark is inserted into the detail coefficients at the wavelet level three. The detailed coefficients which are found at level three are the horizontal details, High Low 3 (HL3); the vertical details, Low High 3 (LH3); and the diagonal details, High High 3 (HH3). The low-pass component, Low Low 3 (LL3), is left unchanged. This is a quantization-based watermarking method which aims to modify wavelet coefficients of high magnitude, thus embedding the watermark into edge and textured regions of an image. The process for watermark insertion is as follows:

5.1.1 Embedding algorithm

1. Two thresholds, t1 and t2, are selected, and any one of the sub-bands LH3 and HL3 is chosen. Next, significant coefficients Cok (k = 1, 2... N) satisfying t1 < Cok < t2 are found.

2. A binary watermark is created, Wat (k); k = 1, 2... N.

3. For k = 1, 2,... N, the embedding of the watermark is applied by modifying Ck as follows:

   If Wat(k) = 1 and Cok > 0, then Cok = t2,
   If Wat(k) = 0 and Cok > 0, then Cok = t1,
   If Wat(k) = 1 and Cok < 0, then Cok = −t2,
   If Wat(k) = 0 and Cok < 0, then Cok = −t1,

4. The embedded position, sub-band label, and the two thresholds t1 and t2 should be saved.

5.1.2 Detection algorithm

The following process details the steps involved for watermark detection:

1. Using the sub-band label and the embedded position, the recovered wavelet coefficients Cok. k = 1, 2... N are obtained.

2. Check each Ck individually:

   If Cok < (t1 + t2) /2, then the recovered watermark bit is 0.
   If Cok ≥ (t1 + t2) /2, then the recovered watermark bit is 1.

This thesis introduces a new quantization-based, blind watermarking algorithm operating in the wavelet domain. This algorithm has several advantages as compared to previously published algorithms. For example, the proposed algorithm is better than the algorithm of Dugad in its ability to survive the same malicious attacks while producing marked images of greater visual quality. The proposed watermarking scheme is a blind scheme not requiring a file containing the positions of the marked coefficients as in the method of Miyazaki.

6. The proposed watermarking scheme

The proposed watermarking scheme is a blind quantization-based scheme. A block diagram detailing its steps is shown in **Figure 1**.

6.1 Watermark embedding

1. The cover image is decomposed into sub-bands using three levels of Daubechies wavelet transform using filters of length 4.

2. Then the coefficients in the third level (except the LL3 and HH3 sub-bands) which have magnitude higher than t1 and lower than t2 are chosen to hide in. Let be the wavelet coefficient with maximum absolute in both HL3 and LH3 sub-bands. A threshold t = α is selected, as mentioned in Eq. (6):

$$0.01 < \alpha < 0.1 \text{ and } t2 > t1 > t. \tag{6}$$

3. Then the binary watermark is created using a secret key, which is a seed of a random generator; the watermark size should be of the same size as the two sub-bands which are selected for embedding.

4. Then apply quantization to each of the selected wavelet coefficients.

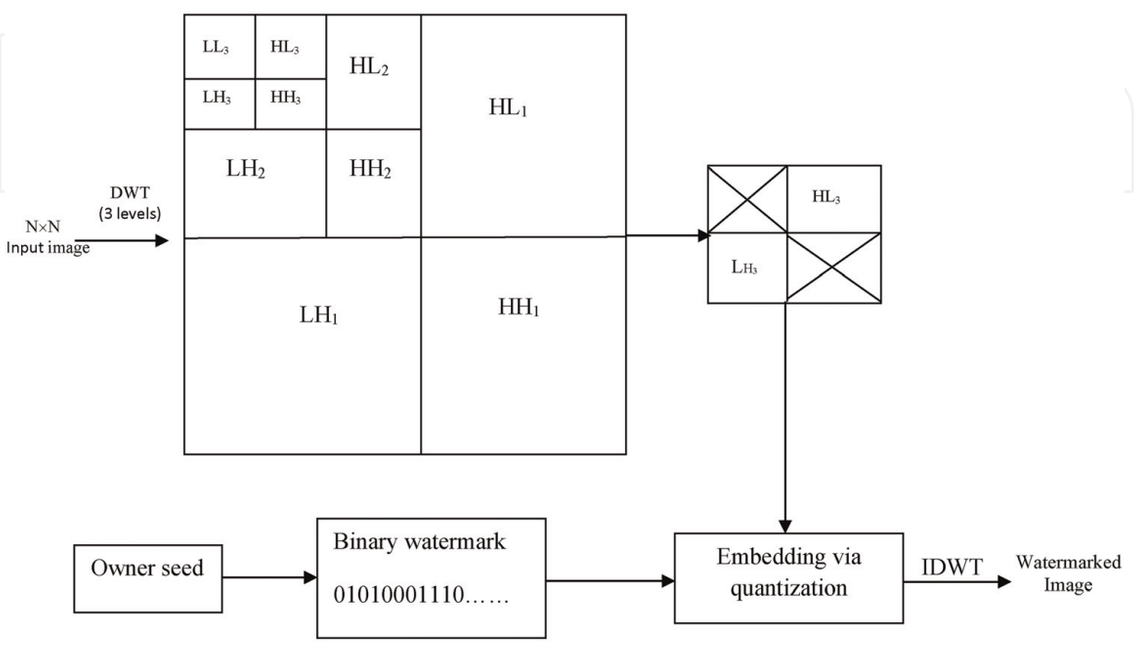

Figure 1.
The proposed image watermarking scheme.

The quantization process is done as shown in Eq. (7):

$$\begin{aligned} &\text{If } = 1 \text{ and } > 0, \text{ then } = t2 - X1, \\ &\text{If } = 0 \text{ and } > 0, \text{ then } = t1 + X1, \\ &\text{If } = 1 \text{ and } < 0, \text{ then } = -t2 + X1, \\ &\text{If } = 0 \text{ and } < 0, \text{ then } = -t1 - X1, \end{aligned} \tag{7}$$

where is the watermark bit corresponding to, and is the watermarked wavelet coefficient. The parameter x1 narrows the range between the two quantization levels t1 and t2 in order to perform a robust oblivious detection. **Figure 2** shows the watermark embedding in a positive wavelet coefficient.

5. After all the selected coefficients are quantized, the inverse discrete wavelet transform (IDWT) is applied, and the watermarked image is obtained.

6.2 Watermark detection

1. The possibly corrupted watermarked image is transformed into the wavelet domain using the same wavelet transform as in the embedding process.

2. The extraction is performed on the coefficients in the third wavelet level (excluding the LL3 and HH3 sub-bands).

3. All the wavelet coefficients of magnitude higher than or equal to t1 + X2 and less than or equal to t2 − X2 are chosen, which are named $w_{ij}^{'s}$. Note that the value of X2 should be lower than the value of X1. This maintains that all the marked coefficients are recovered and dequantized after being attacked. The determination of parameters X1 and X2 to the watermarking technique gives a

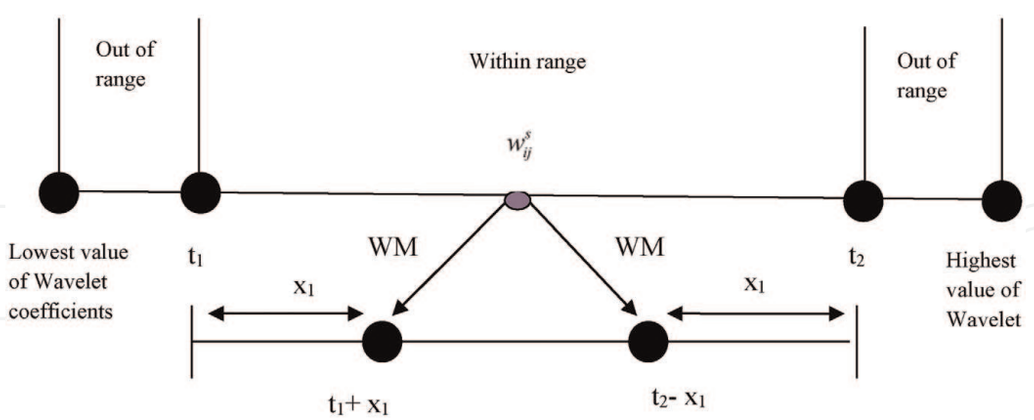

Figure 2.
Watermark embedding for wavelet coefficients in the proposed scheme.

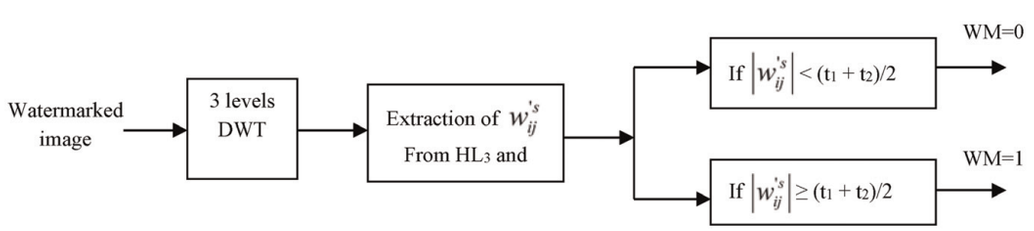

Figure 3.
Watermark detection in the proposed scheme.

degree of tolerance to the system against attacks, i.e., the extraction of watermark bits from the selected wavelet coefficients is done using Eq. (8).

$$\begin{aligned} &\text{If} < (t1 + t2)/2, \text{the recovered watermark bit is } 0. \\ &\text{If} \geq (t1 + t2)/2, \text{the recovered watermark bit is } 1 \end{aligned} \tag{8}$$

The watermark detection process can be shown in **Figure 3**.

Then the correlation process is applied between the recovered watermark and the original watermark, obtained via the secret key, just only in the locations of the selected coefficients.

7. The histogram of equal-area division quantization method in watermarking

The quantization levels are calculated using a method dependent on the image content, and then round off the value of pixels to the nearest quantization level. Using this method, the number of values transmitted over the channel is minimized. HEAD is a quantization method in which the transmitted values are reduced by mapping the values of image pixels to a finite number of quantization levels.

Process of HEAD quantization [11]:

1. First of all, get the histogram of the output, and then the area under the histogram is divided into a number of vertical slices with equal areas. A width of each slice is inversely proportional to its height. Quantization levels are determined by the number of these slices. Both are equal.

2. The midpoint value which is found on the width of each slice is considered as a quantization level.

3. This is called a nonuniform quantization where the density of the quantization levels increases with increasing the probability of the occurrence of the pixel value.

4. We mapped all the pixel values that lie within the width of a slice to the quantization level that is represented by the midpoint of this slice.

7.1 Proposed DWT-HEAD watermarking method

7.1.1 Watermark embedding

The steps of watermark embedding can be summarized as follows:

1. The host image is transformed into the wavelet domain; three-level Daubechies wavelet with filters of length 4 is used. The coefficients of HL3 coefficients are watermarked using HEAD quantization using two quantization levels t1 and t2.

2. Each of the selected wavelet coefficients is quantized. After all the selected coefficients are quantized, the inverse discrete wavelet transform is applied, and the watermarked image is obtained.

7.1.2 Watermark detection

1. The possibly corrupted watermarked image is transformed into the wavelet domain using the same wavelet transform as in the embedding process.

2. The extraction is performed on the coefficients in the first level wavelet transform (HL1).

3. All the wavelet coefficients of magnitude greater than or equal to t1 and less than or equal to t2 are selected. The watermark bits are extracted from each of the selected DWT coefficients with Eq. (9):

$$\text{If} < (t1 + t2)/2, \text{ then the recovered watermark bit is 0.}$$
$$\text{If} \geq (t1 + t2)/2, \text{ then the recovered watermark bit is 1.} \quad (9)$$

8. Simulation results

This section presents the results to compare between the schemes of LSB method, Dugad's method, Miyazaki's method, and the proposed method. Several images are watermarked using the four watermarking methods and subjected to attacks. In order to measure the degradation suffered by host images after watermark insertion, the PSNR is used.

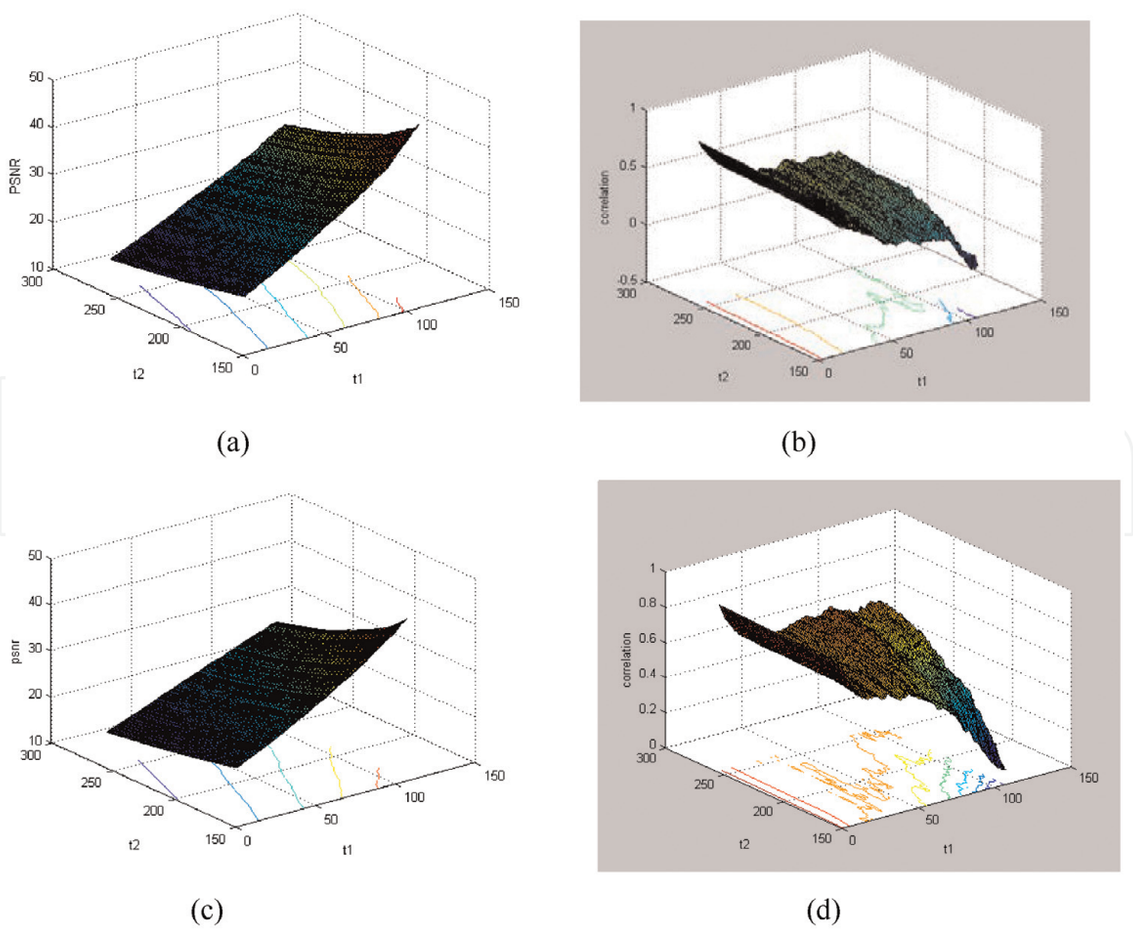

Figure 4.
(a) The thresholds t_1, t_2 vs. PSNR (t_1=115, t_2=200, PSNR=46) (b) Vs. c_r for Mandrill. if image. (t_1=115, t_2=200, c_r = 0.4 in case of resizing) (c) The thresholds t_1, t_2 vs. PSNR.(t_1=90, t_2=200, PSNR=42) (d) Vs. c_r for hat. jpg image (t_1=90, t_2=200, c_r = 0.6 in case of resizing).

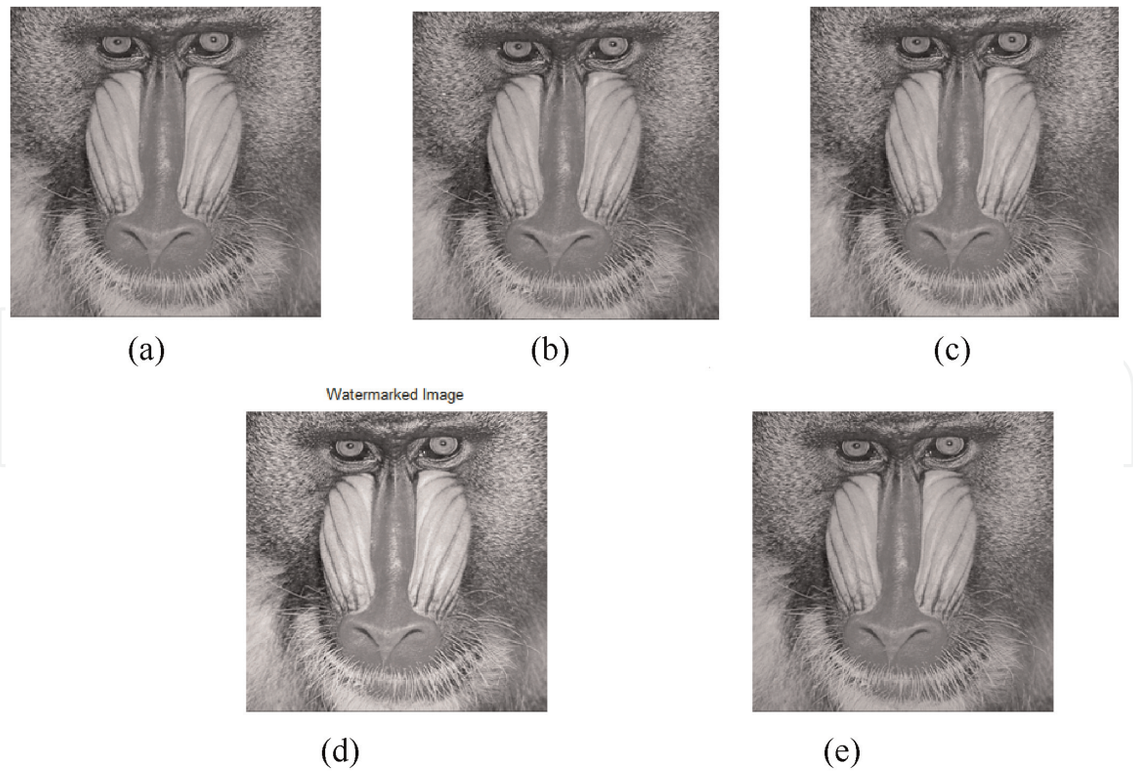

Figure 5.
(a) Original image. (b) Mandrill image marked using watermarking scheme of Dugad in the absence of attacks. (c) Hat image marked using watermarking scheme of Miyazaki in the absence of attacks. (d) Mandrill image marked using LSB. (e) Mandrill image marked using the proposed watermarking method in the absence of attacks.

For all the tests in this chapter, MATLAB is used. All tests are performed upon the 8-bit grayscale 256 × 256 Mandrill, Hat, and Lena images. To simulate the watermarking schemes on the Mandrill image, we set t1 = 115, t2 = 200, and k = 0.1. The suitable thresholds are obtained from the curves in **Figure 4b**. The watermarked images are then attacked with JPEG compression with different compression ratios to make the quality of the images at levels 5 (Q5), 10 (Q10), and 15 (Q15) at the JPEG standard. Other attacks such as the additive white Gaussian noise (AWGN) and cropping attacks are also considered. The same schemes are also applied to the Hat image with similar attacks. The thresholds used for this case are t1 = 90 and t2 = 200. We find from the figures that the suitable thresholds are coming from the curves in **Figure 4d**. To investigate the watermarking methods, we calculate the threshold (t) by using fmax= 528.4 and k = 0.1 so the threshold t = 0.1* fmax=52.84, we will use t1 = 90, t2 = 200 that give the tradeoff between PSNR and correlation as shown in **Figure 4**. The attacks were used to test the new algorithm, we choose the thresholds according to that gives the trade off between the high PSNR and the high Correlation ,in the case of mandrill we find that t1 = 115, t2 = 200, X1 = 20 and X2 = 10. **Figure 5** shows this Watermarked image and the effect of attacking this watermarked image with various attacks. The watermarked images are then attacked with JPEG at levels Q5, Q10, and Q15, AWGN, and cropping.

It can be seen that the watermarking algorithm of Dugad is surviving all the attacks. The high compression ratio using JPEG with quality 5 is one of the attacks applied to the watermarked image and resizing from 256 to 128 is the other attack, it is found that the watermark was not always detected. Results are shown in **Tables 1–3**.

Similar experiments and attacks are carried out for the algorithm in Miyazaki method with t1 = 115 and t2 = 200; we find that the results are better than that of Dugad method because it is a semi-blind method. Results are shown in **Tables 1** and **3**.

Scheme	PSNR	NC
LSB blind	49.9	1
Dugad's blind	42.48	0.57
Miyazaki's non-blind	44.65	1
Proposed scheme blind	46.60	1

Using $t_1 = 115$, $t_2 = 200$, and $k = 0.1$.

Table 1.
Comparing the proposed method with the other three methods of Dugad, Miyazaki, and LSB (Mandrill image).

Types of attacks	NC	WM length in	WM length out
No attacks	1	102	102
JPEG Q5	0.14	102	53
JPEG Q10	0.48	102	77
JPEG Q15	0.85	102	79
Gaussian (0.006)	0.54	102	54
Salt and pepper (0.15)	0.79	102	79
Cropping	0.48	102	38
Half sizing	0.39	102	48

Table 2.
Comparing NC value for the proposed method with the methods of Dugad, Miyazaki, and LSB.

	NC			
Type of attacks	**Blind LSB**	**Blind scheme of Dugad**	**Non-Blind scheme of Miyazaki**	**Blind proposed method**
JPEG Q5	0.0111	0.57	0.75	0.14
JPEG Q10	0.01	0.24	1	0.48
JPEG Q50	0.0193	0.22	1	0.85
Gaussian 0.006	0.0052	0.52	1	0.57
Gaussian 0.01	0.011	0.19	0.93	0.4
Gaussian 0.1	0.0134	0.01	0.49	0.06
Salt and pepper 0.015	0.0030	0.53	0.87	0.45
Salt and pepper 0.15	0.0017	0.037	0.55	0.36
Salt and pepper 0.5	0.0027	0.001	−0.01	0.29
Cropping	−0.0054	0.58	0.95	0.39
Half sizing	0.4245	0.17	0.77	0.49
Subsample 0.7	0.5608	0.25	0.49	0.223
Subsample 0.4	0.3098	0.16	0.71	0.2

Table 3.
Results for the proposed scheme (Mandrill image) (with $t_1 = 115$, $t_2 = 200$, $X_1 = 20$, and $X_2 = 10$).

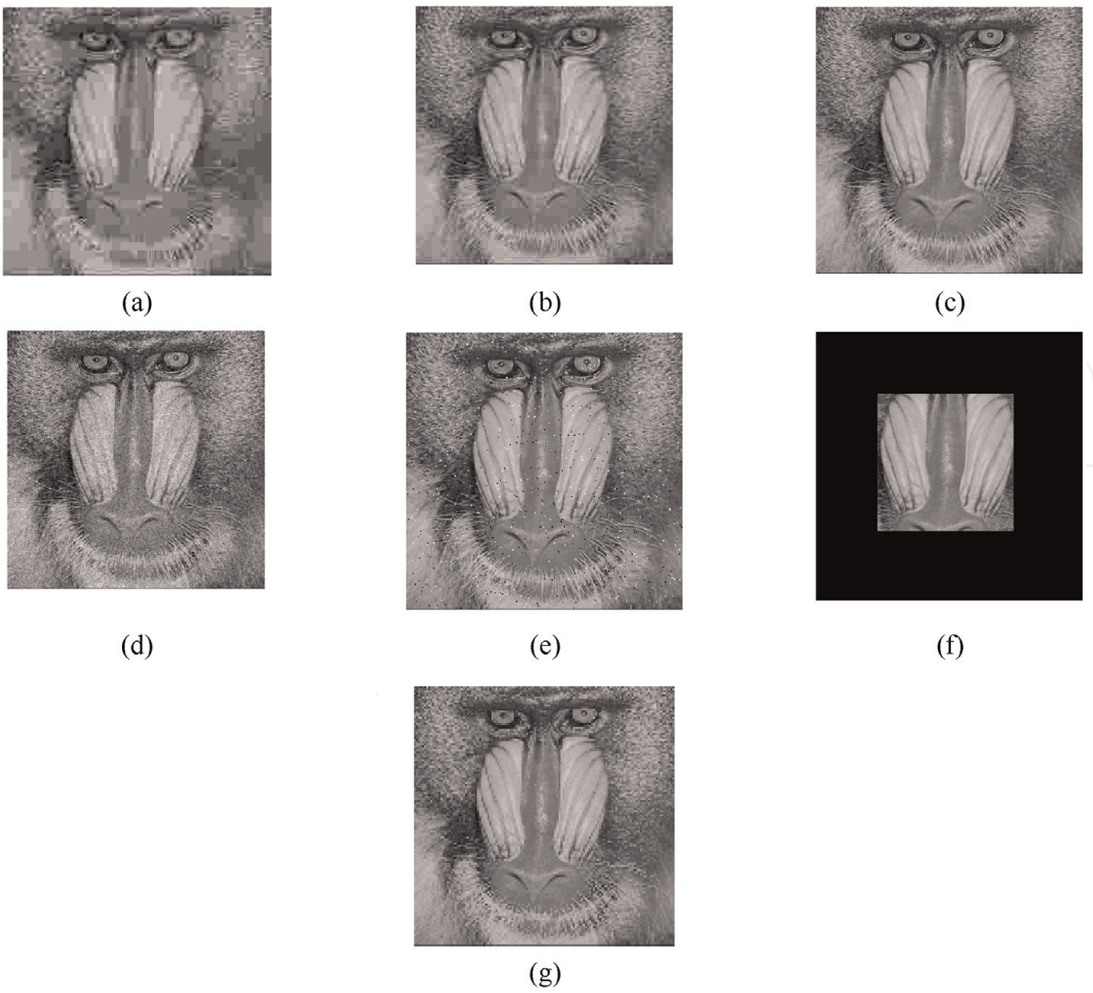

Figure 6.
Attacked image with (a) JPEG quality 5, (b) JPEG quality 10, (c) JPEG quality 15, (d) Gaussian noise (variance = 0.0058), (e) impulse noise (normalized density of 0.015), (f) cropping, and (g) half sizing (followed by resizing back to the original size).

The same attacks were used to test the new algorithm; The thresholds are chosen carefully to achieve tradeoff between the high PSNR and the high Correlation. In the case of Mandrill, we found that t1 = 115, t2 = 200, X1 = 20, and X2 = 10. **Figure 6** shows this watermarked image and the effect of attacking this watermarked image with various attacks. **Table 3** presents the quantitative results for these various attacks.

However, the "cropping" attack poses a problem in that only 38 out of a possible 102 watermark bits were used by the detector, thus decreasing the reliability of the scheme. The scheme is not robust to JPEG quality 5 attack (just like the Dugad method). Thus, while surviving the same attacks as the Dugad scheme, the new scheme does not degrade the watermarked image to the same extent. From **Table 1**, PSNR value is 42.48 dB. The PSNR recorded for the Miyazaki scheme is equal to 44.65dB, the recorded PSNR for LSB is (49.9dB) and PSNR recorded for the new scheme is (46.60dB).

Similar experiments and attacks are carried out for the algorithm in Miyazaki method, Dugad method, LSB method, and the proposed method on Hat image and Lena image, and the results are shown in **Figures 7–10**.

Table 4 presents the PSNR and NC for the proposed method and the other two methods using Hat image. It is seen that our method does not degrade the watermarked image to the same extent as the other two methods. **Table 5** represents the NC for the attacked watermarked images in our proposed method and the other existing methods.

Figure 7.
(a) Original image. (b) Hat image marked using watermarking scheme of Dugad in the absence of attacks. (c) Hat image marked using watermarking scheme of Miyazaki in the absence of attacks. (d) Hat image marked using LSB scheme. (e) Hat image marked using the proposed watermarking method in the absence of attacks.

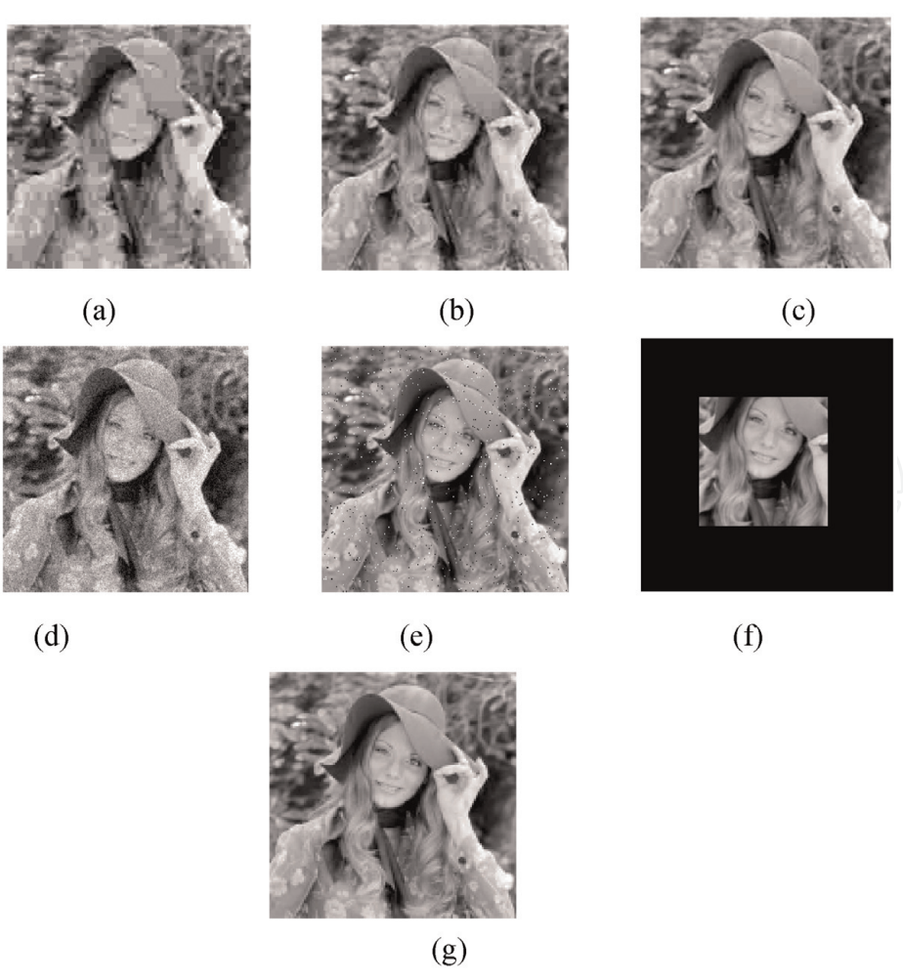

Figure 8.
Attacked image with (a) JPEG quality 5, (b) JPEG quality 10, (c) JPEG quality 15, (d) Gaussian noise (variance = 0.0058), (e) impulse noise (normalized density of 0.015), (f) cropping, and (g) half sizing (followed by resizing back to the original size).

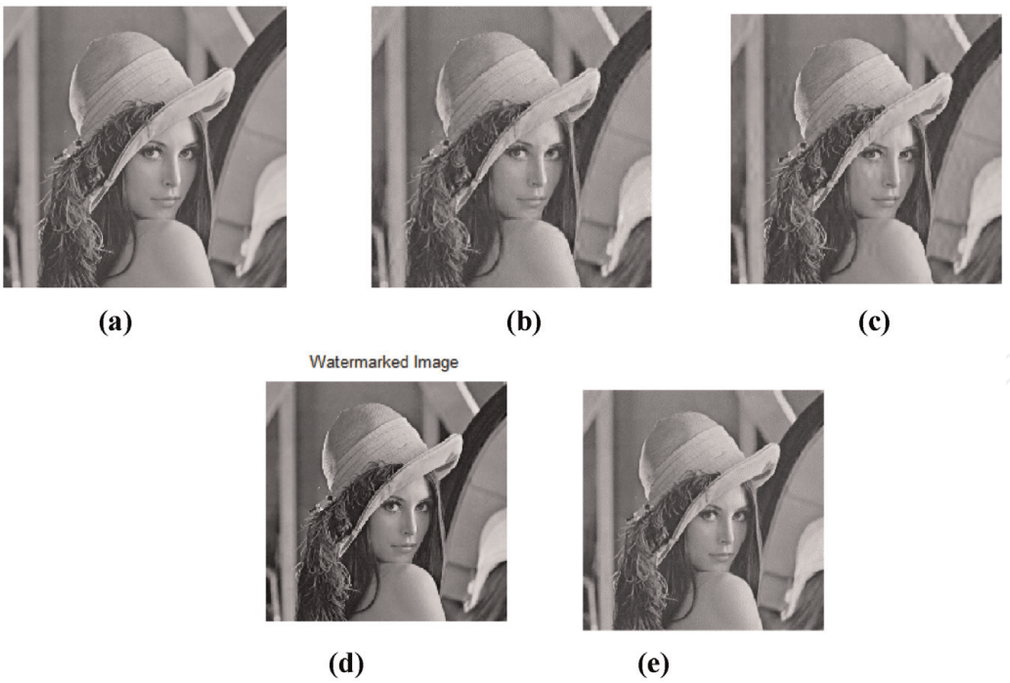

Figure 9.
(a) Original image. (b) Lena image marked using watermarking scheme of Dugad in the absence of attacks. (c) Lena image marked using watermarking scheme of Miyazaki in the absence of attacks. (d) Lena image marked using LSB scheme. (e) Lena image marked using the proposed watermarking method in the absence of attacks.

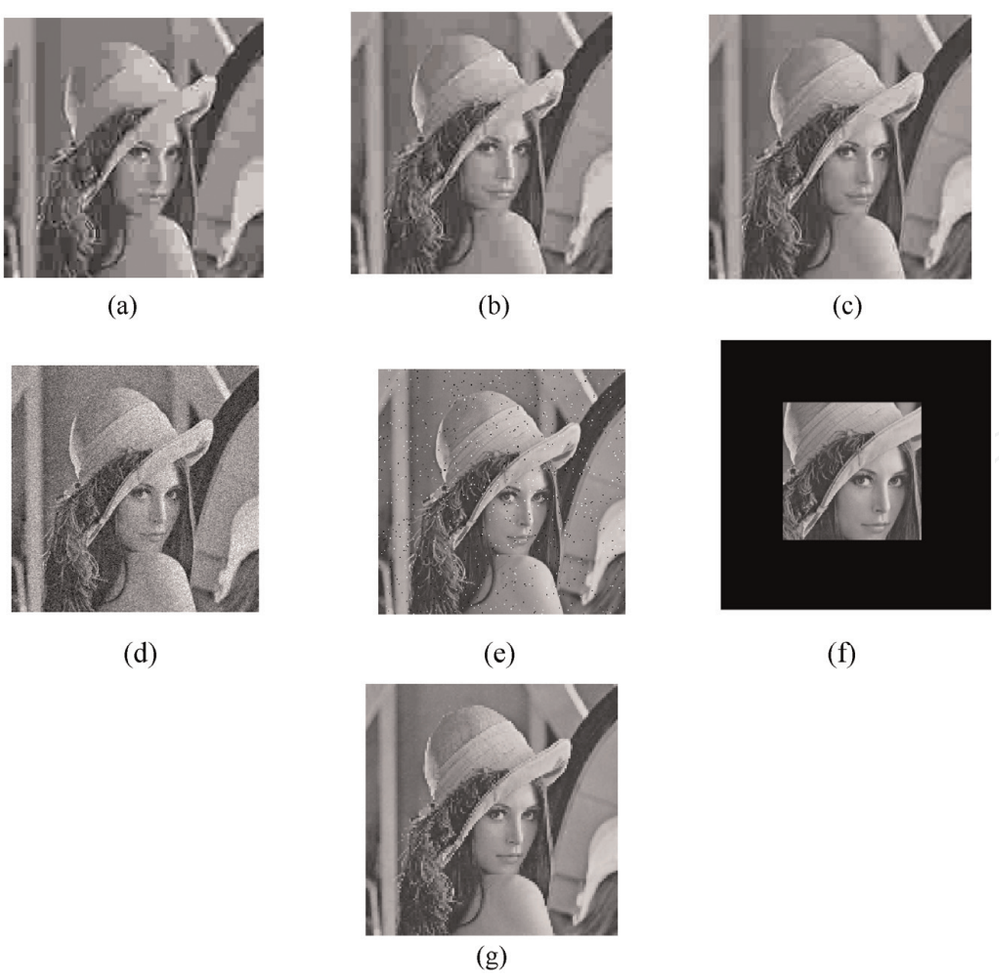

Figure 10.
Attacked image with (a) JPEG quality 5, (b) JPEG quality 10, (c) JPEG quality 15, (d) Gaussian noise (variance = 0.0058), (e) impulse noise (normalized density of 0.015), (f) cropping, and (g) half sizing (followed by resizing back to the original size).

Scheme	PSNR	NC
LSB scheme blind	51	1
Dugad scheme blind	40.09	0.45
Miyazaki scheme non-blind	44.62	1
Proposed scheme blind	45.36	1

Using $t_1 = 90$, $t_2 = 200$, and $k = 0.1$.

Table 4.
Comparing the proposed method with the other two techs of Dugad, Miyazaki, and LSB (hat image).

NC				
Type of attacks	**Blind LSB scheme**	**Blind scheme in Dugad**	**Non-blind scheme of Miyazaki**	**Blind proposed method**
JPEG Q5	−0.0015	0.27	0.44	0.28
JPEG Q10	−0.0038	0.38	0.66	0.46
JPEG Q50	0.0015	0.45	1	0.88
Gaussian 0.006	0.0019	0.28	1	0.67
Gaussian 0.01	0.001	0.189	0.99	0.57
Gaussian 0.1	−8.1606e-007	0.01	0.46	0.05
Salt and pepper 0.015	−7.5838e-004	0.42	0.79	0.45
Salt and pepper 0.15	−0.0053	0.024	0.54	0.12
Salt and pepper 0.5	−0.0012	0.003	0.14	0.03
Cropping	−1.5895e-005	0.20	0.32	0.39
Half sizing	−0.0012	0.25	0.96	0.49
Subsample 0.7	−9.3287e-004	0.31	0.97	0.76
Subsample 0.4	−9.2566e-005	0.26	0.85	0.47

Table 5.
Comparing NC value for the proposed method with the methods of Dugad, Miyazaki, and LSB using hat image.

	NC	WM length in	WM length out
No attacks	1	367	367
JPEG Q5	0.14	367	203
JPEG Q10	0.48	367	271
JPEG Q15	0.85	367	319
Gaussian (0.006)	0.54	367	250
Salt and pepper (0.015)	0.79	367	293
Cropping	0.48	367	78
Half sizing	0.39	367	222

Table 6.
Results for the proposed scheme (hat image) with $t_1 = 90$, $t_2 = 200$, $X_1 = 20$ and $X_2 = 10$.

Scheme	PSNR	NC
LSB scheme blind	50.86	1
Dugad scheme blind	37.42	0.36
Miyazaki scheme non-blind	39.27	1
Proposed scheme blind	45.29	1

Using $t_1 = 120$, $t_2 = 200$, and $k = 0.1$.

Table 7.
Comparing the proposed method with the other two methods of Dugad, Miyazaki, and LSB (Lena image).

NC				
Type of attacks	**Blind LSB scheme**	**Blind scheme of Dugad**	**Non-blind scheme of Miyazaki**	**Blind proposed method**
JPEG Q5	−0.0083	0.15	0.5	0.14
JPEG Q10	−0.0024	0.19	0.88	0.39
JPEG Q50	−0.0014	0.24	0.98	0.83
Gaussian 0.006	0.0038	0.24	0.9	0.32
Gaussian 0.01	0.0013	0.16	0.76	0.25
Gaussian 0.1	4.5235e-004	0.007	0.28	0.04
Salt and pepper 0.015	0.0016	0.18	0.96	0.6
Salt and pepper 0.15	8.2995e-004	0.03	0.35	0.53
Salt and pepper 0.5	5.2785e-004	0.005	0.059	0.47
Cropping	−0.0054	0.18	0.96	0.62
Half sizing	0.42	0.18	0.76	0.49
Subsample 0.7	0.56	0.25	0.83	0.67
Subsample 0.4	0.31	0.18	0.7	0.36

Table 8.
Comparing NC value for the proposed method with the methods of Dugad, Miyazaki, and LSB scheme using Lena image.

	NC	WM length in	WM length out
No attacks	1	129	129
JPEG Q5	0.14	129	57
JPEG Q10	0.39	129	74
JPEG Q15	0.83	129	102
Gaussian 0.006	0.32	129	66
Salt and pepper 0.015	0.6	129	41
Cropping	0.62	129	85

Table 9.
Results for the proposed scheme (Lena image) (with $t_1 = 120$, $t_2 = 200$, $X_1 = 20$ and $X_2 = 10$).

However in **Table 6**, the "cropping" attack poses a problem in that only 78 out of a possible 367 watermark bits were used by the detector, thus decreasing the reliability of the scheme. The scheme is not robust to JPEG quality 5 attacks. Thus, while surviving the same attacks as the Dugad scheme, the new scheme does not degrade the watermarked image to the same extent. From **Table 4**, PSNR value is 45.36 dB.

Table 7 presents the PSNR and NC for the proposed method and the other two methods using Lena image. It is seen that our method does not degrade the watermarked image to the same extent as the other two methods. **Table 8** represents the NC for the attacked watermarked images in our proposed method and the other existing methods.

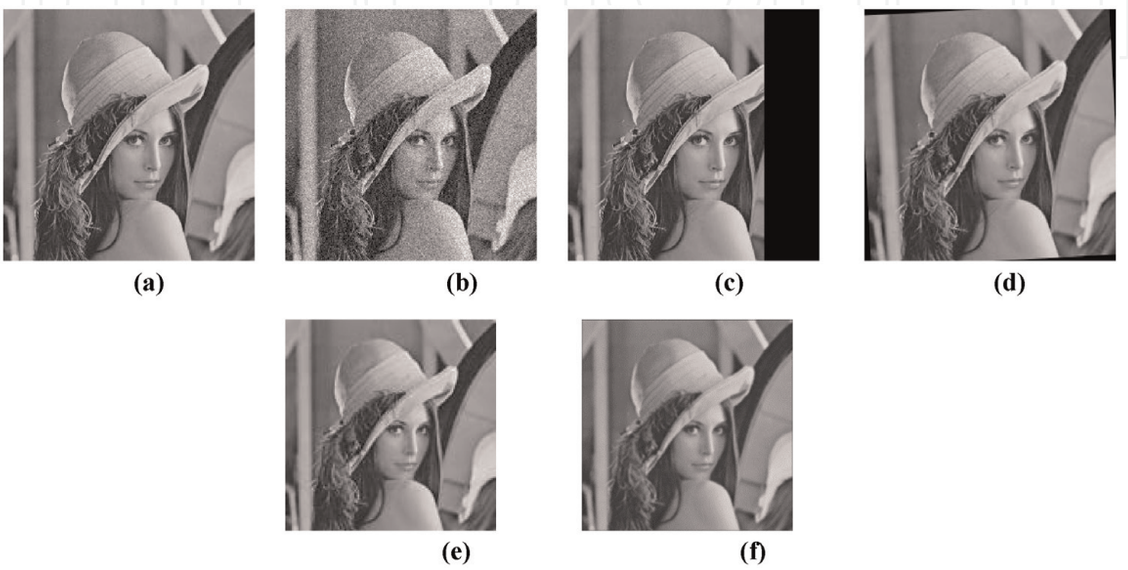

Figure 11.
Watermarked image using HEAD method with DWT with and without attacks for Lena image. (a) Watermarked image PSNR = 51.7 dB without attacks. (b) Attacked image with Gaussian noise with variance = 0.006. (c) Cropped image. (d) Rotated image with 3°. (e) Resized image from 256 to 128–256. (f) Blurred image with 3 × 3 LPF.

Figure 12.
Watermarked image using the HEAD-based DWT method with and without attacks for hat image. (a) Watermarked image PSNR = 49.4 dB without attacks. (b) Attacked image with Gaussian noise with variance = 0.006. (c) Cropped image. (d) Rotated image with 3°. (e) Resized image from 256 to 128–256. (f) Blurred image with 3 × 3 LPF.

	Proposed HEAD watermarking method for Lena image, t1 = 182 and t2 = 268	Proposed HEAD watermarking method for Hat image, t1 = 236 and t2 = 333
No attacks	1	1
Gaussian 0.006	0.75	0.85
Gaussian 0.01	0.55	0.53
Gaussian 0.1	0.14	0.16
Cropping	1	1
Rotation	0.3	0.076
Blurring	0.6	0.43
Resizing 0.5	0.42	0.5

Table 10.
Correlation values for our scheme of Lena and hat images.

However in **Table 9**, the "salt-and-pepper noise" attack poses a problem in that only 41 out of a possible 129 watermark bits were used by the detector, thus decreasing the reliability of the scheme.

8.1 Simulation results of HEAD quantization method

We simulate the watermarking schemes on Lena and Hat images. Results are shown in **Figures 11** and **12**, respectively. The numerical evaluation metrics for all schemes in the absence and presence of attacks are tabulated in **Table 10**. From the table we notice that the proposed watermarking scheme achieves the lowest distortion in the watermarked image in the absence of attacks, and we find that the proposed method using wavelet gives the image with fidelity better than the other existing methods and the table gives the correlation under the presence of attacks; we notice also that a percentage of around 50% of the input watermark bits can be extracted in the proposed scheme with most of the attacks.

We find that we can detect watermark at the presence of blurring, Gaussian noise, cropping, and resizing attack; in the case of rotation attack, detection of watermark is difficult.

9. Conclusions

With this proposed method, blindness, detectability, robustness against attacks, and high watermarked image quality is maintained. Although the robustness of this new scheme is not quite as strong as that presented by Miyazaki method, this can be attributed to its blind nature compared to the semi-blind nature of the Miyazaki method. In LSB method, the attacks like addition of noise with any value or compression of the image using JPEG destroy the embedded watermark, and we cannot detect or extract the watermark at all, although the watermark was recovered perfectly in the ideal case.

Also the watermark may be removed without any effect done on the watermarked image. A blind DWT-based image watermarking schemes depend on

the HEAD quantization of coefficients to embed meaningful information in the image. Experimental results have shown the superiority of the proposed schemes from the host image quality point of view, robustness, and the blindness point of view.

Author details

Abeer D. Algarni[1] and Hanaa A. Abdallah[1,2]*

1 Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, KSA

2 Electronics and Communications Department, Faculty of Engineering, Zagazig University, Egypt

*Address all correspondence to: haabdullah@pnu.edu.sa

References

[1] Zhu W, Xiong Z, Zhang Y. Multiresolution watermarking for images and video. IEEE Transactions on Circuits and Systems for Video Technology. 1999;**9**(4):545-550

[2] Xia XG, Boncelet CG, Arce GR. A multiresolution watermark for digital images. In: Proceedings of the IEEE International Conference on Image Processing (ICIP 1997); Vol. 1; October 1997. pp. 548-551

[3] Dugad K, Ratakonda R, Ahuja N. A new wavelet-based scheme for watermarking images. In: Proceedings of International Conference on Image Processing (ICIP 1998); Vol. 2; Chicago, IL; October 4–7, 1998. pp. 419-423

[4] Tao P, Eskicioglu AM. A robust multiple watermarking scheme in the DWT domain. In: Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference; Philadelphia, PA; October 25–28, 2004. pp. 133-144

[5] Cox IJ, Miller ML, Bloom JA. Watermarking applications and their properties. In: Proceedings of the IEEE International Conference on Information Technology: Coding and Computing; 2000. pp. 6-10

[6] Tsai MJ, Yu KY, Chen YZ. Joint wavelet and spatial transformation for digital watermarking. IEEE Transactions on Consumer Electronics. 2000;**46**(1): 241-245

[7] Barni M, Bartolini F, Cappellini V, Piva A. A DCT-domain system for robust image watermarking. Signal Processing. Special Issue on Copyright Protection and Control. 1998;**66**(3): 357-372

[8] Potdar VM, Chang E. A Quantization Based Robust Image Watermarking Algorithm in Wavelet Domain. Perth, Western Australia: School of Information Systems, Curtin University of Technology. ICT_2005

[9] Miyazaki A, Yamamoto A, Katsura T. A digital watermarking technique based on the wavelet transform and its robustness on image compression and transformation. IEICE Transactions. Special Section on Cryptography and Information Security. 1999;**82**(1):2-10

[10] Zolghadrasli A, Rezazadeh S. Evaluation of spread spectrum watermarking schemes in the wavelet domain using HVS characteristics. The International Journal of Information Science and Technology. 2007;**5**(2): 123-139

[11] El-said SA, Hussein KFA, Fouad MM. Adaptive lossy image compression technique. In: Electrical and Computer Systems Engineering Conference (ECSE'10); 2010