

A robust embedding and blind extraction of image watermarking based on discrete wavelet transform

E. Najafi¹

Received: 11 December 2016 / Accepted: 29 July 2017 / Published online: 14 August 2017
© The Author(s) 2017

Abstract In this study, a new algorithm that can be used for copyright protection is proposed for the embedding and detection of a watermark in the domain of discrete wavelet transform (DWT). The elements of the logo watermark are embedded directly to the three-level DWT decomposed subbands. In addition to that, the scheme is considered as a completely blind scheme for both host image and watermark. Two kinds of security attacks have also been considered which confirms the security of the scheme. The experimental results and computer simulation of the proposed scheme have shown that the proposed approach has the desired properties such as invisibility, blind detection, and robustness against various geometrical and non-geometrical attacks.

Keywords Wavelet transform · Image processing · Image watermarking · Signal detection and filtering

Mathematics Subject Classification 45J05 · 65L60

Introduction

With the fast growth of the Internet, people have paid more and more attention to the security of the network information. The protection of the digital data is an important topic to the owners of the multimedia products. Digital watermarking is embedding hidden data into the

multimedia in such a manner that it cannot be removed and its detection to verify the ownership of digital products.

To be used as a means of copyright protection, the two main requirements of high robustness and capacity and high imperceptibility (low visibility) should be ensured for watermarking schemes. The peak signal-to-noise ratio (PSNR) is criteria that are used to evaluate imperceptibility. There exists a reverse relation between capacity, robustness, and imperceptibility and making a developed compromise between these conflict parameters is the core motivation of the most watermarking schemes.

The watermarking procedure in which the techniques first transform an image into a set of frequency-domain coefficients is frequency-domain techniques [1]. These techniques include discrete cosine transform (DCT) [2, 3], discrete Fourier transform (DFT) [4], radon transform [5], discrete wavelet transform (DWT) [6–9], etc. In these techniques, the watermark is embedded in the transform coefficients of the image. Then, the coefficients are inverse-transformed to form the watermarked image. In this way, the watermark is less visible and more robust to some image-processing operations and attacks. Extraction process of watermark may be dependent or independent of the original image or embedded watermark, which is based on level of required information that are classified into non-blind, semi-blind, or blind detection process. These classes are application-dependent and directly affect on the capacity of the watermarking scheme.

Most of the algorithms of watermarking schemes which are proposed have this common disadvantage that in the extracting process, they require a lot of information of host image and/or embedded watermark and this process is dependent on some information of host image or watermark. It is clear that in some situations and applications, it may be impossible to access to these information. On the

✉ E. Najafi
e.najafi@urmia.ac.ir

¹ Department of Mathematics, Faculty of Science, Urmia University, Urmia, Iran

other hand, each watermark has own data, and if too many watermarks are used, then too many available data are needed to be stored and utilized when they are required. Obviously, these drawbacks make serious restrictions for application of these methods.

In [8, 9], the authors use SVD (singular value decomposition) of subbands of one-level redundant wavelet and integer wavelet decomposition and add the singular values of the watermark to the singular values of the subbands. However, in the detection process, the presented methods require the orthogonal matrices of SVD of the watermark as well as the singular values of the subbands. In Lai et al. [6], the authors decomposed the host image into four subbands (LL, LH, HL, and HH) using DWT and then applied SVD to only the LH and HL subbands. Finally, the watermark image was divided into two halves and then embedded into the singular values of LH and HL, respectively. Again, there is necessity of the orthogonal matrices and singular values of the subbands in the extraction process. Other works such as [10–13] suffer from the same problem.

Although apparently, these algorithms declare high capacity and blind detection, but in fact, only the singular values of the watermark are embedded in the host image and a large percentage of the data of the watermark are stored in an available place apart from the host image. On the other hand, the detection process can not be blind because of dependency to a lot of data of the host image and watermark.

The work which is done in this study is to present an algorithm that does not have the above-mentioned difficulties and also preserves the desired properties of a watermarking procedure. The watermark, which is embedded, is a binary string derived from a logo watermark. The whole of the watermark is embedded in the host image and no additional data of watermark or host image are remained to be preserved beside the algorithm. Using discrete wavelet transform, the watermark is embedded in all detail subbands of three-level decomposition of the image. The extracting procedure is not dependent on any part of the host image or the watermark, and then, the process is fully blind. The algorithm showed good imperceptibility, capacity, and security, and with having high robustness, the proposed scheme is an ideal choice for copyright protection applications.

The remainder of this paper is organized as follows: “Discrete wavelet transformation of images” presents a brief overview regarding the transform applied in the proposed scheme. In the next section, the proposed scheme (i.e., the watermark embedding and extraction procedures) is stated. The experimental setup and results are presented in “Experimental results”. Finally, our conclusions are stated in the last section.

Discrete wavelet transformation of images

In this section, a brief overview of application of DWT for image decomposition is presented. A function (signal) $f(x)$ using discrete wavelet transform can be decomposed into a weighted sum of basis functions $\phi_{j_0,k}(x)$ and $\psi_{j,k}(x)$ (scaling and wavelets functions):

$$f(x) = \frac{1}{\sqrt{M}} \sum_k W_\phi(j_0, k) \phi_{j_0,k}(x) + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{\infty} \sum_k W_\psi(j, k) \psi_{j,k}(x), \quad j, k \in \mathbb{Z}, \quad (2.1)$$

where j_0 is starting scale, M is the length of the signal, $W_\phi(j_0, k)$, and $W_\psi(j, k)$ are approximation and details coefficients, respectively.

In two-dimensional signals (like an image), wavelets and scaling functions are tensor products of the one dimension:

$$\begin{aligned} \phi(x, y) &= \phi(x)\phi(y), & \psi^H(x, y) &= \psi(x)\phi(y), \\ \psi^V(x, y) &= \phi(x)\psi(y), & \psi^D(x, y) &= \psi(x)\psi(y), \end{aligned}$$

and the decomposition of signal $f(x, y)$ of size $M \times N$ will be as

$$\begin{aligned} f(x, y) &= \frac{1}{\sqrt{MN}} \sum_m \sum_n W_\phi(j_0, m, n) \phi_{j_0,m,n}(x, y) \\ &+ \frac{1}{\sqrt{MN}} \sum_{i=H,V,D} \sum_{j=j_0}^{\infty} \sum_m \sum_n W_\psi^i(j, m, n) \psi_{j,m,n}^i(x, y), \end{aligned}$$

for $j, m, n \in \mathbb{Z}$. With this decomposition, the 2D signal is filtered by the filter coefficients h_ϕ (low-pass filter) and h_ψ (high-pass filter) that have two directions X and Y along with a downsampling in each direction to produce the coefficients of the four subbands $W_\phi(j, \cdot, \cdot)$, $W_\psi^H(j, \cdot, \cdot)$, $W_\psi^V(j, \cdot, \cdot)$, and $W_\psi^D(j, \cdot, \cdot)$, where $W_\phi(j+1, \cdot, \cdot)$ is the coefficients of the input image. This procedure is one-level analysis filter bank and an image is divided into four subbands LL, LH, HL, and HH. LH (low–high) is generated by the approximation coefficients (low-pass filter) in X direction and details coefficients (high-pass filter) in Y direction (see Fig. 1).

The inverse discrete wavelet transform is easy and can be accomplished by the upsampling and filtering by the inverse low-pass and high-pass filters and exchanging the split by merging. After decomposition of the image, the details and approximation coefficients are used by inverse DWT to recompose the original image. This process is synthesis filter bank and the filter coefficients (low-pass and high-pass filters) are chosen, such that the reconstruction is perfect [14–16]. Figure 2 illustrates the discrete wavelet and inverse discrete wavelet transforms steps. The basic approach of

Fig. 1 Image decomposition with DWT: subbands of three-level decomposition

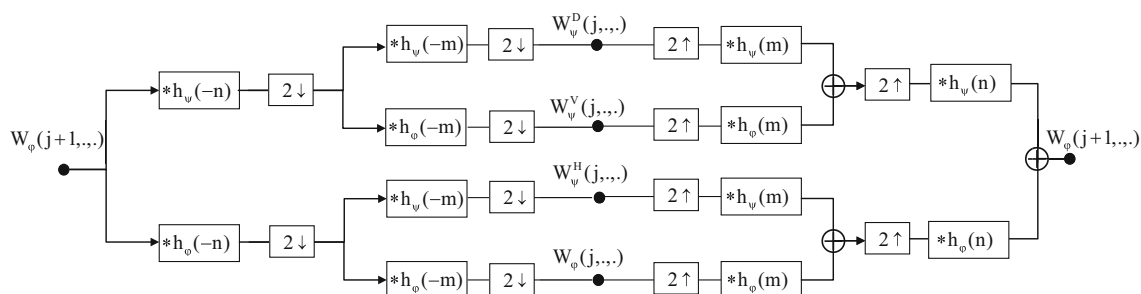
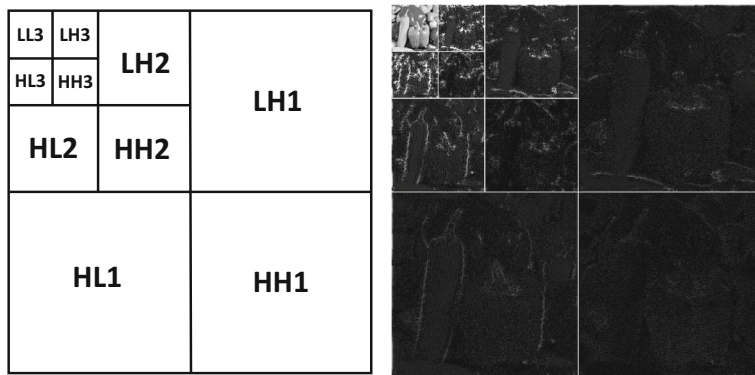


Fig. 2 Image decomposition with DWT: one-level analysis and synthesis filter bank

wavelets in many applications and their usefulness in image processing is demonstrated in three steps: computing a 2D DWT of an image, altering the coefficients of the transform, and finally computing the inverse transform to reconstruct the modified image. DWT properties can be utilized to enhance the robustness and preserve the imperceptibility in the watermarking. Accordingly, this technique is adopted by the scheme proposed in this paper.

detection procedures steps are listed in Algorithms 1 and 2, respectively. The watermark $w = \{w_1, w_2, \dots, w_k\}$, which will be embedded, is a binary string with values $w_j = 0, 1$ for $j = 1, \dots, k$ derived by listing the rows of a logo watermark. In addition, we name $W_\psi^i(j, m, n) = Y_i(m, n)$ the components of the subband $i \in \{LH, HL, HH\}$.

The proposed scheme

The proposed scheme is presented in this section. This scheme includes watermark embedding and extracting processes, as shown in Figs. 3 and 4. The embedding and

The watermark embedding procedure

The human eye is able to detect modifications to the lower frequencies. Therefore, it is better to embed a watermark into an image by modifying large detail coefficients of its multiresolution representation [19, 20]. Detail coefficients belong to the edges and borders of the images, where the

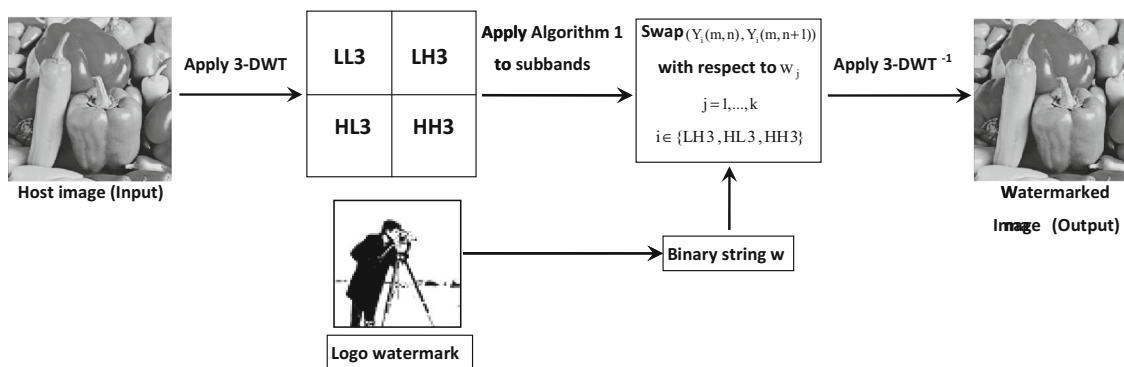


Fig. 3 Watermark embedding process

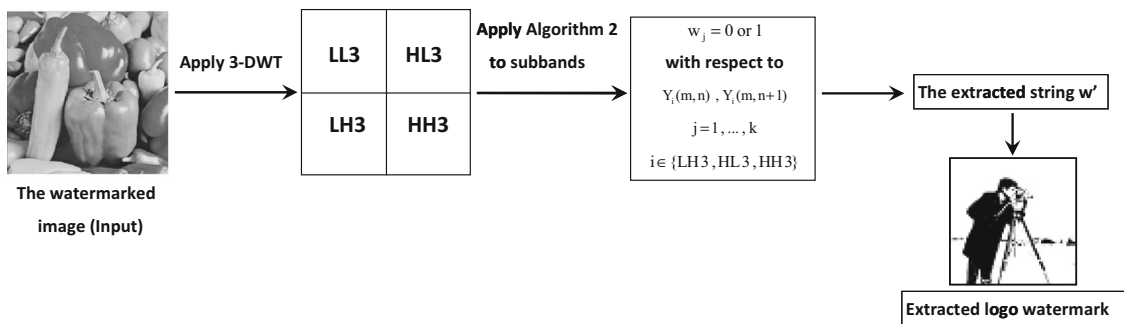


Fig. 4 Watermark detection process

frequency is high and embedding of the watermark in these locations is robust against human visual system.

The original image is decomposed into three levels. The subbands LH3, HL3, and HH3 in three levels are selected for the embedding of the watermark, since these subbands involve a wide range of the frequency spectrum of the image, and then, the robustness of the watermarking scheme will be increased. As mentioned before, all components of the watermark are embedded and no extra data of the watermark remain to be preserved out of the host image. The steps of the embedding process are as follows:

The watermark extraction procedure

For the detection of the watermark, the inverse of the embedding operations is implemented. Along with the detection procedure, no information of host image or embedded watermark is required, and then, the extraction procedure is completely blind. The watermarked image A^{*w} may be distorted by geometrical and non-geometrical attacks (image-processing attacks). After decomposition of the watermarked image A^{*w} in the same level as embedding, Algorithm 2 on the subbands LH3, HL3, and HH3 will be implemented.

Algorithm 1: The watermark embedding process.

-
- Step 1:** Decompose the original image A using 3 levels DWT to subbands LL3, LH3, HL3 and HH3.
- Step 2:** List the rows of the logo watermark and derive binary string w , then embed it by the following scheme and obtain the new modified coefficients:
- For** $i \in \{LH3, HL3, HH3\}$ and $j = 1, \dots, k$ and all m, n **do**
- If** $w_j == 1$ & $Y_i(m, n) < Y_i(m, n + 1)$,
then $\text{swap}(Y_i(m, n), Y_i(m, n + 1))$.
- else If** $w_j == 0$ & $Y_i(m, n) > Y_i(m, n + 1)$,
then $\text{swap}(Y_i(m, n), Y_i(m, n + 1))$.
- Step 3:** The watermarked image is then obtained after applying the inverse DWT on the modified coefficients LH3, HL3 and HH3: $A^w = DWT^{-1}$.
-

Algorithm 2: The watermark detection process.

-
- Step 1:** Decompose the watermarked image A^{*w} using 3 levels DWT and derive the subbands LL3, LH3, HL3 and HH3.
- Step 2:** Extract the binary string $\bar{w} = \{\bar{w}_1, \dots, \bar{w}_k\}$ by the following process:
- For** $i \in \{LH3, HL3, HH3\}$ and $j = 1, \dots, k$ and all m, n **do**
- If** $Y_i(m, n) < Y_i(m, n + 1)$, then $\bar{w}_j = 0$.
- else If** $Y_i(m, n) > Y_i(m, n + 1)$, then $\bar{w}_j = 1$.
- Step 3:** Construct logo watermark using derived binary string w .
-

Algorithm 2 of detection steps is independent of the original image and embedded watermark and this property makes the scheme more applicable in watermarking areas such as fingerprint and copy and copyright protections.

Experimental results

The proposed procedure simulation is implemented in MATLAB. Popular test images of size 512×512 have been used as host images and the Cameraman logo image is selected as a binary watermark. The examination of the efficiency of the proposed scheme under different conditions is considered in terms of imperceptibility and robustness under various attacks. To this end, we compute peak signal-to-noise ratio (PSNR) and normalized correlation coefficient (NCC) which are used repeatedly in the literature. The PSNR, which is used to estimate the imperceptibility, is criteria to evaluate the similarity between the host image x and the watermarked image y by the following relation:

$$PSNR = 10 \log_{10} \left(\frac{\text{Max}(x(i,j))^2}{MSE} \right), \tag{4.1}$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (x(i,j) - y(i,j))^2,$$

where M, N are the size of the image and MSE is the mean square error between the two images. A high PSNR implies good imperceptibility of the watermarked image and its high similarity to the original image, and then, the host image is very slightly affected by the embedding process. The least acceptable value for PSNR is about 38 dB [17].

The similarity between the original watermark w and the extracted watermark \bar{w} is evaluated by the NCC which is criteria for the robustness of the scheme and is calculated as follows:

$$NCC = \frac{\sum_{j=1}^k w_j \bar{w}_j}{\sqrt{\sum_{j=1}^k w_j \sum_{j=1}^k \bar{w}_j}}. \tag{4.2}$$

The NCC has a value between 0 and 1. If this value is closer to 1 under a special attack, then the process has higher robustness against the attack and vice versa. An acceptable value for the NCC is at least 0.75 [18].

The imperceptibility test of the proposed scheme

The imperceptibility of the test images with various sizes of the logo watermark is examined. Obviously, there is a reverse relation between the size of the watermark (the capacity of the watermarking scheme) and PSNR; hence, an optimal size of the watermark must be selected, such

that an acceptable imperceptibility of the watermarked image to be obtained. These results are observed in Fig. 5.

According to these results and to the acceptable value of PSNR, 64×64 is selected as the size of the watermark. Table 1 displays some of the host and watermarked images in which the size of the embedded watermark is 64×64 . The figure shows the efficiency of the proposed scheme in terms of the imperceptibility and invisibility of the embedded watermark.

The robustness test of the proposed scheme

Robustness is the resistance of the embedded watermark against distortions of the watermarked image. These criteria are an important necessity in developing the watermarking algorithms. The distortions may be geometrical or non-geometrical attacks. Tables 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 represent the NCC values of the detected watermark of the proposed scheme when it is impressed by the various attack types. Geometrical attacks such as scaling, rotation, cutting, shearing, and translation were applied. Noise addition (salt and pepper, Gaussian, and speckle noise), filtering, gamma correction, and jpeg compression attacks were selected as non-geometrical attacks (image-processing attacks). The proposed scheme showed good resistance under all attacks with high NCC values, which are shown in Table 2.

First considered that geometrical attack is scaling attack. The scaling is changing the image size and then resizing it to the original one. This attack is considered in Table 3 and the watermarked image is tested under various scaling attacks with different scaling parameters. The NCC values of the table show good resistance of the scheme against this

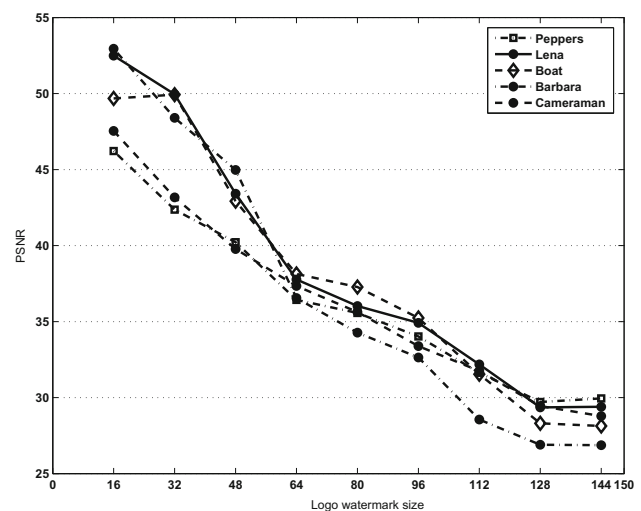




Fig. 5 Imperceptibility values using PSNR (dB) with various watermark sizes for test images of the proposed scheme

Table 1 Original and watermarked images with logo watermark of size 64×64

Original image	Watermark	Watermarked image
		
		
		
		
		

attack. Rotation attack is rotating the watermarked image to a particular angle and then rotating back to the original angle. The watermarked image is considered under various rotation angles and the NCC values in Table 4 shows how the scheme is robust under this attack. Cutting attack also is

applied to the watermarked image with different parameters to show the robustness of the procedure and the results of NCC values are presented in Table 5 verifying resistance of the scheme against this kind of attacks. Finally, shearing and translation attacks are used on the proposed scheme.

Table 2 Pepper watermarked image and the NCC of the extracted watermark under different attacks


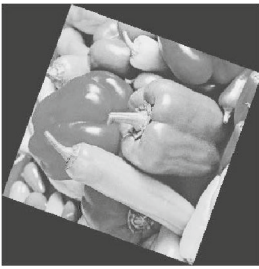


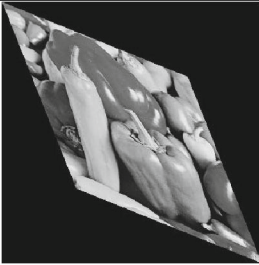



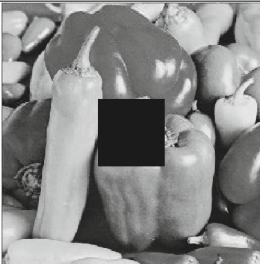
Attack	Scaling (2, 0.5)	Rotation 70°	Jpeg compression Q=40
Water-marked image			
NCC	0.9845	0.9338	0.9554
Attack	Median filter 5 × 5	Shearing (0.4, 0.4)	Cutting (40, 40)
Water-marked image			
NCC	0.9542	0.9645	0.9019
Attack	Gamma correction $\gamma = 0.2$	Translation (50, 40)	Centered cropping 120 × 120
Water-marked image			
NCC	0.9101	0.9515	0.9508

Table 3 Scaling attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Scaling (0.5, 2)	0.9817	0.9814	0.9799	0.9814	0.9797
Scaling (0.25, 4)	0.9103	0.9088	0.9183	0.9133	0.9147
Scaling (0.125, 8)	0.8553	0.8531	0.8708	0.8564	0.8653
Scaling (2, 0.5)	0.9845	0.9871	0.9900	0.9854	0.9862
Scaling (4, 0.25)	0.9483	0.9547	0.9585	0.9507	0.9524
Scaling (8, 0.125)	0.7483	0.7669	0.7920	0.7739	0.7882

Tables 6 and 7 show the NCC values of the attacks under different parameters, confirming the robustness of the scheme.

The second kind of attacks is non-geometrical attacks. Noise addition is considered as one of the image-processing attacks. Gaussian, salt and pepper, and speckle noises

Table 4 Rotation attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Rotation 2°	0.9336	0.9368	0.9413	0.9379	0.9206
Rotation 45°	0.9343	0.9382	0.9400	0.9369	0.9226
Rotation 70°	0.9338	0.9380	0.9408	0.9369	0.9198
Rotation 110°	0.9331	0.9380	0.9411	0.9369	0.9224
Rotation -50°	0.9293	0.9385	0.9368	0.9398	0.9248
Rotation -80°	0.9304	0.9377	0.9380	0.9398	0.9220

Table 5 Cutting attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Cutting (10, 10)	0.9245	0.9260	0.9276	0.9239	0.9042
Cutting (10, 20)	0.9416	0.9418	0.9491	0.9434	0.9287
Cutting (20, 30)	0.9355	0.9384	0.9452	0.9402	0.9244
Cutting (30, 40)	0.8971	0.8838	0.8933	0.8985	0.8779
Cutting (40, 40)	0.8934	0.8785	0.8872	0.8938	0.8726
Cutting (40, 50)	0.9139	0.9127	0.9216	0.9171	0.8965

are considered as noise addition attacks and added to the watermarked image. The NCC values are reported for different selections of variances and densities of noises. These NCC results exhibit good resistance of the scheme against this kind of attack and are shown in Tables 8, 9, and 10. The second type of non-geometrical attacks which are examined are filtering or de-noising attacks. Two classes of these types of attacks are employed for our scheme. Wiener and median filters with different filter block sizes (e.g., 3×3 , 5×5 , 7×7 , 9×9 , and 11×11) are employed and the related NCC values of the extracted watermarks are observed in Tables 11 and 12. These results show the high robustness of the procedure under filtering attacks. The compression of the images is a tool which is employed in many application areas of digital image processing. The watermarking technique must be

able to detect the watermark after compression of the watermarked image with a high NCC value. The Jpeg compression is the most important of the compression procedures of the images. To test the resistance of the process, in our experiments, the different compression rates 90, 80, 70, 50, 30, and 10 were selected to compress the watermarked image. The NCC values of the detected watermark are presented in Table 13 which show good robustness of the scheme against the compression attack. Gamma correction of the images is usually applied in some image-processing applications. We altered the watermarked image by gamma correction with several gamma values varying from 0.1 to 0.9 and then evaluated the NCC of the extracted watermark. High resistance of the scheme is proved against the gamma correction attack. Table 14 shows these NCC values for different gamma values.

The security test of the proposed scheme

In this section, we consider two kinds of security attacks which are discussed in [21] to show the security of the proposed scheme. These attacks are copy attack and ambiguity attack with blind detection and we show that our scheme is resistant against these two attacks, and then, it is a secure scheme.

Copy attack

A copy attack occurs when an adversary copies a watermark from a watermarked image to an arbitrary target image A^t to include it as a watermarked image [22]. Given a legitimately watermarked image, A^w , and an unwatermarked target image, A^t , this method begins by applying a watermark removal attack to A^w to obtain an approximation of the original image, \tilde{A} . For this step, the authors in [22] proposed using a noise-reduction filter. According to the weak robustness results, the median filtering is the best filter to eliminate the watermark and estimate the original image A . The next step is to estimate the added watermark

Table 6 Shearing attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Shearing (0.2, 0.2)	0.9807	0.9797	0.9797	0.9781	0.9677
Shearing (0.2, 0.5)	0.9670	0.9657	0.9683	0.9636	0.9531
Shearing (0.2, 0.7)	0.9518	0.9513	0.9533	0.9508	0.9374
Shearing (0.5, 0.2)	0.9602	0.9614	0.9584	0.9613	0.9466
Shearing (0.7, 0.2)	0.9393	0.9425	0.9395	0.9400	0.9271
Shearing (0.9, 0.2)	0.9185	0.9207	0.9207	0.9141	0.9015



Table 7 Translation attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Translation (10, 10)	0.9837	0.9785	0.9856	0.9824	0.9749
Translation (10, 20)	0.9777	0.9721	0.9795	0.9742	0.9669
Translation (20, 30)	0.9704	0.9597	0.9701	0.9664	0.9541
Translation (30, 40)	0.9626	0.9523	0.9622	0.9569	0.9445
Translation (20, 10)	0.9841	0.9798	0.9849	0.9833	0.9754
Translation (30, 20)	0.9777	0.9740	0.9787	0.9755	0.9677
Translation (40, 30)	0.9702	0.9602	0.9697	0.9666	0.9543

Table 8 Salt and pepper noise attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Salt and pepper noise 0.001	0.9670	0.9676	0.9774	0.9730	0.9425
Salt and pepper noise 0.005	0.9206	0.9227	0.9294	0.9292	0.8923
Salt and pepper noise 0.01	0.9021	0.8913	0.9117	0.9089	0.8635
Salt and pepper noise 0.05	0.8291	0.8247	0.8316	0.8361	0.8023
Salt and pepper noise 0.1	0.7948	0.7890	0.7965	0.7989	0.7670

Table 9 Gaussian noise attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Gaussian noise 0.001	0.9336	0.9188	0.9329	0.9398	0.8901
Gaussian noise 0.005	0.8816	0.8756	0.8849	0.8874	0.8436
Gaussian noise 0.01	0.8441	0.8383	0.8561	0.8517	0.8091
Gaussian noise 0.05	0.7681	0.7756	0.7865	0.7752	0.7534
Gaussian noise 0.1	0.7387	0.7350	0.7447	0.7458	0.7235

Table 10 Speckle noise attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Speckle noise 0.001	0.9634	0.9560	0.9641	0.9674	0.9307
Speckle noise 0.005	0.9277	0.9175	0.9315	0.9361	0.8941
Speckle noise 0.01	0.9099	0.8954	0.9057	0.9131	0.8812
Speckle noise 0.05	0.8454	0.8386	0.8348	0.8582	0.8188
Speckle noise 0.1	0.8124	0.8043	0.8190	0.8255	0.8000

Table 11 Wiener filter attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Wiener filter 3×3	0.9998	0.9994	0.9994	0.9990	0.9955
Wiener filter 5×5	0.9995	0.9997	0.9997	0.9989	0.9947
Wiener filter 7×7	0.9997	0.9994	0.9998	0.9989	0.9943
Wiener filter 9×9	0.9992	0.9997	1.0000	0.9992	0.9942
Wiener filter 11×11	0.9990	0.9998	1.0000	0.9994	0.9953

Table 12 Median filter attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Median filter 3×3	0.9768	0.9806	0.9445	0.9647	0.9802
Median filter 5×5	0.9542	0.9540	0.9206	0.9378	0.9499
Median filter 7×7	0.9096	0.9027	0.8866	0.8978	0.9069
Median filter 9×9	0.8497	0.8554	0.8519	0.8387	0.8440
Median filter 11×11	0.7947	0.7999	0.8063	0.7883	0.7854



Table 13 Jpeg compression attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Jpeg compression $Q = 90$	0.9889	0.9892	0.9908	0.9919	0.9779
Jpeg compression $Q = 80$	0.9815	0.9796	0.9883	0.9869	0.9673
Jpeg compression $Q = 70$	0.9772	0.9698	0.9810	0.9802	0.9526
Jpeg compression $Q = 50$	0.9605	0.9537	0.9658	0.9671	0.9346
Jpeg compression $Q = 30$	0.9419	0.9275	0.9455	0.9540	0.8991
Jpeg compression $Q = 10$	0.8608	0.8429	0.8688	0.8680	0.8292

Table 14 Gamma correction attacks

Attack/image	Peppers	Lena	Boat	Barbara	Cameraman
Gamma correction $\gamma = 0.9$	0.9901	0.9921	0.9930	0.9913	0.9862
Gamma correction $\gamma = 0.8$	0.9831	0.9863	0.9867	0.9836	0.9812
Gamma correction $\gamma = 0.7$	0.9743	0.9801	0.9836	0.9764	0.9738
Gamma correction $\gamma = 0.5$	0.9556	0.9645	0.9746	0.9591	0.9584
Gamma correction $\gamma = 0.3$	0.9259	0.9491	0.9606	0.9436	0.9300
Gamma correction $\gamma = 0.1$	0.8779	0.9300	0.9423	0.9236	0.8872

pattern \tilde{w} by subtracting the estimated original from the watermarked work:

$$\tilde{w} = A^w - \tilde{A}.$$

Finally, the estimated watermark pattern \tilde{w} is added to the unwatermarked image A^t to obtain a watermarked version and thus

$$A^{tw} = A^t + \tilde{w}.$$

This method has been implemented to the test images Peppers as a watermarked image A^w and Lena, Boat, and Cameraman as unwatermarked images A^t . The obtained results for different block sizes m of median filtering are shown in Table 15. Due to weak NCC values we see that our scheme is resistant against this kind of attack.

Ambiguity attack with blind detection

An ambiguity attack against a scheme that uses blind detection is as follows: after watermarking of the original image A by the owner and creating A^w , the adversary embed the fake watermark w^F on the watermarked image A^w and makes rewatermarked image A^{wF} . Then, the detection process tries to extract the fake watermark w^F .

In this case, first, we notice that our embedding scheme is invertible, and using the embedded watermark, we can derive the original image A . Now, if we invert the embedding process on the rewatermarked image A^{wF} using original watermark w , we derive the original image A , while applying this process with fake watermark w^F , will give the watermarked image A^w .

Table 15 Resistance of the proposed scheme against copy attack with weak NCC values

Median filtering block size	Unwatermarked image A^t		
	Lena	Boat	Cameraman
$m = 3$	0.5474	0.6191	0.5773
$m = 5$	0.6005	0.6277	0.6193
$m = 7$	0.6338	0.6485	0.6573
$m = 9$	0.6573	0.6764	0.6771
$m = 11$	0.6773	0.7078	0.6925



Fig. 6 UM and cameraman watermarks used in the comparison of the schemes

Comparative analysis of the proposed scheme

In this section, the comparison of the proposed scheme with the scheme in [23] is considered under approximately the same conditions. The scheme proposed in [23] represents a blind digital watermarking algorithm based on probabilistic neural network (PNN) in the wavelet domain. The watermarking procedure is performed by embedding a logo watermark of size 64×64 in the middle-frequency coefficient block of three DWT levels. The PNN is used during watermark extraction.

Table 16 NCC comparison of the proposed scheme with the scheme in [23]

Type of attack	Cameraman logo		UM logo	
	Our scheme	Scheme in [23]	Our scheme	Scheme in [23]
JPEG compression $Q = 70$	0.9772	0.9572	0.9418	0.8451
JPEG compression $Q = 50$	0.9605	0.9451	0.9117	0.7520
JPEG compression $Q = 10$	0.8950	0.8910	0.6974	0.4395
Rotation $d = 5^\circ$	0.9326	0.9841	0.8554	0.9251
Rotation $d = 45^\circ$	0.9343	0.9762	0.8642	0.8965
Gaussian noise $V = 0.004$	0.8911	0.9924	0.8671	0.9753
Gaussian noise $V = 0.025$	0.8203	0.9928	0.7298	0.9863
Cropping (left upper side 25%)	0.9128	0.9096	0.8043	0.6660
Cropping (right lower side 25%)	0.9893	0.9868	0.9783	0.9023
Median filtering 3×3	0.9868	0.9837	0.9535	0.9329

The robustness test of the scheme in [23] is done under few attacks (only JPEG compression, rotation, Gaussian noise, cropping, and median filter) and the other attacks examined in our discussion are not considered. On the other hand, the security requirement is not discussed. Then, our comparison is limited to the common considered attacks. The used watermarks in both schemes are the UM and Cameraman logos of size 64×64 (Fig. 6). This comparison is presented in Table 16 and the best NCC value is bolded in each attack. An overall comparison shows the priority of our scheme in the common considered attacks.

Conclusion

In this study, a new robust image watermarking based on discrete wavelet transform (DWT) is proposed. This scheme uses DWT properties to achieve the watermarking requirements. These properties are the edge detection and perfect reconstruction of the DWT. In the detection process of the proposed algorithm, there is no need to any data of watermark or host image and this procedure is completely blind. To the blind extraction and its security properties, the proposed scheme is more appropriate for watermarking applications such as fingerprint, copy, and copyright protections. The experimental results showed that the scheme is invisible with a high PSNR and resistant against many geometrical and non-geometrical attacks with a good NCC values. Two security attacks also are considered that confirms the security property of the scheme.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

- Shih, F.Y.: Image Processing and Pattern Recognition. Wiley, Hoboken (2010)
- Lin, S., Chen, C.F.: A robust DCT-based watermarking for copyright protection. *IEEE Trans. Consum. Electron.* **46**(3), 415–421 (2000)
- Patra, J.C., Phua, J.E., Bornand, C.: A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. *Digit. Signal Process.* **20**(6), 1597–1611 (2010)
- Premaratne, P., Ko, C.: A novel watermark embedding and detection scheme for images in DFT domain. In: 7th International Conference on Image Processing and Its Applications, pp. 780–783 (1999)
- Rastegar, S., Namazi, F., Yaghmaie, K., Aliabadian, A.: Hybrid watermarking algorithm based on singular value decomposition and radon transform, *AE. Int. J. Electron. Commun.* **65**(7), 658–663 (2011)
- Lai, C.C., Tsai, C.C.: Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans. Instrum. Meas.* **59**(11), 3060–3063 (2010)
- Lagzian, S., Soryani, M., Fathy, M.: A new robust watermarking scheme based on RDWT-SVD. *Int. J. Intell. Inf. Process.* **2**(1), 22–29 (2011)
- Makbol, N.M., Khoo, B.E.: Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition, *AE. Int. J. Electron. Commun.* **67**(2), 102–112 (2013)
- Makbol, N.M., Khoo, B.E.: A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digit. Signal Process.* **33**, 134–147 (2014)
- Liu, R., Tan, T.: An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans. Multimed.* **4**(1), 121–128 (2002)
- Ganic, E., Eskicioglu, A.M.: Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *J. Electron. Imaging* **14**(4), 043004 (2005)
- Loukhaoukha, K., Chouinard, J.Y., Haj Taieb, M.: Optimal image watermarking algorithm based on LWTSVD via multi-objective ant colony optimization. *J. Inf. Hiding Multimed. Signal Process.* **2**, 303–319 (2011)
- Gupta, A., Raval, M.: A robust and secure watermarking scheme based on singular values replacement. *Sadhana* **37**, 425–440 (2012)



14. Gonzalez, R.C., Woods, R.E.: Digital Image Processing, 3rd edn. Pearson International Edition, London (2008)
15. Daubechies, I.: Ten Lectures on Wavelets. Society for Industrial and Applied Mathematics, Pennsylvania (1992)
16. Goswami, J.C., Chan, A.K.: Fundamentals of Wavelets, Theory, Algorithms, and Applications. Wiley, New York (1999)
17. Lee, Y.P., Lee, J.C., Chen, W.K., Chang, K.C., Su, I.J., Chang, C.P.: High-payload image hiding with quality recovery using tri-way pixel-value differencing. *Inf. Sci.* **191**, 214–225 (2012)
18. Al-Haj, A.: Combined DWT-DCT digital image watermarking. *J. Comput. Sci.* **3**(11), 740–746 (2007)
19. Bounkong, S., Toch, B., Saad, D., Low, D.: ICA for watermarking digital images. *J. Mach. Learn. Res.* **4**, 1471–1498 (2003)
20. Schyndel, R.G.V., Tirkel, A.Z., Osborne, C.F.: A digital watermark. *IEEE Proc. Int. Conf. Image Process.* **2**, 86–90 (1994)
21. Cox, I., Miller, M., Bloom, J.: Digital Watermarking. The Morgan Kaufmann Publishers, San Francisco (2001)
22. Kutter, M., Voloshynovskiy, S., Herrigel, A.: The Watermark Copy Attack, in Security and Watermarking of Multimedia Contents II, SPIE-3971:371380 (2000)
23. Al-Nabhani, Y., et al.: Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. *J. King Saud Univ. Comput. Inf. Sci.* (2015) doi:[10.1016/j.jksuci.2015.02.002](https://doi.org/10.1016/j.jksuci.2015.02.002)

