



A sophisticated and provably grayscale image watermarking system using DWT-SVD domain

Seif Eddine Naffouti¹ · Anis Kricha^{2,3} · Anis Sakly¹

Accepted: 6 June 2022 / Published online: 1 July 2022

© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2022

Abstract

Digital watermarking has attracted increasing attentions as it has been the current solution to copyright protection and content authentication in today's digital transformation, which has become an issue to be addressed in multimedia technology. In this paper, we propose an advanced image watermarking system based on the discrete wavelet transform (DWT) in combination with the singular value decomposition (SVD). Firstly, at the sender side, DWT is applied on a grayscale cover image and then eigendecomposition is performed on original HH (high–high) components. Similar operation is done on a grayscale watermark image. Then, two unitary and one diagonal matrices are combined to form a digital watermarked image applying inverse discrete wavelet transform (iDWT). The diagonal component of original image is transmitted through secured channel. At the receiver end, the watermark image is recovered using the watermarked image and diagonal component of the original image. Finally, we compare the original and recovered watermark image and obtained perfect normalized correlation. Simulation consequences indicate that the presented scheme can satisfy the needs of visual imperceptibility and also has high security and strong robustness against many common attacks and signal processing operations. The proposed digital image watermarking system is also compared to state-of-the-art methods to confirm the reliability and supremacy.

Keywords Copyright protection · Digital image watermarking · Discrete wavelet transform (DWT) · Singular value decomposition (SVD) · Imperceptibility · Robustness

1 Introduction

Owing to the popularity of the Internet and the rapid growth of multimedia technology, interactive media have become the most important gadgets for transmitting information [1]. Day by day, the scenario of the global pandemic situations is increasing, which makes the mode of business and communication is converted into digital form. This means that there are a lot of data are moving worldwide in the digital platform. Consequently, due to the pandemic situation of

COVID-19, exchanging digital multimedia data has become a very frequently task and has caused considerable interest within the community. However, such open access to Internet makes way for digital multimedia data such as text, image, audio and video to be easily duplicated, modified and redistributed without the owner's permission. So, protecting ownership of digital media content has become a paramount issue. Digital watermarking stands here as suitable solution to verify the authenticity and to solve ownership issues. Digital watermarking is a technique for hiding data, which can be a logo for an organization, digital signature or image of an author, into multimedia object like text, image, audio or video. Furthermore, high security requirements of images in many scenarios such as military and trade stimulate the development of digital image encryption [2–5] and forensic algorithms [6]. Transparency and robustness are considered two mainly important properties for digital watermarking algorithm [7], as well they are measured using a quality metric: peak signal-to-noise ratio and normalized correlation, respectively.

✉ Seif Eddine Naffouti
seifeddine.naffouti@gmail.com

¹ Laboratory of Automation, Electrical Systems and Environment (LAESE), National Engineering School of Monastir (ENIM), University of Monastir, 5019 Skaness Monastir, Tunisia

² Laboratory of Advanced Technology and Intelligent Systems (LATIS), National Engineering School of Sousse, 4023 Sousse, Tunisia

³ National Engineering School of Monastir (ENIM), Ibn El Jazzar, 5019 Skaness, Tunisia

According to the domain in which the watermark is inserted, digital watermarking techniques could be classified into two main categories that are in spatial domain and in frequency domain transform. The least significant bit (LSB) substitution, pixel value differencing (PVD), exploiting modification direction (EMD), and modulus function (MF) are some of the well-known approaches in spatial domain [8]. On the contrary, transformed domain-based watermark embedding technique inserts a watermark by altering the transformed coefficients of the original image. There are a lot of transform domain watermarking methods which are available in the various literature such as discrete wavelet transform (DWT) [9], singular value decomposition (SVD) [10], discrete cosine transforms (DCT) [11], discrete Fourier transforms (DFT) [12], discrete Hadamard transform (DHT) [13] and redundant wavelet transform (RWT) [14]. It is said that, in terms of resisting attacks, the frequency domain techniques are not only better than most of spatial domain techniques but also further complex than the spatial method [15] and require higher computational cost [16].

Depending on its objective, data hiding can be divided into watermarking for copyright protection and steganography for securing confidentiality [17]. Researchers have proposed a lot of effective techniques to overcome some of the inherent limitations of data hiding. Therefore, the design of a simple and efficient, yet sufficiently imperceptible and robust watermarking method still constitutes a challenging task. The LSB approaches hide the secret data directly inside the cover image pixel [18]. Wu and Hwang [19] proposed an improved LSB substitution using a group of three pixels as an embedding unit to hide three bit of secret data. The possible modification for each pixel is at most ± 1 . Sahu and Swain [20] improved the hiding capacity (HC) using the concept of bit differencing and modified LSB matching.

The motivation behind pixel value differencing (PVD) steganography [21] is to make a clear distinction among the smooth and textured areas of an image. The smooth areas are the low-intensity sections where the neighboring pixel values are close to each other, but texture areas have a considerable difference. Hence, the smooth areas cannot tolerate high changes as compared to the textured areas. An adaptive PVD approach has been proposed by Swain [22], to improve the HC. The data embedding is performed in both horizontal and vertical directions. Various articles have been proposed in the literature using PVD approaches [23,24].

Aiming to secure information, and copyright protection authentication, the solution is also to apply an appropriate hybrid method. Wu et al. [25] combined the LSB substitution and PVD approach. This improved the HC as compared to the PVD approach of Wu and Tsai [21]. The work has been carried out by many researchers [26–28] to improve the HC as well as security. In the same context, a lot of attention has also been paid to combine the frequency domain

with the eigendecomposition values of the image, i.e., the use of the frequency channels and thus the eigenvalues and their corresponding eigenfunctions of the image. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify areas in the cover image where a watermark can be imperceptibly embedded. One of attractive mathematical properties of SVD is that slight variations of singular values do not affect the visual perception of the cover image, which motivates the watermark embedding procedure to achieve better transparency and robustness. Consequently, many image watermarking techniques combining these two transform methods have been proposed. For example, Yasmeeen and Uddin [29] proposed an improved DWT–SVD-based hybrid approach to further ensure the robustness and protection of digital data. This method contrasted with existing schemes and proved to be a good mechanism for both grayscale and color images. Makbol et al. [30] used DWT–SVD image transform and human visual system (HVS) to improve performance of watermarking scheme where watermark was embedded by modifying several elements in its U matrix. Recently, similar work also has been pursued by Ahmadi et al. [31] in which a hybrid (DWT–SVD) watermarking scheme, human visual system and an intelligence optimization algorithm known as PSO (particle swarm optimization) are used to provide high robustness and capacity. However, their method is not invariant against rotational attacks. Moreover, its security needs to be improved by encrypting the watermark image before embedding. DWT and SVD were also employed in a robust and secure watermarking scheme by Ansari et al. [32]. Zear et al. [33] studied a blind watermarking method by fusing DWT, DCT and SVD, where the noise effects in watermark extraction are suppressed by the back propagation neural network (BPNN). Liu Y et al. [34] designed a non-blind watermarking scheme with DWT and SVD, the security of watermarks has been improved significantly with RSA encryption algorithm. For further detailed description on the aforementioned approaches, we refer keen reader to [35–37].

Further, Liao et al. [38] introduced a novel amplifying channel modification probabilities (ACMP) approach for color images. The traditional steganographic approaches conceal the secret data equally in the RGB channels. On the contrary, Liao et al. explored the correlations among the RGB channels and conceals the data adaptively to achieve high HC and resistance against various steganalysis attacks. Various steganographic approaches utilizing color images were presented in the literature [39,40]. Liao et al. in [41] have newly proposed two payload strategies, which are based on the image texture complexity and the distortion distribution as indicator for secure capacity of each cover image. These strategies are applied on single image steganographic algorithms and experiments shown better resistance to modern universal pooled steganalysis compared to existing methods.

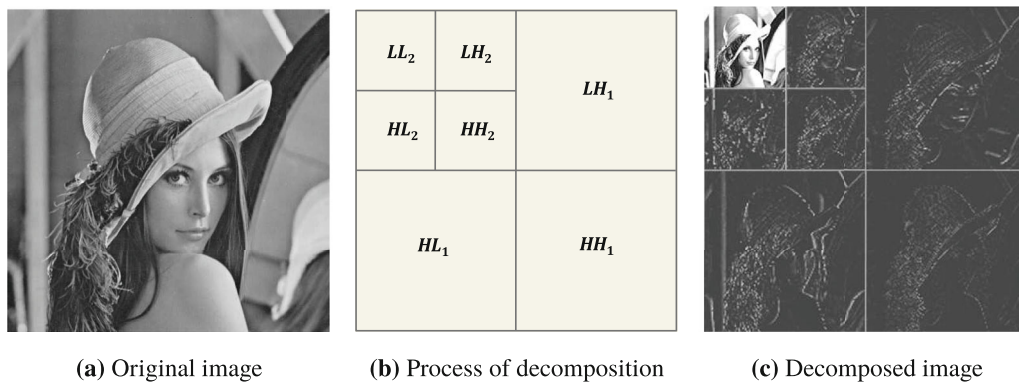


Fig. 1 Example of two-level DWT transform

1.1 Contributions

This paper introduces a sophisticated hybrid SVD-DWT for an efficient image watermarking technique for grayscale image hiding. Because of the conflict between invisibility and robustness, the insertion of watermark is usually made in LH, HL and HH sub-bands to maintain the quality of the original image. As HVS (human visual system) is less sensitive to high-frequency parts, HH sub-band is chosen for embedding watermark as it contains finer details and contributes insignificantly toward signal energy. Hence, watermarking embedding in this region will furnish better image quality, but at the same time yields to poor results when extracting watermark. However, our proposed technique has highly overcome this issue in the watermark extraction process. We aggregated DWT-SVD domain with the chosen HH sub-band in which the watermark should be embedded and extracted too. At last, with these observations in mind, we construct our watermarking approach and demonstrate that guarantees to achieve high invisibility and robustness.

The rest of the paper is structured as follows. Section 2 shows the relevant theoretical background information. The watermark embedding and extraction algorithms proposed in this paper are described in detail in Sect. 3. Section 4 introduces the image quality measures. Section 5 presents the experimental setup and simulation results of the proposed approach with imperceptibility, robustness, computational complexity and capacity analysis and compares its performance with other related algorithms. Finally, conclusions and future work are provided in Sect. 6.

2 Background

This section is devoted to the brief explanations of the concepts being used in the proposed scheme such as DWT and SVD transforms. Interested to know more in detail may refer to the respective studies [10,42–47].

2.1 Discrete wavelet transform (DWT)

Discrete wavelet transform (DWT) is widely used as an ideal tool in the field of frequency analyzing and signal processing, including image watermarking. It is indeed a multiscale signal analysis method, inherits and develops the idea of Fourier transform fixed resolution, having features of multiresolution and local signal analysis [44]. The strength of DWT over Fourier transform is its ability to produce a temporal resolution in which it captures both frequency and location information.

One-level DWT or one-dimensional DWT splits an original image into four non-overlapping multiresolution sub-bands, including a low-frequency sub-band LL and three high-frequency sub-bands HL, LH, HH [42,43]. Among them LL, standing for the coarse-level coefficients is the most similar sub-image to the original image, called approximation sub-band. The other three sub-bands LH, HL and HH represent the finest scale wavelet coefficients denoting horizontal direction detail, vertical and diagonal direction image, respectively. Moreover, the low-frequency sub-band can be further decomposed into another four different sub-bands. Two-level DWT decomposition is shown in Fig. 1, where the low-frequency component represents the most contents of the original image and the high-frequency represents the edge, contour and texture characteristics of the original image. Figure 1b expresses the different frequency schematic picture of the original image ‘Lena,’ and Fig. 1c shows the structures of ‘Lena’ image after the two-level discrete wavelet transform decomposition.

2.2 Singular value decomposition (SVD)

Singular value decomposition (SVD) is a matrix diagonalization efficient algorithm in the numerical linear algebra technique for a variety of applications [10,45–47]. The basic idea behind the SVD-based watermarking techniques is to find the SVD of the cover image or each block of the cover

image and then modify the singular values to embed the watermark. There are three main key features of SVD in digital image watermarking techniques:

1. The singular value of an image has very good stability and noise immunity. When a small perturbation is added to an image, large variation of its singular values does not occur.
2. The singular value in the value sequence obtained by SVD operation of an image specifies the luminance of an image layer, where pairs of singular vectors specify the geometry of the image.
3. The inherent algebraic image properties are demonstrated by the singular values [44,47]. The extracted watermark image will always be disturbed by the process of geometric manipulations, especially the extraction of blind or semi-blind watermarking algorithm. According to the characteristics of SVD, the cover image is able to withstand certain geometric distortions, if singular value decomposition is performed on the processes of watermark embedding and extraction.

From the perspective of image processing, an image can be viewed as a matrix with non-negative scalar entries. Let A be a rectangular matrix with $m \times n$ size; then according to SVD, it can be decomposed mathematically into three matrices as

$$A = USV^T, \quad (1)$$

where U and V are orthogonal (or unitary) matrices, i.e., $UU^T = I$, $VV^T = I$; S is non-negative diagonal matrix whose diagonal elements (singular values) coincide with the square roots of the eigenvalues of $A^T A$ and arranged in descending order as $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n \geq 0$. Thus, the columns of U are the left singular vectors, whereas the columns of V are the right singular vectors of A . A graphical description of the procedure of SVD of an $m \times n$ image is presented in Fig. 2 [48].

3 Proposed watermarking system

In this section, grayscale image watermarking approach is proposed. It is based on SVD and DWT techniques. The major goal of this proposal is to embed a grayscale watermark image into a grayscale image without perceptual degradation of watermark taking into account robustness against several kinds of attacks. Moreover, both imperceptibility and robustness can be achieved simultaneously. The suggested algorithm for secure communication of image belongs to two parts: the watermark embedding and extraction algorithm. Embedding and extraction processes are two main phases for

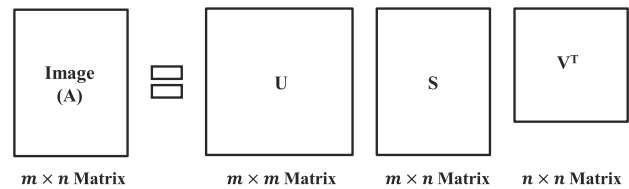


Fig. 2 The procedure of SVD decomposition

image-watermarking scheme. Both parts along with respective flowcharts are described in detail in Sects. 3.1 and 3.2.

3.1 Embedding process for sending side

A step-by-step procedure of the embedding algorithm at the sender side as illustrated in Fig. 3 is explained below:

Step 1: Apply one-level DWT to the original image A to decompose it into four sub-bands as given in Eq. (2).

$$[LL \ LH \ HL \ HH] = \text{DWT}(A) \quad (2)$$

Step 2: Apply the eigendecomposition SVD to the high-frequency sub-band HH as given in Eq. (3).

$$[U_O S_O V_O] = \text{SVD}(HH) \quad (3)$$

where the unitary and diagonal matrices are U_O , V_O and S_O ; superscript O corresponds to original image.

Step 3: Repeat steps 1 to 2 for watermark image W and after eigendecomposition the corresponding matrices are U_W , V_W and S_W ; where superscript W represents watermark image.

Step 4: Modify the singular value of the decomposed image with the singular value of the watermark image using a scaling factor α which controls the strength of the watermark to be inserted. This is given in (4).

$$S_2 = S_O + \alpha \times S_W \quad (4)$$

Step 5: Combine the orthogonal matrices of the decomposed original image with the modified singular value matrix to obtain a modified DWT coefficients as given in (5).

$$HH_2 = U_O S_2 V_O^T \quad (5)$$

where T is transpose of a matrix.

Step 6: Apply one-level inverse DWT (iDWT) to resultant image HH_2 instead of HH sub-band to produce the watermarked image, as shown in (6).

$$A_W = \text{iDWT}(LL \ LH \ HL \ HH_2) \quad (6)$$

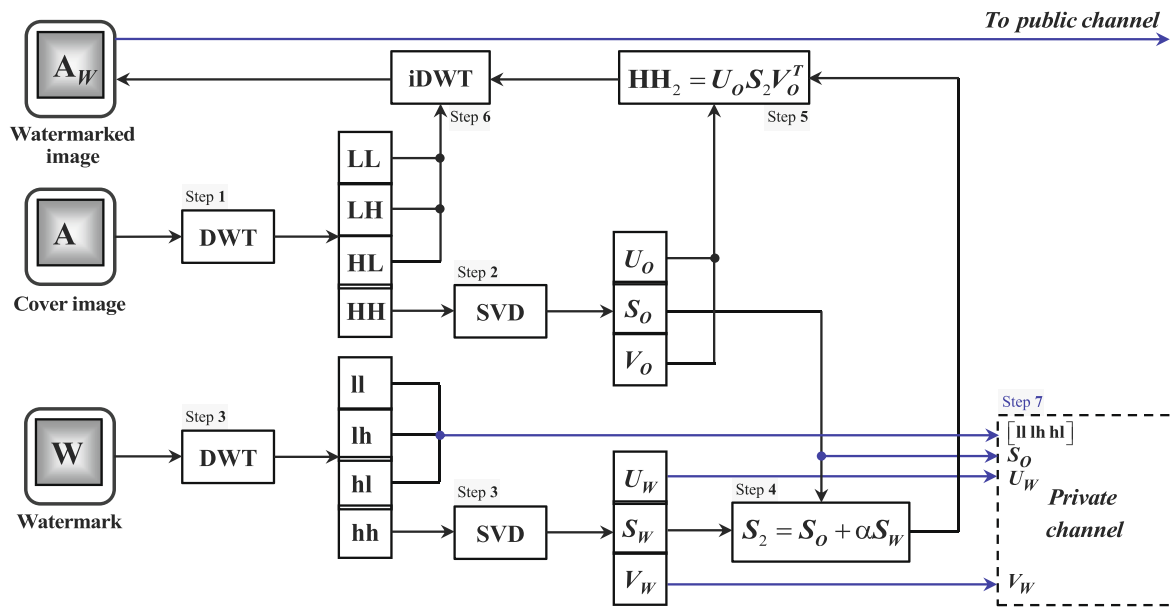


Fig. 3 Block diagram of the proposed embedding algorithm

Step 7: Transmit through a secure channel the diagonal matrix S_O of the original image, the unitary matrices U_W and V_W of the watermark image, and the first three non-modified DWT sub-bands of the watermark to be subsequently used at the receiver side for the extraction watermarking process.

3.2 Extraction process for receiving side

A step-by-step procedure of the extraction algorithm at the receiver side as illustrated in Fig. 4 is detailed below:

Step 1: Apply DWT to the watermarked (possibly distorted) image A_W^* , that we receive it from the public channel, to decompose it into four sub-bands as given in Eq. (7).

$$[LL_2 \ LH_2 \ HL_2 \ HH_2] = DWT(A_W^*) \tag{7}$$

where * is a mark of probable corruption resultant from attacks.

Step 2: Apply SVD to the high-frequency sub-band HH_2 as given in Eq. (8).

$$[U_O^* \ S_O^* \ V_O^*] = SVD(HH_2) \tag{8}$$

Step 3: The diagonal matrix S_O of the decomposed original image is already received from the private channel. Compute the correlation coefficient (Cr) to measure closeness between the diagonal components S_O and S_O^* of the decomposed original image and

the decomposed watermarked image, respectively, such that $Cr(S_O, S_O^*) =$

$$\frac{\sum_m \sum_n (S_O - \bar{S}_O)(S_O^* - \bar{S}_O^*)}{\sqrt{(\sum_m \sum_n (S_O - \bar{S}_O)^2)(\sum_m \sum_n (S_O^* - \bar{S}_O^*)^2)}}$$

where \bar{S}_O and \bar{S}_O^* are the average values of S_O and S_O^* , respectively. The value of Cr ranges between -1 and $+1$. The Cr gives numerical result that expresses how well two diagonal components match. The higher the metric, the more accurate the match.

Step 4: At this stage, even before constructing the watermark, a preliminary decision could be taken to claim that the watermark will be successfully extracted or not. Depending on the Cr value, verify the following conditions:

- (i) If $Cr = 1$, this means that the watermarked image was not attacked. So subtract the received singular value S_O of the decomposed original image from the singular value S_O^* of the decomposed watermarked image and divide the values by the scaling factor α to obtain the singular value of the watermark image. This is given in Eq. (9).

$$S_W^* = (S_O^* - S_O) / \alpha \tag{9}$$

- (ii) If not, i.e., $Cr < 1$ which means that the watermarked image was indeed attacked; recompute the singular value of the watermark without dividing by the scaling factor using Eq. (10).

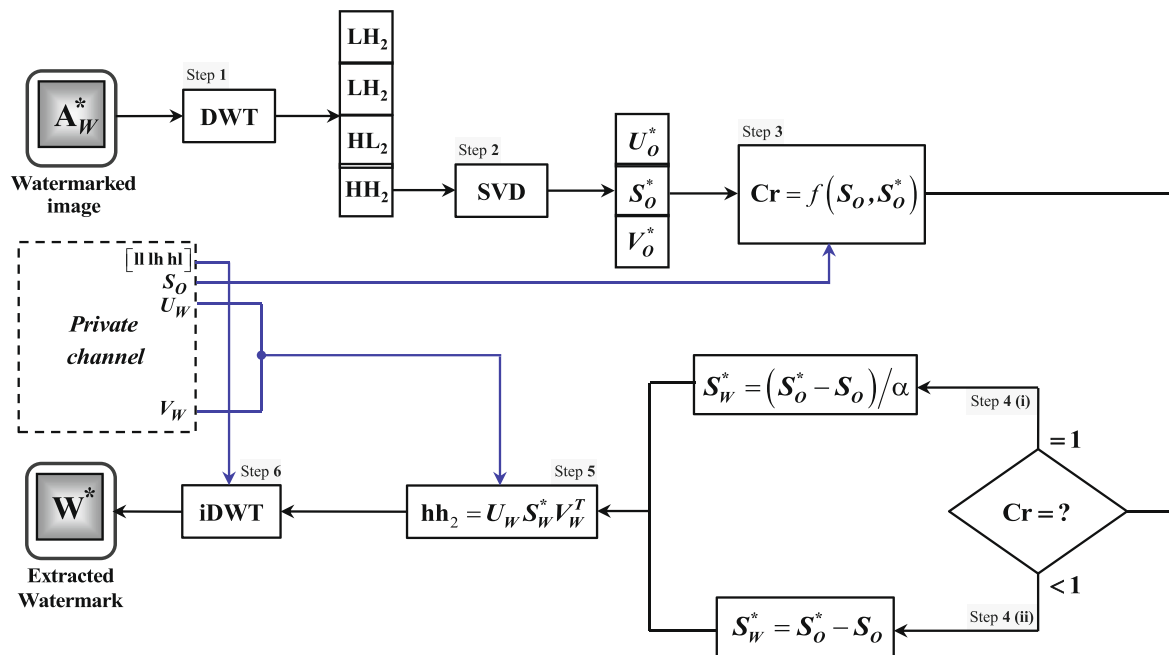


Fig. 4 Block diagram of the proposed extracting algorithm

$$S^*_W = S^*_O - S_O \tag{10}$$

Step 5: The orthogonal matrices of the watermark image are also already received from the private channel; combine them with the recovered singular value matrix S^*_W to obtain a modified DWT coefficients as given in Eq. (11)

$$hh_2 = U_W S^*_W V^T_W \tag{11}$$

Step 6: By using the obtained hh_2 sub-band together with the three other sub-bands of one-level DWT of watermark image, recreate the watermark image W^* by performing the one-level inverse DWT, as shown in Eq. (12)

$$W^* = \text{iDWT}(\text{ll lh hl } hh_2) \tag{12}$$

Step 7: Finally, the sending watermark image W and the recovered image W^* are compared using common performance metrics for image quality assessment.

4 Performance evaluation metrics

Watermarking algorithms are usually evaluated with respect to imperceptibility and robustness. In this paper, PSNR, mean square error (MSE), structural similarity (SSIM) index measure, universal image quality index (UIQI) and normalized

correlation (NC) are chosen as quality assessment parameters.

4.1 Peak signal to noise ratio

The peak signal-to-noise ratio (PSNR) is used to measure a watermarked image quality. The PSNR, which is measured in decibels, defines the resemblance between an original image and the reconstructed image [49]. In the ideal case, the PSNR should be infinite [50]. In fact, this cannot be accomplished with watermarked image. So, the larger PSNR the better. The PSNR in decibels (dB) can be calculated using Eq. (13).

$$PSNR_{\text{dB}} = 10 \log_{10} \left(\frac{A^2_{\text{max}}}{MSE} \right) \tag{13}$$

where A_{max} is the maximum possible pixel value of the grayscale image A .

4.2 Mean square error

Mean square error (MSE) is a standard quality measurement. It is the average of the pixel difference between two images. In ideal case, the MSE must be zero. In fact, this is not reached with watermarked image [51]. So, the smaller the value of MSE, the better the quality is. MSE is defined as

$$MSE = \frac{1}{M \times N} \sum_i^M \sum_j^N (A(i, j) - A_W(i, j))^2 \tag{14}$$

where A is the original image before watermarking, A_W is the watermarked image, and M & N are the original image width and height, respectively.

4.3 Structural similarity

Structural similarity (SSIM) index measure is a method for quality assessment used as a performance metric to evaluate invisibility between two images. It is considered as a full reference metric; in other words, the prediction or measurement of image quality is based on an initial distortion-free or uncompressed image as reference. The SSIM index is defined by

$$SSIM = \frac{(2\mu_A\mu_{A^*} + c_1)(2\sigma_{AA^*} + c_2)}{(\mu_A^2 + \mu_{A^*}^2 + c_1)(\sigma_A^2 + \sigma_{A^*}^2 + c_2)} \tag{15}$$

here, μ_A and μ_{A^*} are the average of image A and A^* , respectively. σ_A^2 and $\sigma_{A^*}^2$ are the variance of image A and A^* , respectively. σ_{AA^*} is the covariance of image A and A^* , respectively. $c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$ are used to keep the stabilization of the division with a weak denominator. L is the dynamic range of the pixel-values (typically $L = 255$), with $k_1 = 0.01$ and $k_2 = 0.03$ by default [52].

4.4 Universal image quality index

Watermarked image quality can be also measured by using universal image quality index (UIQI). In fact, this quality index models any distortion as a combination of three different factors: loss of correlation, luminance distortion, and contrast distortion [53]. The dynamic range of UIQI is $[-1 \ 1]$. A UIQI value closer to 1 specifies that the watermarked image is indistinguishable to the cover image. The UIQI between two images can be calculated as follows:

$$UIQI = \frac{4\sigma_{AA^*}\bar{A}\bar{A}^*}{(\sigma_A^2 + \sigma_{A^*}^2)[(\bar{A})^2 + (\bar{A}^*)^2]} \tag{16}$$

where \bar{A} and \bar{A}^* are the average of image A and A^* , respectively. σ_A^2 and $\sigma_{A^*}^2$ are the variance of image A and A^* , respectively. σ_{AA^*} is the covariance of image A and A^* , respectively.

4.5 Normalized correlation

Normalized correlation (NC) can be used to measure the degree to which the used algorithm can withstand attack. In ideal case, NC should equal 1 [54]. In real, this could be achieved unless the watermarked image does not undergo any kind of attack. A larger NC value means a higher degree of

similarity between two images. The NC is defined as follows:

$$NC = \frac{\sum_i^m \sum_j^n W(i, j) W^*(i, j)}{\sqrt{\sum_i^m \sum_j^n W(i, j)^2} \sqrt{\sum_i^m \sum_j^n W^*(i, j)^2}} \tag{17}$$

where W is the original watermark image and W^* is the corresponding extracted watermark.

5 Experiments and results

In this section, we present the qualitative and quantitative results for image watermarking to evaluate the performance of our proposed framework. Note that reading input images, performing discrete wavelet transform, solving eigenproblem, and computing performance evaluation metrics are all of them implemented in MATLAB© R2015b environment. The effectiveness of our approach is validated by carrying out a comprehensive comparison with several state-of-the-art methods.

5.1 Datasets

The performance of the proposed framework is tested for two different tasks, i.e., for watermark embedding and extraction; as well as it is evaluated on a two challenging standard test images: we use dataset of standard 512×512 grayscale test images provided by computer vision group [55] which contains 49 test images, and image repository provided by the waterloo fractal coding and analysis group [56] that is divided into three sets from which we use 12 images existing in Grayscale Set 2.

5.2 Experimental settings

Several experiments are performed comprehensively for evaluating effectiveness of the proposed algorithm. Seven standard grayscale images, namely ‘Zelda,’ ‘Lena,’ ‘Goldhill,’ ‘Peppers,’ ‘Butterfly,’ ‘Baboon’ and ‘Lake,’ are taken as cover images of size 512×512 as depicted in Fig. 5a–g, whereas WaterMark logo of size 512×512 is used as a watermark image presented in Fig. 5h. Although we have shown just seven test images, the proposed algorithm was also executed on other standard test images obtained from the same aforementioned image databases.

Relative parameter used in the proposed algorithm is set up according to the experiment results. Associated parameter setting is the scaling factor alpha of the watermark image. The scaling factor alpha is chosen manually through a trial-and-error basis. In order to pull the essence of our watermarking algorithm, we recommend $\alpha = 0.01$. This allows our watermarking algorithm itself to achieve its sat-



Fig. 5 a–g Cover images for test: ‘Zelda,’ ‘Lena,’ ‘Goldhill,’ ‘Peppers,’ ‘Butterfly,’ ‘Baboon,’ ‘Lake,’ respectively; **h** Watermark image

Table 1 List of various attacking operations and their parameter values

Full name of attack type	Attack index	Parameter	Parameter values
Gaussian noise	Gs	Mean, variance	0 and 0.01 (default)
Salt & pepper noise	Slp	Noise density	0.05 (default)
Speckle noise	Spn	Variance	0.05 (default)
Rotation + crop	Rtc	Angle	45°
Cropping	Cr	Proportion	TL1/4
Translation	Tr	Displacement	(80 × 80)
Histogram equalization	HE	Bins	64 (default)
Rescaling	Rsc	Scale	512 → 256 → 512
Sharpening	Shp	Amount, radius	1 and 0.8 (default)
Gaussian filter	GF	Filter size and standard deviation	[3 × 3] and 0.5 (default)
Average filter	Avg	Filter size	[3 × 3] (default)
Median filter	Md	Neighborhood size	[3 × 3] (default)
Wiener filter	WF	Neighborhood size	[3 × 3] (default)
Gamma correction	Gc	Gamma value	0.2
Flipping of rows	Fpr	Dimension	1 (default)
Flipping of columns	Fpc	Dimension	2

isfactory performance and thus to fulfill a better trade-off between imperceptibility and robustness as simultaneously as possible.

To estimate the robustness and reliability of the proposed method, watermarked images are exposed against different kinds of image attacks. The image attacks can be divided into four categories and are listed as follows: (1) noising attack: Gaussian noise (Gs), salt & pepper noise (Slp), and speckle noise (Spn); (2) denoising attack: Gaussian filter

(GF), average filter (Avg), median filter (Md) and Wiener filter (WF); (3) image-processing attack: histogram equalization (HE), sharpening (Shp) and gamma correction (Gc); (4) geometrical attack: rotation + crop (Rtc), cropping (Cr), translation (Tr), rescaling (Rsc), flipping of rows (Fpr) and flipping of columns (Fpc), which are listed in Table 1 with their corresponding attack parameters, where abbreviation of TL donates the position of top-left corner.

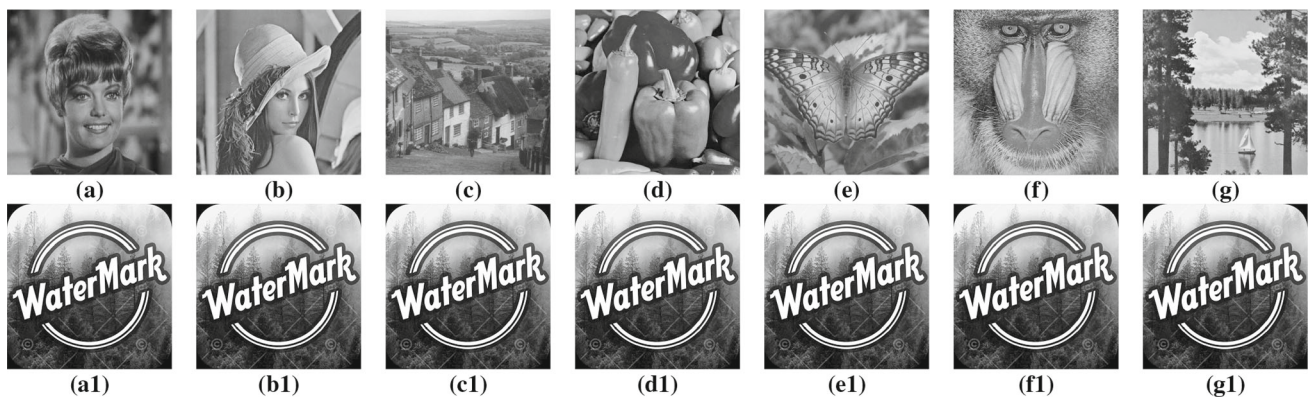


Fig. 6 Results of watermarked images and corresponding extracted watermarks without attack: **a–g** watermarked images; **a1–g1** extracted watermarks

5.3 Proof of imperceptibility

Imperceptibility is an important feature of the watermarking scheme. In this subsection, the imperceptibility analysis of the proposed scheme is done. PSNR and SSIM are most commonly used objective performance metrics to examine the perceptual transparency of the watermarking techniques. In general, if the PSNR value is ≥ 48 dB that means the quality of image is excellent and there is no changes which can be noticed. PSNR value in between 35 and 48 dB means good image quality and PSNR value ranging from 29 to 35 dB signifies acceptable image quality. PSNR value below 25 dB means the image is perceptible. Figure 6a–g illustrates the watermarked versions of original images after applying the proposed embedding algorithm. Table 2 displays the testimony of these images, and tabulates PSNR, MSE, SSIM, UIQI and NC values of all watermarked images under no attack. Still referring to Table 2, the proposed watermarking method is excellent in terms of imperceptibility since the average PSNR value is 48.1308 dB, and the PSNR values from all watermarked images are above 48 dB. Maximum PSNR and UIQI values are obtained for ‘Baboon’ image and are found here as 48.1314 dB and 1.0000, respectively. Moreover, SSIM, UIQI and NC are greater than 0.999 in each case. MSE, in turn, as a distortion index, illustrates low values that indicate higher quality. So, all values of these metrics provide well-founded results for the watermarked images. Obviously, no matter which cover image is used, the transparency of the image is always very good; which means that the proposed method performs well in imperceptibility.

Furthermore, PSNR, MSE, SSIM, UIQI and NC are reused to evaluate the proposed extracting algorithm under no attack. Figure 6a1–g1 illustrates the extracted watermarks from the watermarked images, and the subsequent Table 3 conveys all their numerical results between original and extracted watermark. As can be seen in this table, maximum SSIM

Table 2 PSNR (dB), MSE, SSIM, UIQI and NC values of watermarked images under no attack

Cover image	PSNR	MSE	SSIM	UIQI	NC
Zelda	48.1308	1.0000	0.9999	0.9997	1.0000
Lena	48.1308	1.0000	1.0000	0.9999	1.0000
Goldhill	48.1308	1.0000	1.0000	0.9999	1.0000
Peppers	48.1309	1.0000	1.0000	0.9990	1.0000
Butterfly	48.1306	1.0000	1.0000	0.9999	1.0000
Baboon	48.1314	0.9999	1.0000	1.0000	1.0000
Lake	48.1308	1.0000	1.0000	0.9999	1.0000
Average	48.1308	0.9999	0.9999	0.9997	1.0000

Table 3 PSNR (dB), MSE, SSIM, UIQI and NC values of extracted watermark image under no attack

Cover image	PSNR	MSE	SSIM	UIQI	NC
Zelda	36.0046	16.3162	1.0000	0.9776	0.9996
Lena	35.9681	16.4538	1.0000	0.9774	0.9996
Goldhill	35.9415	16.5550	1.0000	0.9771	0.9996
Peppers	36.0900	15.9987	1.0000	0.9777	0.9996
Butterfly	36.0635	16.0964	1.0000	0.9768	0.9996
Baboon	35.9474	16.5324	1.0000	0.9773	0.9996
Lake	35.9814	16.4038	1.0000	0.9775	0.9996
Average	35.9995	16.3366	1.0000	0.9773	0.9996

of 1.0000 is obtained for all extracted watermark images, while UIQI and NC values are very close to 1; that shows a high reconstruction of the extracted watermark images. In addition, PSNR and MSE values also validate the output. In short, original grayscale watermark image could be extracted completely without attack .

Table 4 Comparison chart of the proposed method with the state-of-the-art methods under no attack. All methods used ‘Lena’ as a test image

Method	Watermarked image		Extracted watermark	
	PSNR	SSIM	PSNR	NC
Yasmeen and Uddin [29]	43.8362	0.9909	26.1248	0.9934
Ahmadi et al. [31]	43.3281	0.9721	–	1
Agoyi et al. [49]	29.49	0.867	–	1
Ernawan et Kabir [52]	–	0.9965	–	1
Begum and Uddin [57]	50.9125	0.9745	–	1
Verma et al. [58]	41.5107	–	–	1
Wang and Zhao [59]	40.74	0.9996	–	1
Wang [60]	42.38	–	–	1
Salama and Mokhtar [61]	41.28	–	30	–
Das et al. [62]	41.78	–	–	1
Khare and Srivastava [63]	59.9850	0.9999	–	1
Takore et al. [64]	45.2223	–	–	–
Proposed method	48.1308	1.0000	35.9681	0.9996

Bold values indicate the data with the best comparison results

Table 5 Comparison chart of the proposed method with the state-of-the-art methods under no attack. All methods used ‘Peppers’ as a test image

Method	Watermarked image		Extracted watermark	
	PSNR	SSIM	PSNR	NC
Agoyi et al. [49]	34.3	0.9067	–	1
Ernawan et Kabir [52]	–	0.9968	–	0.9872
Begum and Uddin [57]	48.9065	0.9721	–	1
Verma et al. [58]	38.19	–	–	1
Wang and Zhao [59]	40.10	0.9995	–	1
Khare and Srivastava [63]	60.2320	0.9998	–	1
Ray et al. [65]	27.3823	–	–	–
Hu et al. [66]	45.128	–	–	1
Kang et al. [67]	42.25	0.9747	–	1
Kazemivash et al. [68]	37.7683	–	–	1
Kazemivash et al. [69]	38.9708	–	–	1
Moeinaddini et al. [70]	51.9802	0.9814	–	–
Proposed method	48.1309	1.0000	36.0900	0.9996

Bold values indicate the data with the best comparison results

Table 5 indicates the comparison of the watermarked image and extracted watermark for the proposed method against several baseline approaches (see [29,31,49,52,57–64] and references therein); in which all methods used ‘Lena’ as a test image. As is observed from this table, especially compared to the methods of [29,31,49,52,58–62,64], our proposal obtains better results in terms of PSNR and SSIM. For instance, the proposed method significantly outperforms [29] by 4.2946 dB and 0.91%, respectively, in PSNR and SSIM for watermarked image; 9.8433 dB and 0.62%, respectively, in PSNR and NC for extracted watermark. [57] and [63] also obtain good invisibility, and their average PSNRs are greater

than 55 dB. However, the invisibility of [49] is poor so that PSNR value is less than 30 dB.

Again, the three performance criteria, i.e., PSNR, SSIM and NC, are used in order to evaluate the quality of the watermarked image and the extracted watermark quantitatively. Table 5 illustrates the quality using these metrics and the comparison between the proposed method and the state-of-the-art methods [49,52,57–59,63,65–70] without attacks. Note that all these methods used ‘Peppers’ as a test image. As can be seen in this table, maximum SSIM of 1.0000 is obtained for the proposed scheme, which means that the visual quality of the watermarked image is excellent. For the extracted watermark, our proposed method performs better than [52]

Attack	Image						
	Zelda	Lena	Goldhill	Peppers	Butterfly	Baboon	Lake
Gaussian Noise	 20.1432	 21.1377	 20.8396	 20.2903	 21.3645	 20.9658	 20.9635
Salt & Pepper Noise	 18.2875	 19.1788	 18.8515	 18.0719	 19.4086	 19.3897	 18.5991
Speckle Noise	 18.6774	 20.1882	 20.4104	 19.0156	 20.1676	 18.7338	 19.0666
Rotation (45°) + Crop	 10.0542	 10.0855	 9.5552	 7.8913	 9.3698	 10.4708	 8.7228
Cropping (TL1/4)	 11.8788	 11.5970	 10.3297	 12.1822	 10.7021	 11.9241	 10.8275
Translation 80 × 80	 7.6401	 8.5995	 7.4339	 7.8895	 8.2904	 9.4116	 8.1434
Histogram Equalization	 21.8884	 21.2714	 21.2714	 23.2649	 23.8514	 18.468	 25.3644
Rescaling	 34.7696	 33.7839	 30.7496	 31.057	 29.4468	 23.6147	 29.9531
Sharpening	 38.4032	 35.0200	 33.0937	 34.5253	 32.4733	 25.7684	 31.7031
Gaussian filter	 42.3672	 39.9859	 38.2391	 39.347	 37.6375	 31.6101	 37.6247

Fig. 7 The watermarked images and their corresponding PSNR values after sixteen attacks





Average filter	 34.8471	 31.7619	 29.6950	 31.4577	 29.7084	 23.2393	 29.5604
Median filter	 37.4769	 35.1215	 31.5749	 34.8100	 31.6155	 23.7148	 30.8524
Wiener filter	 39.0258	 37.2113	 33.9568	 36.4450	 34.3111	 27.3632	 33.7481
Gamma correction	 7.0992	 8.3902	 7.7648	 7.8011	 8.0157	 8.6986	 8.3188
Flipping of rows	 12.3190	 12.4341	 11.3620	 9.6407	 12.6012	 12.7869	 9.9762
Flipping of columns	 14.1621	 11.2974	 13.9777	 10.1896	 14.6125	 14.5999	 12.3968

Fig. 7 continued

by 1.24%, whereas is slightly lower than [49,57–59,63,65–70] with a very little difference of 0.0004 in terms of the NC metric.

In summary, with regard to the result of Fig 6, Tables 5 and 6 and the brief discussion, it is obvious that the proposed algorithm achieves good transparency whether for the watermarked image or the extracted watermark under no attack.

5.4 Proof of robustness

Robustness implies that how efficiently the watermark can be extracted from various intention or accidental types of attacks employed in the watermarked image. To test the robustness and reliability of the proposed method, sixteen common attacks are performed on watermarked images, and their descriptions are given in Table 1. Thus, to show the performance of our algorithm more intuitively, the seven watermarked images of the proposed algorithm are exposed to these attacks, the corrupted watermarked test images are shown in Fig. 7 and then the corresponding UIQI and NC

values of the extracted watermarks are given in Table 6. As illustrated in the table, the average values of UIQI and NC metrics for each extracted watermark remained above 0.88 and 0.999, respectively. Moreover, the proposed algorithm has strong resistance to sharpening, rotation+cropping (Rtc), cropping and other attacks. Even if the watermarked images are simultaneously rotated by 45° and cropped to fit the size of the input images, good watermarks can still be extracted, and the mean value of NC reaches 0.999. Still referring to Fig. 7 and Table 6, when the top-left corner of the watermarked images is cropped by 1/4, we have noticed that they are strongly distorted as their mean value of PSNR is under 13 dB; nevertheless, the extracted watermarks are easily identifiable according to the mean value of NC which is still greater than 0.999, while the mean value of UIQI reaches 0.97, which in turns indicate the high robustness of the system.

s

In order to ensure the fairness and show the advantage of the proposed scheme in terms of robustness, experimental

Table 6 UIQI and NC values of the watermarks extracted from the watermarked image under sixteen different attacks

Attack	Image																Average	
	Zelda		Lena		Goldhill		Peppers		Butterfly		Baboon		Lake		NC		UIQI	NC
	UIQI	NC	UIQI	NC	UIQI	NC	UIQI	NC	UIQI	NC	UIQI	NC	UIQI	NC	UIQI	NC	UIQI	NC
No attack	0.9776	0.9996	0.9774	0.9996	0.9771	0.9996	0.9777	0.9996	0.9768	0.9996	0.9773	0.9996	0.9773	0.9996	0.9773	0.9996	0.9773	0.9996
Gs	0.9159	0.9997	0.8994	0.9995	0.9042	0.9996	0.9010	0.9995	0.9233	0.9998	0.9052	0.9998	0.8987	0.9995	0.9068	0.9996	0.9068	0.9996
Slp	0.8957	0.9993	0.8728	0.9989	0.8755	0.9990	0.8674	0.9988	0.9047	0.9996	0.8872	0.9995	0.8612	0.9987	0.8806	0.9991	0.8806	0.9991
Spn	0.9063	0.9994	0.8944	0.9993	0.9114	0.9995	0.8889	0.9992	0.9175	0.9997	0.8770	0.9993	0.8896	0.9990	0.8978	0.9993	0.8978	0.9993
Ric	0.9805	0.9998	0.9547	0.9998	0.9469	0.9999	0.9616	0.9998	0.9738	0.9998	0.9315	0.9998	0.9539	0.9998	0.9575	0.9998	0.9575	0.9998
Cr	0.9759	0.9996	0.9753	0.9996	0.9749	0.9996	0.9720	0.9996	0.9732	0.9995	0.9602	0.9993	0.9728	0.9995	0.9720	0.9995	0.9720	0.9995
Tr	0.9741	0.9996	0.9713	0.9996	0.9659	0.9996	0.9619	0.9996	0.9488	0.9996	0.9272	0.9994	0.9469	0.9995	0.9566	0.9995	0.9566	0.9995
HE	0.9812	0.9997	0.9826	0.9998	0.9832	0.9998	0.9824	0.9998	0.9825	0.9998	0.9873	1.0000	0.9763	0.9998	0.9822	0.9998	0.9822	0.9998
Rsc	0.9655	0.9994	0.9655	0.9993	0.9599	0.9992	0.9515	0.9992	0.9319	0.9990	0.9131	0.9980	0.9424	0.9990	0.9471	0.9990	0.9471	0.9990
Shp	0.9815	0.9998	0.9850	0.9998	0.9849	0.9999	0.9848	0.9999	0.9793	0.9999	0.9845	1.0000	0.9850	0.9999	0.9835	0.9999	0.9835	0.9999
GF	0.9726	0.9995	0.9724	0.9995	0.9701	0.9994	0.9685	0.9994	0.9611	0.9993	0.9520	0.9990	0.9649	0.9993	0.9659	0.9993	0.9659	0.9993
Avg	0.9668	0.9994	0.9676	0.9993	0.9624	0.9992	0.9592	0.9992	0.9401	0.9991	0.9232	0.9982	0.9523	0.9991	0.9530	0.9990	0.9530	0.9990
Md	0.9701	0.9995	0.9729	0.9995	0.9677	0.9994	0.9677	0.9994	0.9621	0.9993	0.9425	0.9987	0.9636	0.9993	0.9638	0.9993	0.9638	0.9993
WF	0.9652	0.9995	0.9707	0.9995	0.9658	0.9994	0.9663	0.9994	0.9333	0.9993	0.9341	0.9989	0.9596	0.9993	0.9564	0.9993	0.9564	0.9993
Gc	0.9729	0.9995	0.9700	0.9994	0.9678	0.9994	0.9712	0.9995	0.9620	0.9992	0.9401	0.9986	0.9641	0.9993	0.9640	0.9992	0.9640	0.9992
Fpr	0.9776	0.9996	0.9772	0.9996	0.9774	0.9996	0.9777	0.9996	0.9768	0.9996	0.9773	0.9996	0.9771	0.9996	0.9773	0.9996	0.9773	0.9996
Fpc	0.9776	0.9996	0.9773	0.9996	0.9773	0.9996	0.9777	0.9996	0.9768	0.9996	0.9773	0.9996	0.9772	0.9996	0.9773	0.9996	0.9773	0.9996

and comparative results of NC values with other previous watermarking methods [49,52,58,59,66,67,71] for cover images ‘Lena’ and ‘Peppers’ are performed and compiled in Tables 7 and 8, respectively. From these tables, we briefly detail our observations of the behavior of these algorithms including our algorithm. It can be clearly seen that the proposed algorithm has strong robustness, especially against rotation+cropping (Rtc), cropping and translation attacks, and the NC value under each attack is greater than 0.9995. The performance of [49] to deal with the flipping of columns attack is better than that of the proposed algorithm, but this algorithm is less resistant to Gaussian noise, histogram equalization, rescaling, sharpening and gamma correction attacks than the proposed algorithm. NC values of the extracted watermarks computed only for ‘Lena’ image show that [52] is highly robust to histogram equalization and sharpening but performs poorly against salt and pepper noise, speckle noise, 45-degree rotation+cropping (Rtc), cropping, translation and denoising attacks. On the other hand, by calculating the average NC values for the two used test images, we surprisingly realized that our proposed scheme is superior to [52] method for all listed attacks. Moreover, the proposed algorithm outperforms [58,59,66] in each case. In terms of its resistance to the unique attack namely Gaussian filtering (GF), [67] shows stronger robustness than our algorithm, but for other attacks, the proposed algorithm is superior to [67].

As a remark, despite the fact that our watermarked images were undergo severe attacks, since we have set the parameters of the attacks with values greater than or equal to that used in the aforementioned watermarking techniques (see Tables 7 and 8 then compare data in parentheses), the proposed algorithm shows stronger resistance to sharpening, rotation+cropping (Rtc), and histogram equalization attacks, and has strong robustness under each attack.

5.5 Computational complexity

This section describes the computational complexity of the proposed approach in terms of big-Oh notation, where worst-case scenarios are considered. The complexity of digital image watermarking approaches is usually assessed in terms of required number of different operations. Let us remind the reader that we have introduced a grayscale image watermarking system using DWT-SVD domain. The complexity of the proposed watermarking scheme is therefore determined by analyzing independently the time complexity of these two frequency domains. Generally speaking, the time complexity of DWT of size $M \times N$ is $O(MN)$; the wavelet transforms incur lesser time complexity due to nice features of space-frequency localization and multiresolutions. Here, the size of cover image is $M \times N$ and the size of watermark image is $m \times n$, where $M = m$ and $N = n$. Further, the dimension of cover image in this scheme is the

same, i.e., $M = N$. So, the time complexity of DWT in our watermarking method is $T_{DWT|M=N} = O(M^2)$. On the other hand, the time complexity of SVD in general case requires $O(\min(M \times N^2, M^2 \times N))$, wherefore its complexity in the proposed scheme is $T_{SVD|M=N} = O(M^3)$. Therefore, the overall time complexity (T) for the presented algorithm is given by

$$T = T_{DWT|M=N} + T_{SVD|M=N} = O(M^3)$$

from which we deduce that this technique has cubic complexity. All in all, according to the chosen solution, the moderate computational complexity and the high results in terms of imperceptibility and robustness make the proposed approach practical for real-time applications.

5.6 Capacity analysis

In this section, we provide a detailed analysis of the capacity of the proposed watermarking algorithm and compare it with other seven related algorithms [72–78]. The capacity of a watermarking algorithm is defined as the ratio of the number of bits contained in the maximum embeddable watermark to the number of pixels in the cover image. In the proposed watermarking algorithm, the 8 bits grayscale watermark image of size 512×512 is embedded in the cover image of size 512×512 . The number of bits contained in this watermark is $512 \times 512 \times 8 = 2097152$, so the capacity of our algorithm is $2097152 / (512 \times 512) = 8$. Table 9 gives the capacity of the proposed algorithm and those of the related comparison algorithms [72–78]. From Table 9, we can see that [72,73] and [77] have the same capacity, namely 0.015625, and the capacity of the proposed algorithm is 512 times that of these three algorithms. Moreover, our algorithm is superior to [74,75] and [76] in terms of capacity, whereas it has the same capacity as [78]. In brief, our algorithm has a large capacity.

5.7 Comparative analysis

Based on the sizes and types of the cover image and the watermark image, the comparison results of the proposed algorithm and those of the main related algorithms [72–78] are given in Table 10. It can be concluded from the table that all the algorithms use 512×512 grayscale images as the cover image; the proposed algorithm and the algorithms in [74–76,78] use grayscale watermarks, while [72,73] and [77] are only applicable to binary watermark images. [73,74] embed watermarks into some selected blocks of the redistributed invariant discrete wavelet transform (RIDWT), wherefore [74], in particular, did not well satisfy the invisibility requirement. [76] embeds watermarks in the integer wavelet transform (IWT), whereas [78] uses a DCT on the

Table 7 Comparison of NC values of the extracted watermark computed for ‘Lena’ image under different types of attacks

Attack index	Agoyi et al. [49]	Ernawan et Kabir [52]	Verma et al. [58]	Wang and Zhao [59]	Hu et al. [66]	Kang et al. [67]	Gong et al. [71]	Proposed method
Gs (0.01)	0.6362	0.9614 (0.005)	0.8320 (0.05)	0.9983 (0.001)	0.939 (0.005)	0.8142	0.9769 (0.001)	0.9995
Slp (0.05)	-	0.9309 (0.03)	0.9141 (0.01)	0.9868 (0.01)	0.983	0.8386 (0.02)	0.9502 (0.005)	0.9989
Spn (0.05)	-	0.8451 (0.04)	0.9102 (0.01)	0.9955 (0.01)	0.980 (0.005)	0.8075	0.9631 (0.005)	0.9993
Rtc (45°)	-	0.4941 (2°)	0.7305 (5°)	0.3928	-	-	-	0.9998
Cr (1/4)	-	0.8048	0.9922 (10%)	-	-	0.9574	0.9964 (1/16)	0.9996
Tr (80 × 80)	-	0.4128 (10, 10)	0.7891 (2, 15)	-	-	-	-	0.9996
HE (64)	0.9776	1.0000	0.9336	0.8176	0.962	0.9953	0.9495	0.9998
Rsc (0.5)	-0.6178	0.9922	0.9453	0.9977	0.6408	0.9987	0.9946	0.9993
Shp (1, 0.8)	0.4561	1.0000	0.9648	0.9891	-	0.9993	-	0.9998
GF (3 × 3), 0.5	-	0.9346	0.9570	0.9959	-	1.0000	0.9754	0.9995
Avg (3 × 3)	-	0.9346	0.8633	-	-	0.9641	-	0.9993
Md (3 × 3)	-	0.9377	0.9258	0.9971	0.956	0.9967	0.9928	0.9995
WF (3 × 3)	-	-	-	-	-	-	-	0.9995
Gc (0.2)	0.981	-	-	0.7637	-	-	-	0.9994
Fpr (1)	-	-	-	-	-	-	-	0.9996
Fpc (2)	1	-	-	-	-	-	-	0.9996

The horizontal bar indicates that there are no relevant data in the corresponding paper. The data in parentheses represent the parameters of the attacks. Bold values represent the data with the best comparison results

Table 8 Comparison of NC values of the extracted watermark computed for ‘Peppers’ image under different types of attacks. The horizontal bar indicates that there is no relevant data in the corresponding paper. The data in parentheses represent the parameters of the attacks. Bold values represent the data with the best comparison results

Attack index	Agoyi et al. [49]	Emawan and Kabir [52]	Verma et al. [58]	Wang and Zhao [59]	Hu et al. [66]	Kang et al. [67]	Gong et al. [71]	Proposed method
Gs (0.01)	0.6684	0.8928 (0.005)	0.8008 (0.05)	0.9986 (0.001)	0.904 (0.005)	0.8052	0.9646 (0.001)	0.9995
Slp (0.05)	-	0.8883 (0.03)	0.9102 (0.01)	0.9782 (0.01)	0.982	0.8544 (0.02)	0.9611 (0.005)	0.9988
Spn (0.05)	-	0.8398 (0.04)	0.8906 (0.01)	0.9964 (0.01)	0.995 (0.005)	0.8166	0.9982 (0.005)	0.9992
Rtc (45°)	-	0.4986 (2°)	0.7227 (5°)	0.1365	-	-	-	0.9998
Cr (1/4)	-	0.8544	0.9727 (10%)	-	-	0.9588	0.9302 (1/16)	0.9996
Tr (80 × 80)	-	0.4713 (10, 10)	0.7773 (2, 15)	-	-	-	-	0.9996
HE (64)	0.8968	0.9743	0.9375	0.8579	-	0.9960	1	0.9998
Rsc (0.5)	-0.5945	0.9072	0.9414	0.9942	-	0.9987	0.9786	0.9992
Slp (1, 0.8)	0.9926	0.9883	0.9766	0.9877	-	0.9993	-	0.9999
GF (3 × 3), 0.5	-	0.9536	0.9609	0.9955	-	1.0000	0.9498	0.9994
Avg (3 × 3)	-	-	0.8594	-	-	0.9723	-	0.9992
Md (3 × 3)	-	0.9190	0.9180	0.998	-	0.9765	0.9911	0.9994
WF (3 × 3)	-	-	-	-	-	-	-	0.9994
Gc (0.2)	0.9921	-	-	0.7647	-	-	-	0.9995
Fpr (1)	-	-	-	-	-	-	-	0.9996
Fpc (2)	1	-	-	-	-	-	-	0.9996

Table 9 Capacity comparison between the proposed algorithm and related algorithms

Metric	Ali et al. [72]	Ali et al. [73]	Ali et al. [74]	Ansari et al. [75]	Makbol et al. [76]	Roy et al. [77]	Li et al. [78]	Proposed method
Size of cover image	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512
Number of bits in the maximum embeddable watermark	4096	4096	32768	131072	524288	4096	2097152	2097152
Capacity (b/p)	0.015625	0.015625	0.125	0.5	2	0.015625	8	8

Table 10 Comparative analysis of the proposed algorithm and other related algorithms

Metric	Ali et al. [72]	Ali et al. [73]	Ali et al. [74]	Ansari et al. [75]	Makbol et al. [76]	Roy et al. [77]	Li et al. [78]	Proposed method
Size of cover image	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512
Type of cover image	Gray	Gray	Gray	Gray	Gray	Gray	Gray	Gray
Size of watermark	64 × 64	32 × 32	64 × 64	128 × 128	256 × 256	64 × 64; 128 × 32	64 × 64	512 × 512
Type of watermark	Binary	Binary	Gray	Gray	Gray	Binary	Gray	Gray
Transform domain	RIDWT + DWT + FRFT + SVD	RIDWT + SVD	RIDWT + SVD	DWT + SVD	IWT + SVD	RDWT + DCT	RIDWT + DCT+ SVD	DWT + SVD
Embedding sub-bands	LL_1	Some blocks of LL	Some blocks of LL	All sub-bands	LL_1	8 × 8 blocks	LL_1 and HH_1	HH_1
Signal quality	Good	Good	Acceptable	Good	Good	Good	Good	Excellent
Invisibility (PSNR)	41.8765	41.8765	29.5839	38.4103	41.2234	41.3464	41.9616	48.1308
Capacity (b/p)	0.015625	0.015625	0.125	0.5	2	0.015625	8	8

basis of the RIDWT, and selects low-frequency and high-frequency regions for embedding watermarks; both schemes, despite competitiveness, have less invisibility than the proposed algorithm. Differently, the proposed algorithm and [75] embed watermarks in the discrete wavelet domain, but this algorithm uses a blend of DWT-SVD domain, and selects high-frequency region for embedding watermarks, which results higher robustness. Obviously, the proposed algorithm has higher reliability and invisibility. Moreover, except for [78] with which we are equal, the proposed algorithm is superior to the other algorithms in terms of capacity.

6 Conclusions and future work

In this paper, a revisited hybrid watermarking technique based on DWT and SVD has been presented to achieve simultaneously the trade-off between robustness and invisibility. At the sender side, the one-level DWT is used to decompose the original image to seek for the embedding position and then the watermark is inserted. Some key parameters are transmitted through a private channel to later recover the watermark image. At the receiver end, our system can recognize if the received watermarked image is attacked or not by computing Cr value. The use of the scaling factor is mandatory for extracting watermark from merely watermarked image; otherwise, the watermark is correctly and efficiently extracted from the watermarked attacked image as long as the scaling factor is no longer used. Comprehensive performance analysis of the proposed scheme is conducted including imperceptibility analysis, robustness analysis, computational complexity and capacity analysis. The proposed approach has been implemented with acceptable computational complexity of $O(M)^3$. This result remains encouraging and ensures that the proposed approach would be practical for real time processes. Besides that, experimental results of the proposed algorithm clearly account for high level of robustness, security, reliability and imperceptibility, so it can be used for copyright protection and content authentication.

The limitations of this paper and future research directions are given below. First, as watermarking is carried out in HH sub-band, robustness of the proposed scheme against salt and pepper attack is moderate. We see, as well, some future directions for our work. Our algorithm is designed for gray cover images and watermarks, and it is not suitable for binary watermarks. Based on the proposed watermarking algorithm, the study of watermarking algorithms for embedding binary watermarks is a first direction for future research. Second, we will also work on hiding multiple grayscale or binary watermarks into the gray cover image for more flexibility.

Acknowledgements The authors would like to sincerely thank Nadia Magneat Thalmann, Ph.D. Editor-in-Chief, and three anonymous

reviewers who gave insightful comments and helpful suggestions that improved the technical and editorial quality of this paper. This work is an independent work and did not receive any funding from any agency either directly or indirectly.

Declaration

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Tarhouni, N., Charfeddine, M., Amar, C.B.: Novel and robust image watermarking for copyright protection and integrity control. *Circuits Syst. Signal Process.* **39**(10), 5059–5103 (2020)
2. Murali, P., Niranjana, G., Paul, A.J., Muthu, J.S.: Domain-flexible selective image encryption based on genetic operations and chaotic maps. *The Visual Computer*, pp. 1–23, (2022)
3. Wang, X., Su, Y., Zhang, H., Zou, C.: A new hybrid image encryption algorithm based on Gray code transformation and snake-like diffusion. *The Visual Computer*, pages 1–22, (2021)
4. Benrhouma, O., Hermassi, H., El-Latif, A., Ahmed, A., Belghith, S.: Chaotic watermark for blind forgery detection in images. *Multimed. Tools Appl.* **75**(14), 8695–8718 (2016)
5. Belazi, A., Abd El-Latif, A.A., Rhouma, R., Belghith, S.: Selective image encryption scheme based on DWT, AES S-box and chaotic permutation. In: 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 606–610. IEEE, (2015)
6. Liao, X., Li, K., Zhu, X., Liu, K.R.: Robust detection of image operator chain with two-stream convolutional neural network. *IEEE J. Selected Topics Signal Process.* **14**(5), 955–968 (2020)
7. Zhang, L., Xiao, J.-W., Luo, J.Y.: A robust color image watermarking based on SVD and DWT. *Int. J. Commun. (IJC)* **3**, 62 (2014)
8. Sahu, A.K., Swain, G.: An optimal information hiding approach based on pixel value differencing and modulus function. *Wireless Pers. Commun.* **108**(1), 159–174 (2019)
9. Ouhsein, M., Hamza, A.B.: Image watermarking scheme using nonnegative matrix factorization and wavelet transform. *Expert Syst. Appl.* **36**(2), 2123–2129 (2009)
10. Mohammad, A.A., Alhaj, A., Shaltaf, S.: An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Process.* **88**(9), 2158–2180 (2008)
11. Phadikar, A., Maity, S.P., Verma, B.: Region based QIM digital watermarking scheme for image database in DCT domain. *Comput. Elect. Eng.* **37**(3), 339–355 (2011)
12. Lu, W., Lu, H., Chung, F.-L.: Feature based robust watermarking using image normalization. *Comput. Elect. Eng.* **36**(1), 2–18 (2010)
13. Moeinaddini, E., Ghasemkhani, R.: A novel image watermarking scheme using blocks coefficient in DHT domain. In: 2015 The International Symposium on Artificial Intelligence and Signal Processing (AISP), pp. 159–164. IEEE, (2015)
14. Vali, M.H., Aghagolzadeh, A., Baleghi, Y.: Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition. *Expert Syst. Appl.* **114**, 296–312 (2018)
15. Kumar, S., Dutta, A.: Performance analysis of spatial domain digital watermarking techniques. In: 2016 International Conference on Information Communication and Embedded Systems (ICICES), pp. 1–4. IEEE (2016)

16. Ali, M., Ahn, C.W., Pant, M.: A robust image watermarking technique using SVD and differential evolution in DCT domain. *Optik* **125**(1), 428–434 (2014)
17. Peng, J., Abd El-Atty, B., Khalifa, H.S., Abd El-Latif, A.A.: Image watermarking algorithm based on quaternion and chaotic Lorenz system. In: Eleventh International Conference on Digital Image Processing (ICDIP 2019), volume 11179, pp. 111790W. International Society for Optics and Photonics (2019)
18. Hussain, M., Wahab, A.W.A., Idris, Y.I.B., Ho, A.T., Jung, K.-H.: Image steganography in spatial domain: A survey. *Signal Process. Image Commun.* **65**, 46–66 (2018)
19. Wu, N.-I., Hwang, M.-S.: A novel LSB data hiding scheme with the lowest distortion. *Imag. Sci. J.* **65**(6), 371–378 (2017)
20. Sahu, A.K., Swain, G.: An improved data hiding technique using bit differencing and LSB matching. *Internetwork. Indonesia J.* **10**(1), 17–21 (2018)
21. Wu, D.-C., Tsai, W.-H.: A steganographic method for images by pixel-value differencing. *Pattern Recogn. Lett.* **24**(9–10), 1613–1626 (2003)
22. Swain, G.: Adaptive pixel value differencing steganography using both vertical and horizontal edges. *Multimed. Tools Appl.* **75**(21), 13541–13556 (2016)
23. Akhila, L., Manoj, V.: Image Steganography using Pixel Value Differencing with Modulus Function and Optimization. In: 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 1369–1373. IEEE (2022)
24. Liu, H.-H., Lin, Y.-C., Lee, C.-M.: A digital data hiding scheme based on pixel-value differencing and side match method. *Multimed. Tools Appl.* **78**(9), 12157–12181 (2019)
25. Wu, H.-C., Wu, N.-I., Tsai, C.-S., Hwang, M.-S.: Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEE Proc.-Vis. Image Signal Process.* **152**(5), 611–615 (2005)
26. Hussain, M., Riaz, Q., Saleem, S., Ghafoor, A., Jung, K.-H.: Enhanced adaptive data hiding method using LSB and pixel value differencing. *Multimed. Tools Appl.* **80**(13), 20381–20401 (2021)
27. Singh, S.: Adaptive PVD and LSB based high capacity data hiding scheme. *Multimed. Tools Appl.* **79**(25), 18815–18837 (2020)
28. Swain, G.: Very high capacity image steganography technique using quotient value differencing and LSB substitution. *Arab. J. Sci. Eng.* **44**(4), 2995–3004 (2019)
29. Yasmeen, F., Uddin, M.S.: An efficient watermarking approach based on LL and HH edges of DWT-SVD. *SN Comput. Sci.* **2**(2), 1–16 (2021)
30. Makbol, N.M., Khoo, B.E., Rassem, T.H.: Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Proc.* **10**(1), 34–52 (2015)
31. Ahmadi, S.B.B., Zhang, G., Wei, S., Boukela, L.: An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics. *Vis. Comput.* **37**(2), 385–409 (2021)
32. Ansari, I.A., Pant, M., Ahn, C.W.: PSO optimized and secured watermarking scheme based on DWT and SVD. In: Proceedings of Fifth International Conference on Soft Computing for Problem Solving, pp. 411–424. Springer (2016)
33. Zear, A., Singh, A.K., Kumar, P.: A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimed. Tools Appl.* **77**(4), 4863–4882 (2018)
34. Liu, Y., Tang, S., Liu, R., Zhang, L., Ma, Z.: Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Syst. Appl.* **97**, 95–105 (2018)
35. Singh, R.K., Shaw, D.K., Sahoo, J.: A secure and robust block based DWT-SVD image watermarking approach. *J. Inf. Optim. Sci.* **38**(6), 911–925 (2017)
36. Naik, N. S., Naveena, N., Manikantan, K.: Robust digital image watermarking using DWT+ SVD approach. In: 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICIC), pp. 1–6. IEEE (2015)
37. Furqan, A., Kumar, M.: Study and analysis of robust DWT-SVD domain based digital image watermarking technique using MATLAB. In: 2015 IEEE International Conference on Computational Intelligence & Communication Technology, pp. 638–644. IEEE (2015)
38. Liao, X., Yu, Y., Li, B., Li, Z., Qin, Z.: A new payload partition strategy in color image steganography. *IEEE Trans. Circuits Syst. Video Technol.* **30**(3), 685–696 (2019)
39. Moran, M. B., Ochi, L. S., Conci, A., Araujo, A., Muchaluat-Saade, D. C.: Iterated local search for RGB image steganography. In: 2018 25th International conference on systems, signals and image processing (IWSSIP), pp. 1–5. IEEE (2018)
40. Liao, X., Chen, G., Yin, J.: Content-adaptive steganalysis for color images. *Security Commun. Netw.* **9**(18), 5756–5763 (2016)
41. Liao, X., Yin, J., Chen, M., Qin, Z.: Adaptive payload distribution in multiple images steganography based on image texture features. *IEEE Trans. Depend. Secure Comput.* (2020)
42. Mallat, S.G.: A theory for multiresolution signal decomposition: the wavelet representation. *IEEE Trans. Pattern Anal. Mach. Intell.* **11**(7), 674–693 (1989)
43. Wang, M.-S., Chen, W.-C.: A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography. *Comput. Stand. Interf.* **31**(4), 757–762 (2009)
44. Cui, X., Niu, Y., Zheng, X., Han, Y.: An optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image. *PLoS ONE* **13**(5), e0196306 (2018)
45. Andrews, H., Patterson, C.: Singular value decomposition (SVD) image coding. *IEEE Trans. Commun.* **24**(4), 425–432 (1976)
46. Konstantinides, K., Natarajan, B., Yovanof, G.S.: Noise estimation and filtering using block-based singular value decomposition. *IEEE Trans. Image Process.* **6**(3), 479–483 (1997)
47. Chung, K.-L., Yang, W.-N., Huang, Y.-H., Wu, S.-T., Hsu, Y.-C.: On SVD-based watermarking algorithm. *Appl. Math. Comput.* **188**(1), 54–57 (2007)
48. Kadian, P., Arora, N., Arora, S. M.: Performance evaluation of robust watermarking using DWT-SVD and RDWT-SVD. In: 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 987–991. IEEE (2019)
49. Agoyi, M., Çelebi, E., Anbarjafari, G.: A watermarking algorithm based on chirp z-transform, discrete wavelet transform, and singular value decomposition. *SIVIP* **9**(3), 735–745 (2015)
50. Al-Mansoori, S., Kunhu, A.: Robust watermarking technique based on DCT to protect the ownership of Dubaisat-1 images against attacks. *Int. J. Comput. Sci. Netw. Security (IJCSNS)* **12**(6), 1 (2012)
51. Mohamed, M., El-Mohandes, A.: Hybrid DCT-DWT watermarking and idea encryption of internet contents. *Int. J. Comput. Sci. Issues (IJCSI)* **9**(1), 394–401 (2012)
52. Ernawan, F., Kabir, M.N.: A block-based RDWT-SVD image watermarking method using human visual system characteristics. *Vis. Comput.* **36**(1), 19–37 (2020)
53. Wang, Z., Bovik, A.C.: A universal image quality index. *IEEE Signal Process. Lett.* **9**(3), 81–84 (2002)
54. Hemdan, E., El Fishawy, N., Attiya, G., El-Samie, F.: An efficient image watermarking approach based on wavelet fusion and singular value decomposition in wavelet domain. In: Proceeding of 3rd International Conference on Advanced Control Circuits And Systems (ACCS'013), number 1-10, (2013)
55. Computer vision group. Dataset of standard 512×512 grayscale test images. <https://ccia.ugr.es/cvg/CG/base.htm>. Accessed: 03-2022

56. The waterloo fractal coding and analysis group. Image repository. <https://links.uwaterloo.ca/Repository.html>. Accessed: 03-2022
57. Begum, M., Uddin, M.S.: Implementation of secured and robust DFT-based image watermark through hybridization with decomposition algorithm. *SN Comput. Sci.* **2**(3), 1–13 (2021)
58. Verma, V.S., Jha, R.K., Ojha, A.: Digital watermark extraction using support vector machine with principal component analysis based feature reduction. *J. Vis. Commun. Image Represent.* **31**, 75–85 (2015)
59. Wang, B., Zhao, P.: An adaptive image watermarking method combining SVD and Wang-Landau sampling in DWT domain. *Mathematics* **8**(5), 691 (2020)
60. Wang, T.: Digital image watermarking using dual-scrambling and singular value decomposition. In: 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), vol. 1, pp. 724–727. IEEE (2017)
61. Salama, A.S. Mokhtar, M.A.: Combined technique for improving digital image watermarking. In: 2016 2nd IEEE International Conference on Computer and Communications (ICCC), pp. 557–562. IEEE, (2016)
62. Das, C., Panigrahi, S., Sharma, V.K., Mahapatra, K.: A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. *AEU-Int. J. Electron. Commun.* **68**(3), 244–253 (2014)
63. Khare, P., Srivastava, V.K.: A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT. *J. Intell. Syst.* **30**(1), 297–311 (2021)
64. Takore, T.T., Kumar, P.R., Devi, G.L.: A robust and oblivious grayscale image watermarking scheme based on edge detection, SVD, and GA. In: Proceedings of 2nd International Conference on Micro-Electronics, Electromagnetics and Telecommunications, pp. 51–61. Springer (2018)
65. Ray, A.K., Padhiary, S., Patra, P.K., Mohanty, M.N.: Development of a new algorithm based on SVD for image watermarking. In: Computational Vision and Robotics, pp. 79–87. Springer (2015)
66. Hu, K., Wang, X., Hu, J., Li, D., Du, L., Wang, H., Qin, H.: Robust and efficient image watermarking via EMD and dimensionality reduction. *The Visual Computer*, pp. 1–18 (2021)
67. Kang, X.-B., Zhao, F., Lin, G.-F., Chen, Y.-J.: A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength. *Multimed. Tools Appl.* **77**(11), 13197–13224 (2018)
68. Kazemivash, B., Moghaddam, M.E.: A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm. *Multimedia Tools Appl.* **76**(20), 20499–20524 (2017)
69. Kazemivash, B., Moghaddam, M.E.: A predictive model-based image watermarking scheme using Regression Tree and Firefly algorithm. *Soft. Comput.* **22**(12), 4083–4098 (2018)
70. Moeinaddini, E., Afsari, F.: Robust watermarking in DWT domain using SVD and opposition and dimensional based modified firefly algorithm. *Multimed. Tools Appl.* **77**(19), 26083–26105 (2018)
71. Gong, L.-H., Tian, C., Zou, W.-P., Zhou, N.-R.: Robust and imperceptible watermarking scheme based on Canny edge detection and SVD in the contourlet domain. *Multimed. Tools Appl.* **80**(1), 439–461 (2021)
72. Ali, M., Ahn, C.W., Pant, M.: An efficient lossless robust watermarking scheme by integrating redistributed invariant wavelet and fractional Fourier transforms. *Multimed. Tools Appl.* **77**(10), 11751–11773 (2018)
73. Ali, M., Ahn, C.W., Pant, M., Siarry, P.: An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. *Inf. Sci.* **301**, 44–60 (2015)
74. Ali, M., Ahn, C. W., Pant, M., Siarry, P.: A reliable image watermarking scheme based on redistributed image normalization and SVD. *Discrete Dynam. Nature Soc.*, **2016**, (2016)
75. Ansari, I.A., Pant, M.: Multipurpose image watermarking in the domain of DWT based on SVD and ABC. *Pattern Recogn. Lett.* **94**, 228–236 (2017)
76. Makbol, N.M., Khoo, B.E., Rassem, T.H., Loukhaoukha, K.: A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. *Inf. Sci.* **417**, 381–400 (2017)
77. Roy, S., Pal, A.K.: A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling. *Multimed. Tools Appl.* **76**(3), 3577–3616 (2017)
78. Li, Y.-M., Wei, D., Zhang, L.: Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain. *Inf. Sci.* **551**, 205–227 (2021)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Seif Eddine Naffouti has received the Engineering and the M.S. degrees in Electrical Engineering from the National Engineering School of Monastir (ENIM), University of Monastir, Tunisia, in 2012 and 2013, respectively, and the Ph.D. degree in Electrical Engineering and in Instrumentation & Image computing from ENIM and University of Burgundy, France, both in 2018. He is currently an assistant professor at the National Engineering School of Tunis (ENIT), University of Tunis El-Manar, Tunisia. His current research interests include mainly 3D pattern recognition and matching for intelligent computer vision systems, computer graphics, and image processing.



Anis Kricha received the engineering degree in electrical engineering, the DEA degree in automatic and signal processing as well as the Ph.D. degree in electrical engineering from the National Engineering School of Tunis (ENIT) in 2001 2004, and 2012, respectively. From 2006 to 2012, he was working as an assistant professor in the Department of Electrical Engineering in the National Engineering School of Monastir (ENIM), University of Monastir, Tunisia. Since 2013, he

has been an associate professor in the same school in signal and image processing. He is a member of the Laboratory of Advanced Technology and Intelligent Systems (LATIS). His research interests include mainly image processing, watermarking, computer vision, segmentation, compression, pattern recognition, artificial intelligence, document analysis and recognition.



Anis Sakly has received the Diploma degree in electrical engineering from the National Engineering School of Monastir (ENIM) in 1994 and the Ph.D. degree in electrical engineering from the National Engineering School of Tunis in 2005. He is currently a Professor with ENIM. His research interests are in the analysis and synthesis of intelligent control systems, particularly soft computing-based control approaches.