



# A robust image watermarking scheme in hybrid transform domains resisting to rotation attacks

Peijia Zheng<sup>1,2</sup>  · Yonghong Zhang<sup>1</sup>

Received: 22 December 2018 / Revised: 29 October 2019 / Accepted: 19 November 2019 /  
Published online: 3 March 2020  
© Springer Science+Business Media, LLC, part of Springer Nature 2020

## Abstract

Image watermarking provides a promising solution to digital media copyright protection. However, the robust performance of the watermarking scheme should be carefully considered. In this paper, we propose a robust image watermarking scheme, which shows good robustness against common watermarking attacks and rotation attacks. The hybrid method based on discrete wavelet transform (DWT) and discrete cosine transform (DCT) helps concentrate the image energy and improve the robust performance of the image watermarking scheme. Besides, the employment of singular value decomposition (SVD) makes the proposed scheme more robust against rotation attack. We conduct experiments on the visual quality and the robustness of our watermarking scheme. The experimental results are generally satisfactory.

**Keywords** Image watermarking · Robust watermarking · Rotation attack · Singular value decomposition (SVD)

## 1 Introduction

Digital watermarking is an important technique for copyright protection, traitor tracing, authentication, secretive communication, etc., by hiding proprietary information in digital media. Cryptographic techniques permit only valid key holders access to encrypted data. However, once the encrypted data is decrypted, it is not able to track its reproduction or retransmission. Thus, digital watermarking has been proposed to complement cryptographic techniques. Over the years, digital watermarking, especially image watermarking, has received considerable attention from researchers in the fields of data hiding.

---

✉ Peijia Zheng  
zhpj@mail.sysu.edu.cn

Yonghong Zhang  
zhangyh267@mail2.sysu.edu.cn

<sup>1</sup> School of Data and Computer Science, Sun Yat-Sen University, Guangzhou, 510006, China

<sup>2</sup> Guangdong Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou, 510006, China

In general, we can classify digital watermarking schemes into two groups: fragile and robust watermarking schemes. Fragile watermarking schemes [26, 27] are fragile to most modifications and therefore used in content authentication and integrity attestation. In contrast, robust watermarking schemes [2, 4, 29] that are robust to most kinds of image processing operations, are generally used in ownership verification and copyright protection of digital media. Besides, according to the embedding domain of the host image, we can group digital watermarking schemes into two types: spatial domain and frequency domain watermarking schemes. The spatial domain watermarking schemes carry out watermark embedding via modifying the intensities of image pixels. However, those watermarking schemes are not very robust against most of the image process operations. On the contrary, the frequency domain watermarking schemes are more popular in digital watermarking, due to the stronger robustness against the common kinds of watermarking attacks. The frequency-domain watermarking techniques convert the host media into frequency coefficients with available transform methods. Generally, watermarks embedded in the transform domain are more robust and less perceptible, compared with the spatial domain watermarking schemes. Various frequency domains have been utilized in digital watermarking schemes, including DCT [7, 8, 20, 22, 33, 35], DFT [3–5], DWT [1, 9, 17, 31, 34], and SVD [2, 13, 28, 30], etc.

In addition, watermarking schemes can also be divided into blind and non-blind watermarking schemes based on the mechanisms of watermark extraction. For a watermarking scheme, if an original image is necessary for the watermark extraction algorithm, we call it non-blind watermarking scheme; otherwise, we call it blind watermarking scheme.

There are numerous new approaches proposed for image watermarking. In [11], Golea et al. designed a color image watermarking by using SVD. Lin et al. [21] proposed a hierarchical fragile image watermarking scheme for content recovery and tampering detection. In [19], Lee et al. developed a dual watermark technique for both recovery and image tampering detection, which can recover an acceptable original image when the watermarked image is damaged for the first time. Jia [16] proposed a color image watermarking algorithm based on SVD. Lee et al. designed a blind watermarking scheme based on the DCT domain in [18], which is robust against cropping and JPEG compression. Patra et al. [25] suggested a DCT-domain watermarking scheme by using the Chinese Remainder Theorem, which is reported to be robust against JPEG compression and cropping except for several noise attacks. In [6], Chen et al. presented an image watermarking encryption scheme based on the fractional Fourier transform. Guo et al. [14] proposed a robust image watermarking scheme based on DWT and DCT. It is reasonable to investigate the robustness against various attacks, including noise attacks, compression attacks, and rotation attacks at the same time. Thus, designing an image watermarking scheme resisting these attacks is still very meaningful.

In this paper, we propose a robust image watermarking against different attacks, especially rotation attacks. Existing robust image watermarking schemes have achieved good robustness under the geometric distortions, common image processing operations, etc. However, the design of robust image watermarking against rotation attacks still deserves our attention. To improve the robustness, we choose to embed a watermark in the transform domain rather than the spatial domain. The DWT has the characteristic of excellent spatial localization and multi-resolution properties. After applying DWT or DCT to an image, most significant information of the image is concentrated on the upper left corner of the coefficient matrix. Considering the robustness against rotation attacks, we also choose SVD to extract rotation-invariant features for watermark embedding. Hence, we propose to embed a watermark in hybrid transform domains of the DWT, the DCT, and the SVD. Specifically, we embed the watermark in the low-frequency coefficients to ensure the robustness

of watermark and use an image splitting method to improve the visual quality of the watermarked images. After performing DWT on the image, we split the coefficients into blocks by downsampling and then apply DCT to these blocks. The watermark is embedded by replacing some coefficients. Taking advantage of the energy compaction characteristics of DWT and DCT and the similarity of adjacent coefficient blocks, the watermark is robust and transparent.

However, most SVD-based watermarking schemes will cause a false positive problem (FPP) due to embedding watermarking into the singular matrix direct or indirect. By applying SVD, the main features of images are contained in singular vector matrices rather than the singular value matrix that only indicate the brightness information of the original image. Therefore, an attacker can use other singular vector matrices to get a false watermark and claim ownership. In this paper, to solve this problem, we adopt a signature-based authentication mechanism to check the fidelity of the watermarked image.

The remainder of this paper is organized as follows. Section 2 gives some introductions on the DWT, the DCT, and the SVD. In Section 3, we detail the proposed robust image watermarking scheme. Section 4 shows some experiments on visual quality and robustness. Finally, we conclude our paper in Section 5.

## 2 Different transform domains of images

In this section, we briefly summarize some important techniques employed in our watermarking scheme, including the DWT, the DCT, and the SVD.

### 2.1 Discrete wavelet transform

The DWT is a very popular mathematical tool used in the field of signal processing. By using different wavelet bases and decomposition levels, the DWT can extract various kinds of information related to frequency and location from the input signal. The implementation of the DWT is usually carried out through Mallat's algorithm [24]. Let us use  $\mathbf{x} = \{x_1, x_2, \dots, x_n\}$  to represent the input one-dimensional signal, where  $n$  is the length of the  $\mathbf{x}$ . Suppose that  $h_d(k)$  and  $g_d(k)$  are the low-pass and the high-pass decomposition filter coefficients, respectively. According to Mallat's algorithm [24], the recursive definition of the DWT can be given as

$$c_j(k) = \frac{1}{\sqrt{2}} \sum_{l \in \mathbb{Z}} h_d(2k-1)c_{j-1}(l) \quad (1)$$

$$d_j(k) = \frac{1}{\sqrt{2}} \sum_{l \in \mathbb{Z}} g_d(2k-1)c_{j-1}(l) \quad (2)$$

where  $j$  represents the decomposition level of the DWT,  $c_j(k)$  and  $d_j(k)$  are the approximation and the detail wavelet coefficients, respectively. In particular, the initial wavelet transform coefficient sequence  $\{c_0(l)\}_l$  is defined as the input signal  $\mathbf{x}$ .

Suppose that  $h_r(k)$  and  $g_r(k)$  are the low-pass and the high-pass reconstruction filter coefficients, respectively. For the inverse DWT (IDWT), according to the fast algorithm proposed by Mallat [24], we can recursively compute as

$$c'_j(k) = \frac{1}{\sqrt{2}} \sum_{l \in \mathbb{Z}} h_r(k-2l)c'_{j+1}(l) + g_r(k-2l)d'_{j+1}(l) \quad (3)$$

where  $c'_j(k)$  and  $d'_j(k)$  are the approximation and the detail wavelet coefficients in the  $j$ -level reconstruction, respectively. We sketch the block diagrams for the two-level DWT and IDWT in Fig. 1.

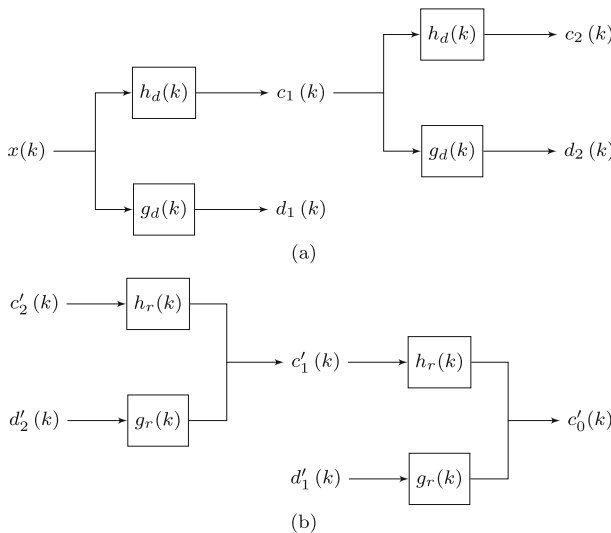
We will focus on the case that the input signal is an image in the rest of this paper. After performing the DWT, the input image will be divided into four frequency subbands, namely low-frequency subband ( $LL$ ), horizontal-frequency subband ( $HL$ ), vertical-frequency subband ( $LH$ ), and diagonal-frequency subband ( $HH$ ). Generally, the low-frequency subband concentrates most of the energy of the original image. The leveled decomposition of the DWT is then performed on the basis of low-frequency subband. Specifically, the  $j$ -level DWT decomposition takes the  $(j - 1)$ -level low-frequency subband as input, which is detailed in (1)-(2). We show the example of the first-order wavelet decomposition in Fig. 2b, where the original image is the Lena image.

### 2.2 Discrete cosine transform

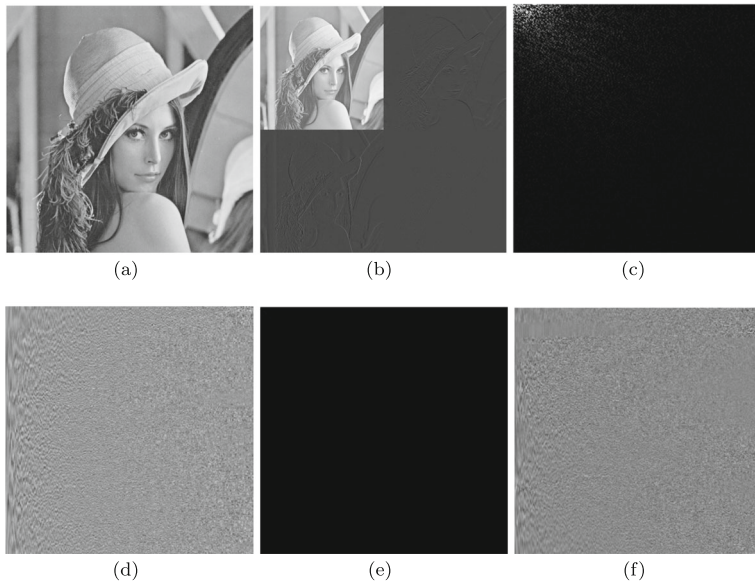
The DCT is also an important tool for numerous applications in science and engineering, particularly for digital signal processing. The DCT-II is the most commonly used form of the DCT, the formula of two-dimensional DCT-II as

$$F(u, v) = \beta(u)\beta(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i, j) \cos \left[ \frac{(i + 0.5)\pi}{N} u \right] \cos \left[ \frac{(j + 0.5)\pi}{N} v \right] \quad (4)$$

$$\beta(u) = \begin{cases} \sqrt{\frac{1}{N}}, & u = 0 \\ \sqrt{\frac{2}{N}}, & u \neq 0. \end{cases} \quad (5)$$



**Fig. 1** Block diagrams. **a** The implementation of the two-level DWT. **b** The implementation of the two-level IDWT



**Fig. 2** Transform domains using different transforms. **a** Original image. **b** DWT transform coefficients. **c** DCT transform coefficients. **d** The matrix  $U$  of left-singular vectors. **e** The singular matrix  $S$ . **f** The matrix  $V$  of left-singular vectors

where  $f(i, j)$  is the input image, and  $F(u, v)$  is the corresponding DCT transform coefficients. By applying the inverse DCT (IDCT) to the DCT transform coefficients, the original input image can be obtained as

$$f(i, j) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \beta(u)\beta(v)F(u, v) \cos \left[ \frac{(i + 0.5)\pi}{N} u \right] \cos \left[ \frac{(j + 0.5)\pi}{N} v \right] \quad (6)$$

After being transformed into the DCT domain, the original image can be divided into a DC component and a series of AC components. The AC components consist of three parts, the low frequency, the intermediate frequency and the high frequency. In most cases, the information is mainly concentrated in the low-frequency part. We show the DCT transform coefficients of the Lena image in Fig. 2c.

### 2.3 Singular value decomposition

SVD is a method of matrix decomposition. SVD does not require that the decomposed matrix be square. Assuming that our matrix  $A$  is a matrix of  $M \times N$ , we define the SVD of matrix  $A$  as:

$$A = USV^T. \quad (7)$$

where  $U$  is an  $M \times M$  orthogonal matrix,  $S$  is an  $M \times N$  diagonal matrix, and  $V$  is an  $N \times N$  orthogonal matrix. Hence, we have

$$AA^T = USV^T (USV^T)^T = US^2U^T, \quad (8)$$

$$A^T A = (USV^T)^T USV^T = VS^2V^T. \quad (9)$$

The above two equations show that  $U$  and  $V$  can be obtained from the eigenvectors of  $AA^T$  and  $A^T A$ , respectively. The square roots of the eigenvalues of  $AA^T$  or  $A^T A$  are the singular values of  $S$ . We show the experimental results of the SVD decomposition of the Lena image in Fig. 2d-f.

### 3 The proposed image watermarking scheme

In this section, we propose a robust image watermarking scheme against rotation attacks, by using the aforementioned techniques of the DWT, the DCT, and the SVD. For convenience, we summarize the parameters and notations used in our scheme in Table 1.

#### 3.1 Watermarking embedding

Suppose that the original image is denoted by  $I = \{I(x, y)\}$ , and the watermark message is denoted by  $\mathbf{b} = \{b_0, b_1, \dots\}$ . Our watermark embedding algorithm is given as follows.

- Step 1. In order to protect the original watermark message, we apply the scrambling method to the original message  $\mathbf{b}$ , and then perform rearrangement to obtain a watermark matrix  $W = \{w_{ij}\}$ , with a key  $K_1$ . Without loss of generality, we assume that the size of  $W$  is  $h \times h$ . Even if the watermark  $W$  were illegally extracted, the message sequence  $\mathbf{b}$  would not be exposed to the adversary directly.
- Step 2. We perform the DWT on the original image  $I$ , and obtain the four coefficient subbands  $LL$ ,  $HL$ ,  $LH$  and  $HH$ .  $LL$  represents the low-frequency subband of the DWT coefficients, which dominates the energy of all the DWT coefficients.
- Step 3. In order to improve the robustness, we choose the  $LL$  subband for embedding. We split the  $LL$  subband into non-overlapping  $h \times h$  blocks. We then randomly choose  $m$  blocks and perform the DCT on these blocks to obtain the DCT coefficient blocks, denoted by  $\{A_i\}_{i=1}^m$ .
- Step 4. We perform the SVD on every DCT block  $A_i$  and obtain the corresponding SVD decomposition, i.e.,  $A_i = U_i S_i V_i^T$ . We save  $\{S_i\}_{i=1}^m$  in the key  $K_2$ . We also use the SVD to decompose the watermark matrix. That is, we perform the SVD on  $W$  and obtain  $W = U_w S_w V_w^T$ .  $U_w$  and  $V_w$  are then stored as the key  $K_3$ .
- Step 5. To avoid the FPP, we apply the signature generation procedure to the set of  $U_w$  and  $V_w$  to obtain an 8-bit digital signature, i.e.,  $Sig_K = \text{Sig}(\cdot)(K_3) = \text{Sig}(U_w, V_w)$ , where  $\text{Sig}(\cdot)$  denotes a practical digital signature algorithm.  $Sig_K$  will be integrated as a digital signature into the watermarked image at the final step of the watermark embedding procedure.
- Step 6. We perform watermark embedding by inserting the singular value matrix of the watermark into that of the DCT coefficients. Specifically, for the  $i$ th block, we carry out the watermark embedding as

$$T_i = S_i + \alpha S_w \quad (10)$$

**Table 1** Summary of parameters and notations

Notation	Meaning
$I$	The original cover image
$\mathbf{b}$	The watermark message
$W$	The watermark matrix rearranged from $\mathbf{b}$
$LL$	The low-frequency subband of The two-level DWT coefficients of $I$
$h$	The size of block DCT
$A_i$	The DCT coefficient blocks of $LL$
$U_i$ and $V_i$	The orthonormal matrices for $A_i$
$S_i$	The diagonal matrix for $A_i$
$U_w$ and $V_w$	The orthonormal matrices for $W$
$S_w$	The diagonal matrix for $W$
$sig_K$	An 8-bit digital signature
$\alpha$	The watermark embedding strength
$T_i$	The modified singular values of $S_i$
$\tilde{U}_i$ and $\tilde{V}_i$	The orthonormal matrices for $T_i$
$R_i$	The diagonal matrix for $T_i$
$A'_i$	The modified DCT coefficient block
$I_w$	The watermarked image
$K_i$	The watermarking key
$LL'$	The low-frequency subband of The two-level DWT coefficients of $I_w$
$\hat{A}_i$	The DCT coefficient blocks of $LL'$
$\hat{U}_i$ and $\hat{V}_i$	The orthonormal matrices for $\hat{A}_i$
$\hat{S}_i$	The diagonal matrix for $\hat{A}_i$
$B_i$	The modified singular value matrix
$\hat{S}_w$	The scaled singular matrix
$\hat{W}$	The extracted watermark
$\hat{\mathbf{b}}$	The extracted watermark message

where  $T_i$  is the modified singular values of  $S_i$ , and  $\alpha$  is the watermark embedding strength, which controls the energy of the watermark signal to be embedded. Larger energy of the watermark signal will help the watermarking images against more intense watermarking attacks.

Step 7. We perform the SVD on  $T_i$  and obtain the decomposition  $T_i = \tilde{U}_i R_i \tilde{V}_i^T$ . We then obtain the modified DCT coefficient block by computing the matrix

$$A'_i = U_i R_i V_i^T, \tag{11}$$

where  $A'_i$  contains the watermark information. We set  $\{\tilde{U}_i, \tilde{V}_i\}_{i=1}^m$  as the key  $K_4$ .

Step 8. We perform the IDCT on every block  $A'_i$ , build up all the blocks and get the low-frequency subband of the DWT coefficients. After applying the IDWT to the DWT coefficients, we finally obtain the watermarked image  $I_w$ .

We sketch the proposed watermark embedding process in Fig. 3.

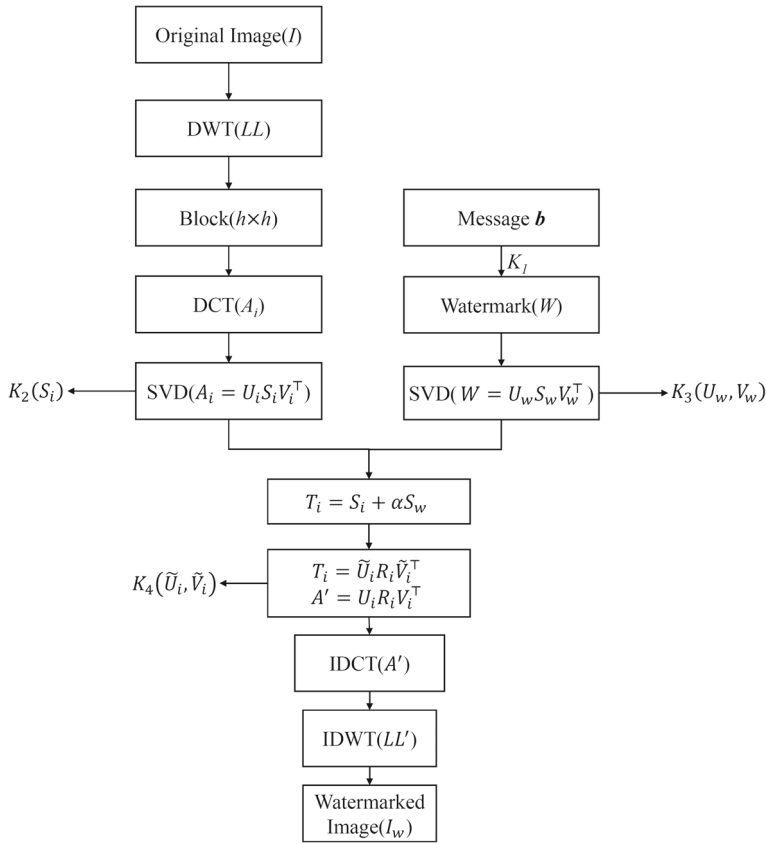


Fig. 3 The procedure of the watermark embedding

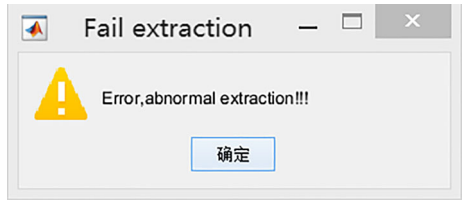
### 3.2 Watermark extraction

To ensure that the watermark message can be correctly extracted, the watermark key pair  $(K_1, K_2, K_3, K_4)$  is sent to watermark extractor. Given a watermarked image  $I_w$ , the proposed watermark extraction algorithm can be described as follows.

- Step 1. First of all, we perform a safety verifying on the watermarked image in order to avoid the FPP. We extract the digital signature (denoted by  $Sig_K$ ) from the watermarked image. We then carry out the signature verifying  $Ver(K_3, Sig_K) = Ver(U_w, V_w, Sig_K)$ , where  $Ver(\cdot)$  denotes the signature verifying algorithm corresponding to  $Sig(\cdot)$ . If the output of the signature verifying procedure is true, the watermark extraction process continues. Otherwise, the watermark extraction process would terminate like Fig. 4, as an FPP is detected.
- Step 2. We perform the DWT on the input image  $I_w$ , and obtain the four DWT coefficient subbands  $LL', HL', LH',$  and  $HH'$ .
- Step 3. We split the  $LL'$  subband into non-overlapping blocks of size  $h \times h$ , and then select  $m$  blocks at the same positions as in the embedding process. After that, we perform the DCT on these selected blocks to get the DCT coefficient blocks  $\{\hat{A}_i\}_{i=1}^m$ .



Fig. 4 Fail extraction



Step 4. We perform the SVD on every block  $\hat{A}_i$ , and obtain  $\hat{A}_i = \hat{U}_i \hat{S}_i \hat{V}_i^T$ . By using the key  $K_4$ , we obtain the modified singular value matrix  $B_i$  with the watermark information, i.e.,

$$B_i = \tilde{U}_i \hat{S}_i \tilde{V}_i^T \tag{12}$$

Step 5. By using the watermark key  $K_2$ , we calculate the scaled singular matrix according to the following formula:

$$\hat{S}_w = \frac{1}{\#\{B_i\}} \sum_i \frac{B_i - S_i}{\alpha} \tag{13}$$

where  $\alpha$  is the watermark embedding strength, and  $\#\{B_i\}$  represents the number of block in  $\{B_i\}$ .

Step 6. We compute the extracted watermark as

$$\hat{W} = U_w \hat{S}_w V_w^T, \tag{14}$$

and then rearrange  $\hat{W}$  to obtain the extracted watermark message  $\hat{\mathbf{b}}$  by using the key  $K_1$ .

The proposed watermark extraction procedure is sketched in Fig. 5. We can consider the proposed scheme to be a semi-blind watermarking. The key  $K_1$  is the seed used by the pseudo-random algorithm to generate random numbers or permutation. Thus, the data capacity of the key  $K_1$  is 1. Suppose that the size of the original image  $I$  is  $M \times M$ . The data capacities of the keys  $K_2$ ,  $K_3$ , and  $K_4$  are  $mh$ ,  $2h^2$ , and  $2mh^2$ , respectively. Thus, the data

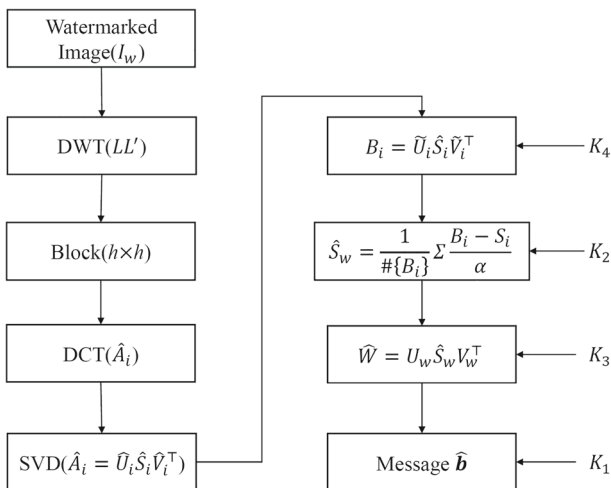


Fig. 5 The procedure of the watermark extraction

capacity of  $K_2$  and  $K_4$  is  $mh + 2mh^2$ , which is generally smaller than the storage space of the image, i.e.,  $M^2$ . For example, if  $M = 512$ ,  $h = 8$ , and  $m = 20$  for some practical image and watermark message, then  $mh(1 + 2h) = 2720 \ll 262144 = M^2$ . Therefore, although  $K_2$  and  $K_4$  are related with the image, the proposed watermarking algorithm is efficient and effective in practice.

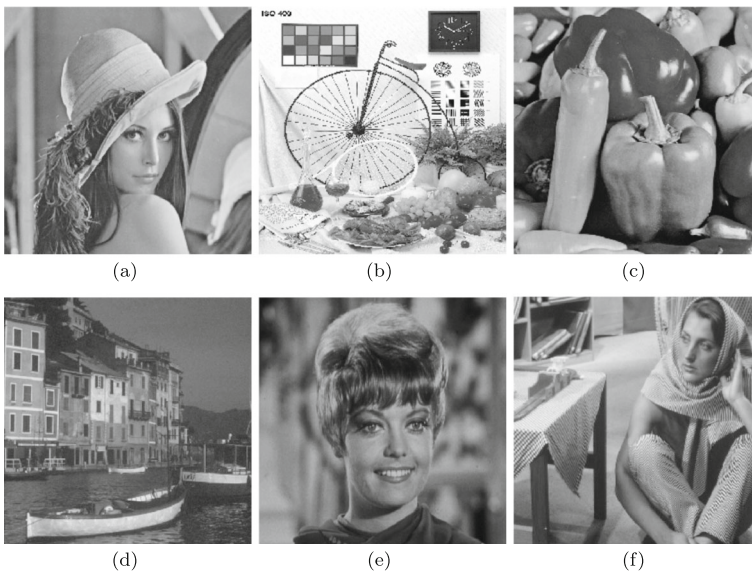
## 4 Simulation and experimental results

We test the proposed watermarking scheme on a database of 50 gray images of  $512 \times 512 \times 8$  bits. Some sample images in the database are shown in Fig. 6. The test watermark is a gray image of  $64 \times 64 \times 8$  bits, which is shown in Fig. 7c. We choose  $m = 16$  DCT blocks in the  $LL$  subband for watermark embedding.

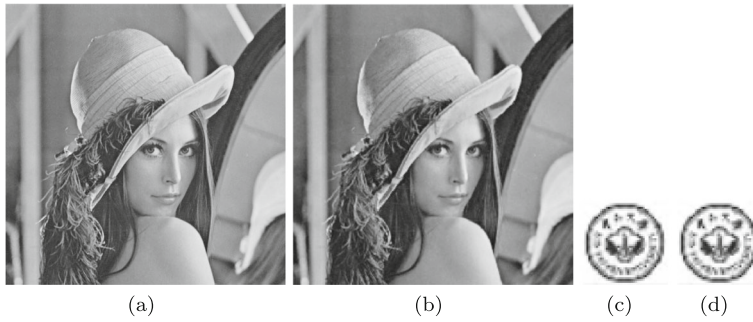
### 4.1 Visual performance

After performing the Haar wavelet transform on the original image, we segment the  $LL$  subband into  $64 \times 64$  blocks. We perform the DCT on every block and then apply the SVD to them before watermark embedding. The embedding strength is chosen as 0.01. We show the experimental results of “Lena” image in Fig. 7. To evaluate the visual quality of the watermarked image, we use the peak signal-to-noise ratio (PSNR) measure. The quality of the extracted watermark measured by the normalized correlation coefficient (NC). The PSNR of the original image  $I$  and the watermarked image  $I_w$  is computed as

$$PSNR = 10 \log_{10} \left( \frac{255^2}{\frac{1}{M^2} \sum_{i,j=0}^{M-1} (I(i,j) - I_w(i,j))^2} \right), \quad (15)$$



**Fig. 6** Some examples of the original images. **a** Lena. **b** Bike. **c** Peppers. **d** Portofino. **e** Zelda. **f** Women



**Fig. 7** Visual effect of our watermarking scheme on “Lena” image. **a** Original “Lena” image. **b** Watermarked image. **c** Original watermark. **d** Extracted watermark

where the size of the image is  $M \times M$ . If the original watermark  $W$  and the extracted watermark  $W_\epsilon$  are size of  $M' \times M'$ , their NC value can be computed as

$$NC = \frac{\sum_{i,j=1}^M (W(i, j) - \bar{W})(W_\epsilon(i, j) - \bar{W}_\epsilon)}{\sqrt{\sum_{i,j=1}^M (W(i, j) - \bar{W})^2} \sqrt{\sum_{i,j=1}^M (W_\epsilon(i, j) - \bar{W}_\epsilon)^2}} \tag{16}$$

where  $\bar{W}$  and  $\bar{W}_\epsilon$  are the sample means for  $W$  and  $W_\epsilon$ , respectively. The PSNR of the watermarked “Lena” image is 40.43 dB, while its NC is 1.00.

In order to find a suitable embedding strength, different values of  $\alpha$  are selected and tested. The experimental results are as shown in Table 2, where the watermarking attack is rotation attack.

We provide more experiments on a database of 50 gray images. To show the advantage of our scheme, we conduct experiments to compare with some related works, including the following two watermarking schemes [10, 23].

**Table 2** Results of different  $\alpha$

Value of $\alpha$	Result without attack		Result under attack	
	PSNR	NC	PSNR	NC
0.001	73.947	1.000	12.909	0.8767
0.002	67.927	1.000	12.908	0.8769
0.003	64.405	1.000	12.906	0.8771
0.004	61.906	1.000	12.905	0.8773
0.005	59.968	1.000	12.904	0.8775
0.006	58.385	1.000	12.902	0.8777
0.008	55.886	1.000	12.900	0.8781
0.01	53.947	1.000	12.896	0.8785
0.03	44.405	1.000	12.866	0.8822
0.05	39.968	1.000	12.834	0.8858
0.08	35.886	1.000	12.781	0.8908
0.1	33.947	1.000	12.742	0.8940

- “DWS” [10]. DWS combines the DWT and the SVD to enhance the robustness of the watermarking scheme. In DWS, the SVD is performed on  $LL$  subband of the DWT coefficients. The watermark is then embedded into the diagonal matrix.
- “IWS” [23]. IWS combines the IWT, the AT and the SVD to improve the performance. Firstly, apply IWT to the original image. Then embed the scrambled watermark into the SVD domains of the four IWT subbands.

The comparison results are shown in Table 3, from which we can see that the proposed watermarking scheme generally outperforms the compared schemes in visual quality without watermarking attacks. Specifically, the proposed scheme achieves higher PSNR values for all the tested images. The watermark is invisible among the watermarked images and can be completely recovered after extraction. Compared with DWS that does not use DCT, our scheme has slightly larger values of NC on some test images, i.e., the Bike and the Portofino images. Meanwhile, our scheme also ensures high imperceptible watermarked images whose PSNRs are greater than 52 dB. Thus, the proposed scheme has better visual quality than the two compared schemes DWS and IWS.

#### 4.2 Robustness under different watermarking attacks

In this subsection, we conduct experiments to study the robustness of the proposed watermarking scheme under different types of attacks, especially the lossy compression attacks and the rotation attacks. We also provide the comparison results between the proposed watermarking scheme and those schemes listed above. The robustness of the watermarking scheme under the watermarking attack is evaluated in the same PSNR of the watermarked images. We introduce the watermarking attacks used in our experiments as follows.

- “Noise attack”. Add 1% noise into the watermarked image. We test three kinds of noises, i.e., speckle noise, gaussian noise, and salt and pepper noise.
- “Cropping attack”. Crop a block of size  $250 \times 250$  from the watermarked image, the size of which is  $512 \times 512$ .
- “BDCTIm”. Divide the watermarked image into blocks of size  $8 \times 8$ , and then apply DCT to each block. Retain the low and middle-frequency coefficients (36 coefficients in total) in each block, which has a total of 64 coefficients.
- “DCTIm”. Perform DCT on the whole image and discard half of the coefficients.
- “DWTII”. Perform DWT and retain only the  $LL$  subband.

**Table 3** Performance comparison without watermarking attacks

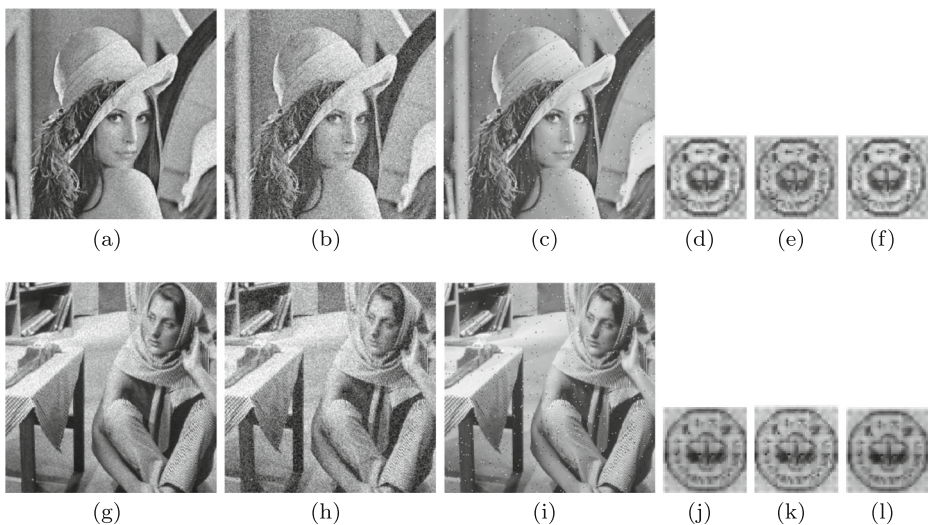
Images	Proposed algorithm		DWS		IWS	
	PSNR	NC	PSNR	NC	PSNR	NC
Lena	53.947	1.000	51.963	1.000	44.304	1.000
Bike	53.247	1.000	50.427	0.999	44.730	1.000
Peppers	54.043	1.000	51.643	1.000	45.292	1.000
Portofino	53.816	1.000	49.962	0.999	44.685	1.000
Zelda	52.951	1.000	50.496	1.000	43.341	1.000
Women	53.697	1.000	51.506	1.000	44.887	1.000

- “JPEG- $\alpha$ ”. Perform JPEG lossy compression with a quality factor  $\alpha$ , where  $\alpha$  is chosen as 30, 60, and 90 in the experiment.
- “Rotation  $\theta$ ”. Perform the rotation attack with the rotation angle  $\theta$ , where there are three values of  $\theta$  in the experiment, i.e.,  $10^\circ$ ,  $30^\circ$ , and  $45^\circ$ .
- “Gaussian blur”. Perform Gaussian low-pass filtering to blur the image in the spatial domain.

The experimental results on robustness are presented in the following. In Fig. 8, we show the noised watermarked image of two sample images after three types of noises, i.e., speckle noise, gaussian noise, and salt and pepper noise, as well as the extracted watermarks from these noised images. We can see that the watermarks can be correctly extracted from the two test images after the three kinds of noise attacks. Some of the experimental results of cropping attacks with different positions are shown in Fig. 9, where we crop the blocks of size  $250 \times 250$  at the top left corner, the central region, and the bottom right corner of the original images, respectively. From Fig. 9, we find that the original watermarks can be correctly extracted after these cropping operations.

We present the experimental results after discarding parts of the transform coefficients in Fig. 10, where the DCT, the DWT, and block DCT are employed, respectively. It is found that we can still extract the original watermarks even when only parts of the transform coefficients are retained after different kinds of transforms. In Fig. 11, we show the experimental results of performing lossy JPEG compression on the two sample images. We adopt three different quality factors, i.e., 90, 60, and 30. We can see that the watermarks can be correctly obtained from the JPEG-compressed watermarked images.

The experimental results of performing the Gaussian low-pass filtering with different intensities on the original images are shown in Fig. 12. We select three different sizes of filters, including  $5 \times 5$ ,  $6 \times 6$ , and  $10 \times 10$ . We can see that it is able to extract the original watermarks from the blurred watermarked images.



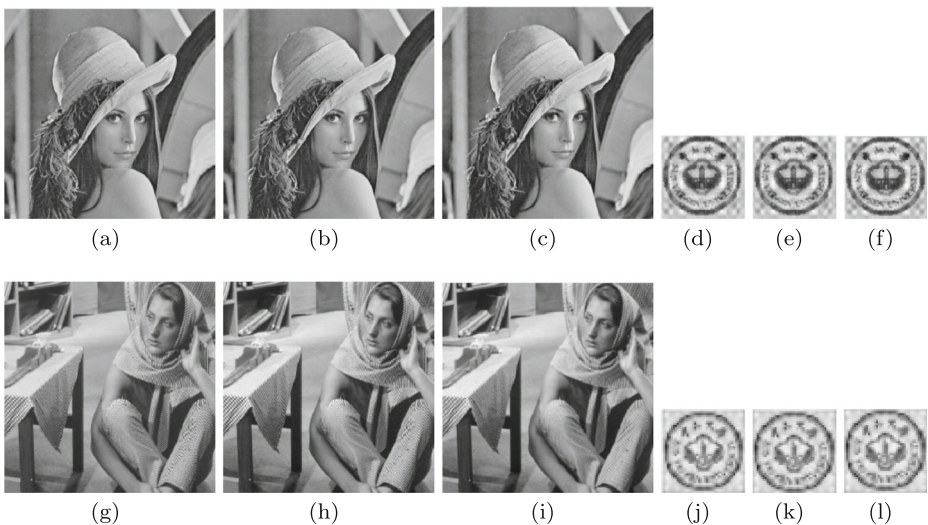
**Fig. 8** Different kinds of noise attacks (add 1%). Columns 1, 2, and 3 are the watermarked images attacked with speckle noise, Gaussian noise, and salt & pepper noise, respectively. Columns 4, 5, and 6 are the watermarks extracted from the images in Columns 1, 2, and 3, respectively



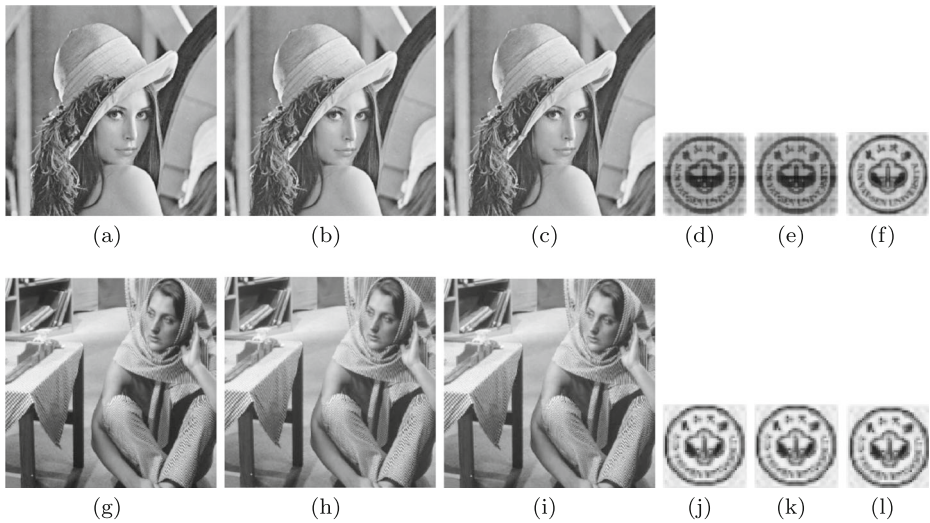


**Fig. 9** Cropping attacks with different positions. Columns 1, 2, and 3 are the watermarked images cropped at the top left corner, the center, and the bottom right corner, respectively. Columns 4, 5, and 6 are the watermarks extracted from the images in Columns 1, 2, and 3, respectively

We also show the experimental results of the rotation attacks with different rotation angles in Fig. 13. Three different rotation angles are chosen, i.e.,  $10^\circ$ ,  $30^\circ$ , and  $45^\circ$ . When the watermarked image is rotated, the black regions are introduced and the resolution is enlarged. In the watermark extraction process, we will crop the rotated image to keep it

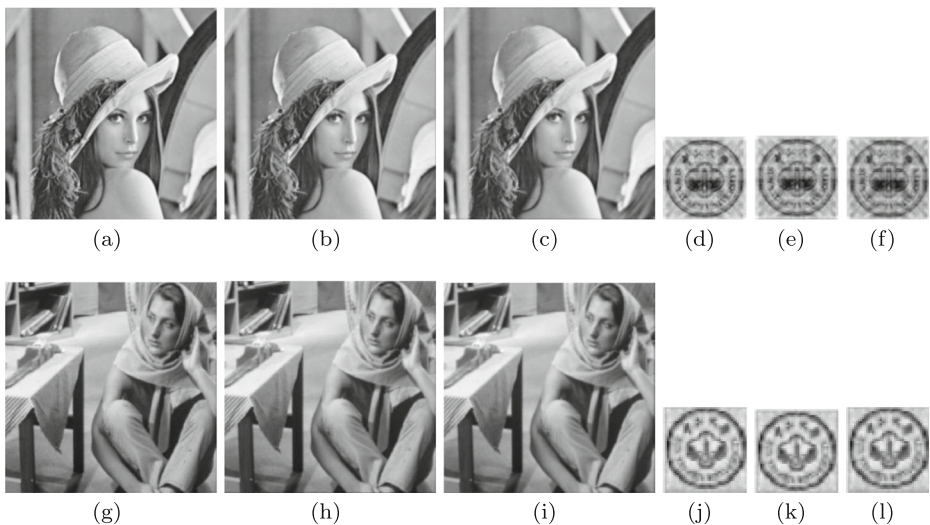


**Fig. 10** Different kinds of transform domain attacks. Columns 1, 2, and 3 are the watermarked images attacked with BDCTIm, DCTIm, and DWTIm, respectively. Columns 4, 5, and 6 are the watermarks extracted from the images in Columns 1, 2, and 3, respectively

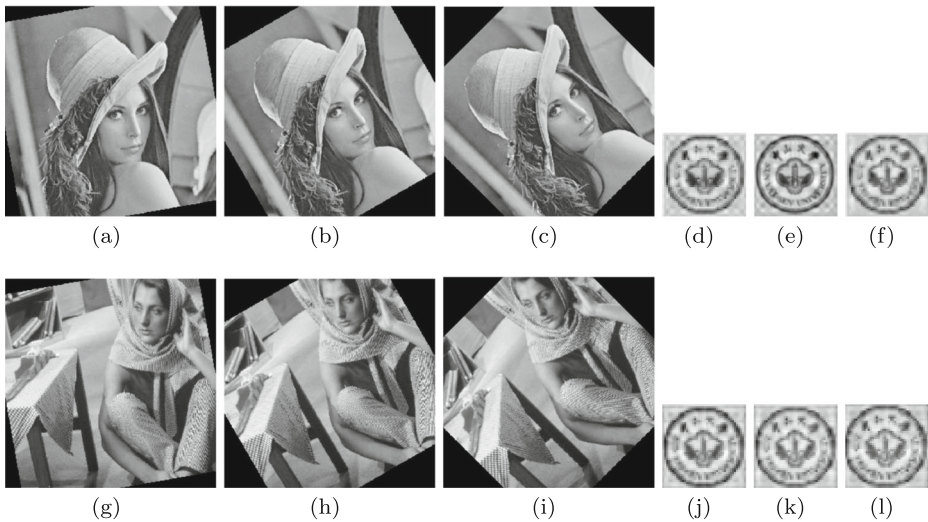


**Fig. 11** Lossy JPEG compression attacks with different quality factors. Columns 1, 2, and 3 are the watermarked images attacked with JPEG compression using the quality factors of 90, 60, and 30, respectively. Columns 4, 5, and 6 are the watermarks extracted from the images in Columns 1, 2, and 3, respectively

in the original resolution. The blocks from the attacked image are then not exactly consistent with the original ones during the embedding process. However, from Fig. 13, we can see that the watermark can be correctly extracted from the rotated images, regardless of what rotation angle is. That is because the block splitting is conducted in the DWT domain rather than the spatial domain, and the singular value matrix  $S$  of the SVD factorization is



**Fig. 12** Gaussian blur attacks with different sizes of filters. Columns 1, 2, and 3 are the watermarked images attacked using Gaussian low-pass filtering with the filter sizes of  $5 \times 5$ ,  $6 \times 6$ , and  $10 \times 10$ , respectively. Columns 4, 5, and 6 are the watermarks extracted from the images in Columns 1, 2, and 3, respectively

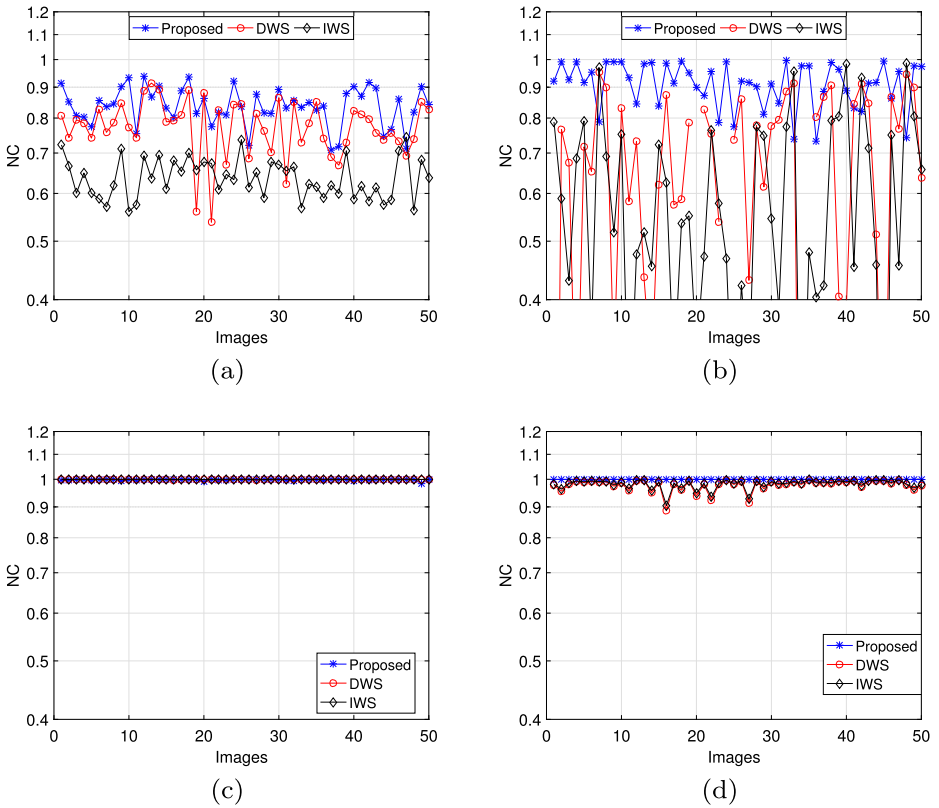


**Fig. 13** Rotation attacks with different rotation angles. Columns 1, 2, and 3 are the watermarked images attacked using rotation attacks with the rotation angles of  $10^\circ$ ,  $30^\circ$ , and  $45^\circ$ , respectively. Columns 4, 5, and 6 are the watermarks extracted from the images in Columns 1, 2, and 3, respectively

less affected by the rotation attack. From the experimental results shown in Figs. 8–13, we can observe that the proposed watermarking scheme has a satisfactory performance against most of the attacks.

To further investigate the advantages of the proposed scheme, we conduct more experiments to compare our method with the related image watermarking schemes [10, 23] with the same embedding strength  $\alpha = 0.01$ . We carry out the proposed watermarking scheme as well as the compared watermarking schemes on same test image set. Specifically, we compute the NC values for different images after different kinds of watermarking attacks, including noise attack, cropping attack, transform attack, lossy compression, and rotation attack. The experimental results are shown in Figs. 14, 15 and 16, where the  $x$ -axis denotes the indexes of the images and the  $y$ -axis represents the NC values between the original and the extracted watermarks. From Figs. 14–16, we find that the NC values of the proposed watermarking scheme are higher and more stable than the two compared watermarking schemes, for most of the cover images and the watermarking attacks. For example, under the cropping attack, our scheme has much higher NC values than the “DWS” scheme. Under the lossy JPEG compression attack with a quality factor of 30, our scheme also greatly outperforms the “IWS” scheme, where the extracted watermarks are badly destroyed. As for the robustness resisting the rotation attacks, from Fig. 16, we can observe that the proposed watermarking scheme achieves the best robustness among the three watermarking schemes for almost all the test images. Both the two compared watermarking schemes are not able to resist the rotation attacks, since the NC values of “DWS” and “IWS” are unstable and fluctuate around 0.5. However, the proposed scheme is very robust to the rotation attacks with any rotation angles. For example, under the rotation attack with the rotation angle of  $100^\circ$ , most of the NC values of the proposed watermarking scheme are close to 0.9. In general, according to our experimental results, we can see that the proposed





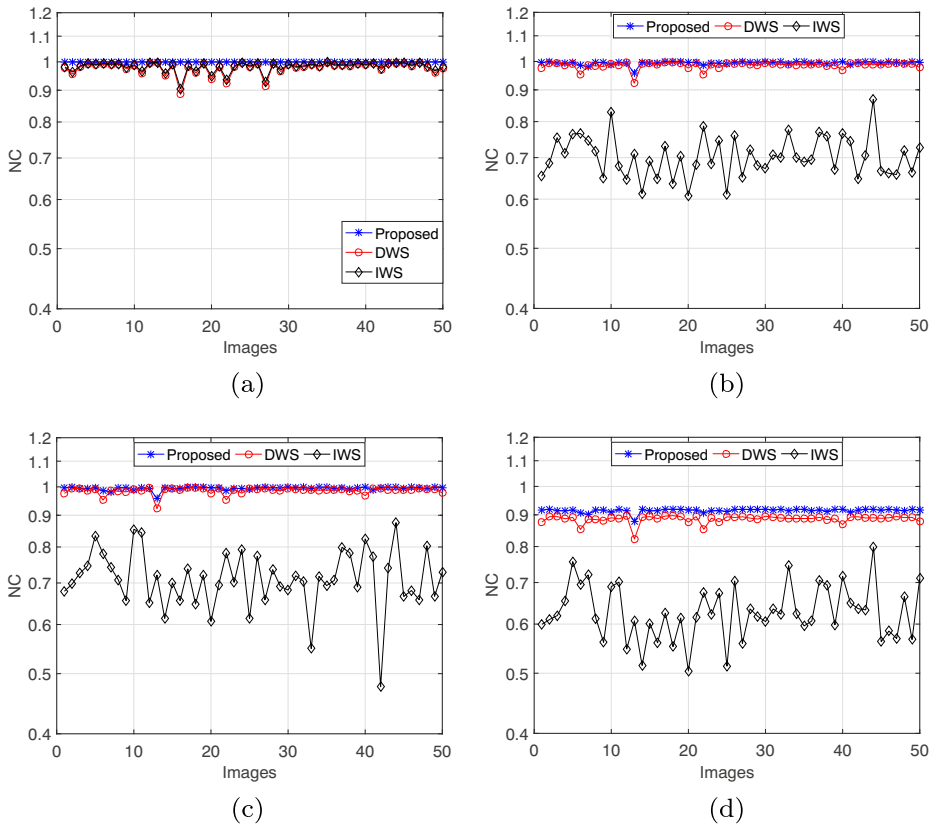
**Fig. 14** Robustness comparison against some common watermarking attacks. **a** Noise attack. **b** Cropping attack. **c** BDCTIm. **d** DWTII

watermarking scheme has better robustness, and in particular, behave much better against the rotation attacks than the compared schemes.

### 4.3 Further investigations

#### 4.3.1 The influence of $h$ on the watermarking performance

We investigate the watermarking performance regarding different values of  $h$ . Specifically, we adopt four different values of  $h$ , i.e., 8, 16, 32, and 64, for the same watermark matrix of  $512 \times 512 \times 8$  bits. We study the perceptual quality as well as the robust performance against four common watermarking attacks, i.e., noise attack, cropping attack, JPEG compression attack, and rotation attack. The experimental results for different values of  $h$  are given in Table 4. We can see that the average PSNR values are the same for these different  $h$  values. As for the robust performance, the NC values for cropping attack, JPEG compression attack, and rotation attack are all larger than 0.9, for all values of  $h$ . When the noise attack is

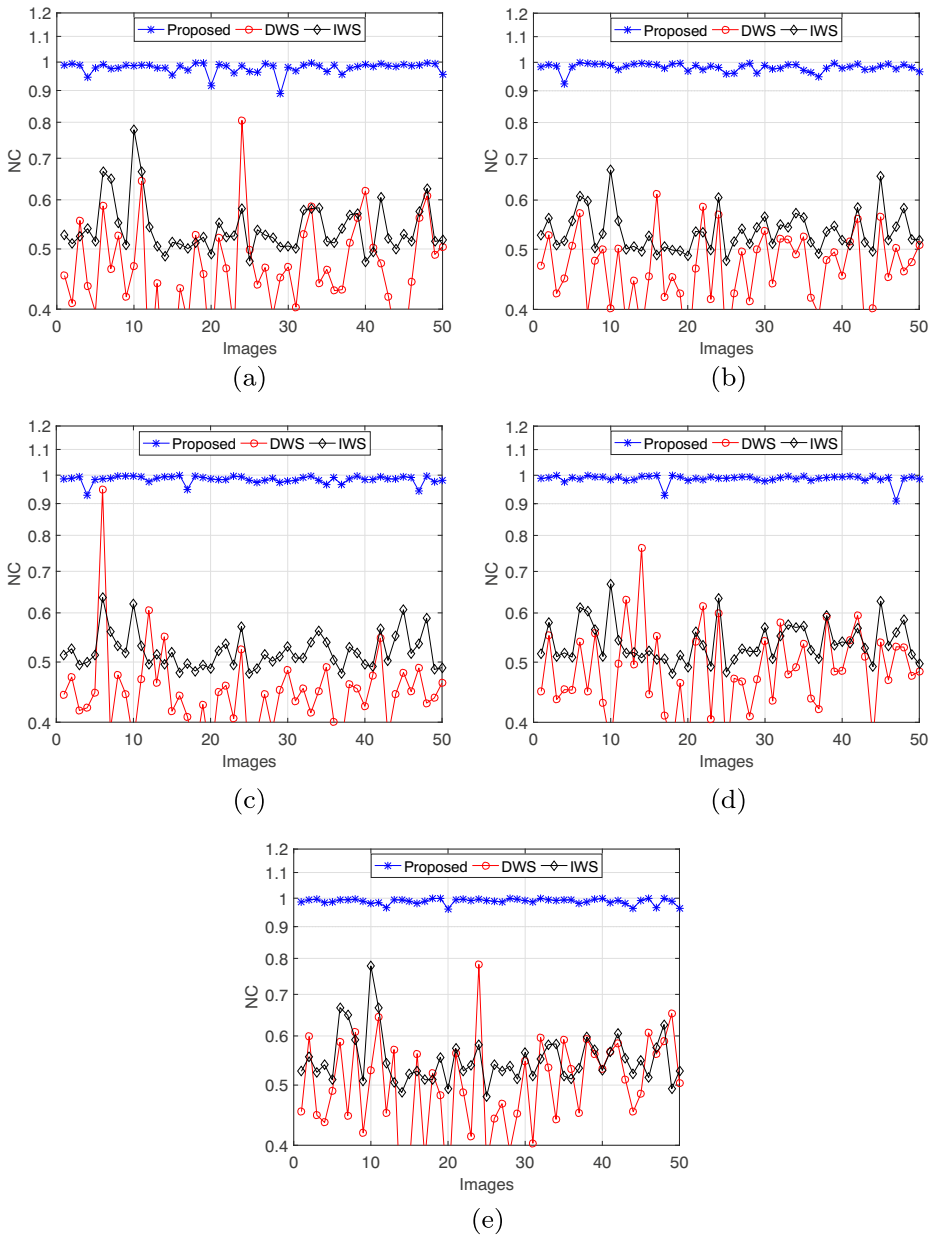


**Fig. 15** Robustness comparison against some common watermarking attacks. **a** DWTII. **b** JPEG-90. **c** JPEG-60. **d** JPEG-30

performed, a smaller value of  $h$  helps improve the robustness. Thus, the value of  $h$  generally has less effect on the watermarking performance except for the robustness against the noise attack.

### 4.3.2 Embedding capacity

To investigate the embedding capacity, we vary the value of  $h$  and then compute the average PSNR value of the watermarked images. By studying the relationship between the parameter  $h$  and the PSNR of the watermarked image, we can learn the embedding capacity. We have compared our scheme with the related schemes DWS [10] and IWS [23]. The size of the embedded watermark matrix is  $h \times h \times 8$  bits. The testing results are shown in Table 5. Even when the size of the watermarking matrix is  $256 \times 256 \times 8$  bits, the watermarked images can have a high average PSNR value of 50.724 dB. On the contrary, the average PSNR values for DWS and IWS are 37.559 dB and 46.627 dB, respectively. In particular, when the watermark matrix is size of  $512 \times 512 \times 8$  bits, our scheme can achieve an



**Fig. 16** Robustness comparison against different rotation attacks. **a** Rotation 10°. **b** Rotation 30°. **c** Rotation 45°. **d** Rotation 60°. **e** Rotation 100°

average PSNR value of 47.704, while the schemes of DWS and IWS cannot work. Thus, we can see that the proposed scheme has a higher embedding capacity than the two compared schemes.

**Table 4** The influence of  $h$  on the watermarking performance

$h$		8	16	32	64
PSNR		53.680	53.680	53.680	53.680
NC	Noise attack	0.9641	0.9191	0.8078	0.7026
	Cropping attack	1.0000	1.0000	1.0000	1.0000
	JPEG-60	0.9999	0.9998	0.9991	0.9985
	Rotation 45°	0.9999	0.9987	0.9768	0.9677

### 4.3.3 Comparison with other rotation-against watermarking scheme

We compare our scheme with another rotation-against watermarking scheme [15], which also perform watermark embedding in the DWT-DCT-SVD domain. Without loss of generality, we consider three rotation angles, i.e., 30°, 45°, and 60°. After performing the rotation attacks with angle 30°, the average NC values for our scheme and the scheme [15] are 0.98 and 0.97, respectively. When the rotation angles are 45° and 60°, the average NC values of the proposed scheme are 0.98 and 0.99, respectively; while the average NC values of the scheme [15] are 0.97 and 0.97, respectively. Therefore, we can see that the robustness of the proposed scheme is better than the scheme [15] against some common rotation attacks.

### 4.3.4 Discussion on the robust performance

The DWT and the DCT can help improve the robustness against noise attack, compression attack, cropping attack, and blurring attack, while the SVD can enhance the robustness against rotation attack. Generally, noise attack, compression attack, and blurring attack will affect the high-frequency subband and have less effect on the low-frequency subband [12]. The DWT on the whole image can help us to extract global features of the image, and eliminate the influences of noise attack and blurring attack. While the block DCT on the DWT coefficients can help extract local features, and resist compression attack and cropping attack. By using the DWT and the DCT, we embed the watermark information into the low-frequency subband, and therefore, our scheme has high robustness against these watermarking attacks. The expression  $USV^T$  of the SVD factorization can be considered as a composition of three geometrical transformations [32]: a rotation  $U$ , a scaling  $S$ , and another rotation  $V$ . The rotation attack will change the rotation matrices  $U$  and  $V$ , while have less affect on the scaling matrix  $S$ . We embed the watermark information into the matrix  $S$ , and can achieve enhanced robustness against rotation attacks. Thus, we combine the DWT, the DCT, and the SVD in the proposed scheme, to make our scheme resist noise attack, compression attack, blurring attack, cropping attack, and rotation attack.

**Table 5** Comparison of the embedding capacity

$h$		8	16	32	64	128	256	512
PSNR	Our scheme	72.120	65.996	59.839	53.680	52.426	50.724	47.704
	DWS	67.972	61.885	55.828	49.775	43.712	37.559	–
	IWS	70.515	63.428	58.010	54.070	50.850	46.627	–

## 5 Conclusions

In this paper, we design a robust image watermarking scheme resisting noise attack, compression attack, blurring attack, as well as rotation attack. By employing the DCT, the DWT, and the SVD, we propose a robust rotation-invariant watermarking scheme against these watermarking attacks. The main contributions are listed as follows.

1. By studying the properties of the DWT, the DCT, and the SVD, we propose a watermarking scheme that combines the DWT, the DCT, and the SVD. The DWT and the DCT have satisfactory characteristics to help improve the robustness against noise attack, compression attack, and blurring attack, while the SVD can strengthen the robustness against rotation attacks.
2. By conducting experiments on the proposed scheme, we demonstrate that the proposed scheme has good robustness against various attacks, in particular, rotation attacks.

By using our watermarking scheme, it is able to design image-watermarking applications in copyright protection and traitor tracing. We will focus on the following three aspects in our future works. (1) Extend the proposed scheme to the application scenario of color image watermarking. (2) Enhance the robustness of the proposed scheme to adapt to new types of watermarking attacks. (3) Transplant the proposed scheme to image watermarking in the encrypted domain to develop secure, and robust image watermarking techniques.

**Acknowledgements** This work was supported in part by the Guangdong Natural Science Foundation under Grant 2019A1515010746 and Grant 2015A030310319, in part by the Fundamental Research Funds for the Central Universities under Grant 19LGPY218, in part by the NSFC under Grant 61502547, and in part by the Opening Project of Guangdong Province Key Laboratory of Information Security Technology under Grant 2017B030314131.

## References

1. Agarwal C, Mishra A, Sharma A (2013) Gray-scale image watermarking using GA-BPN hybrid network. *J Vis Commun Image Represent* 24(7):1135–1146
2. Ali M, Ahn CW, Pant M (2014) A robust image watermarking technique using svd and differential evolution in dct domain. *Optik-Int J Light Electron Opt* 125(1):428–434
3. Ansari R, Devanalamath MM, Manikantan K, Ramachandran S (2012) Robust digital image watermarking algorithm in dwt-dft-svd domain for color images. In: 2012 International conference on communication, information & computing technology (ICCICT). IEEE, pp 1–6
4. Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2012) Robust digital image watermarking using interest points and dft domain. In: 2012 35Th international conference on telecommunications and signal processing (TSP), pp 715–719. IEEE
5. Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2015) Robust watermarking method in dft domain for effective management of medical imaging. *SIViP* 9(5):1163–1178
6. Chen M, Zhang Z, Cai Z, Pan Y (2016) A novel image encryption method based on fractional fourier transform and odd-even quantification. In: Eighth international conference on digital image processing (ICDIP 2016). International society for optics and photonics, vol 10033, pp 1003332
7. Das C, Panigrahi S, Sharma VK, Mahapatra K (2014) A novel blind robust image watermarking in dct domain using inter-block coefficient correlation. *AEU-Int J Electron Commun* 68(3):244–253
8. Deb K, Al-Seraj MS, Hoque MM, Sarkar MIH (2012) Combined dwt-dct based digital image watermarking technique for copyright protection. In: 2012 7Th international conference on electrical and computer engineering. IEEE, pp 458–461
9. Dubolia R, Singh R, Bhadoria SS, Gupta R (2011) Digital image watermarking by using discrete wavelet transform and discrete cosine transform and comparison based on psnr. In: 2011 International conference on communication systems and network technologies. IEEE, pp 593–596

10. Furqan A, Kumar M (2015) 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. IEEE, pp 638–644
11. Golea NEH, Seghir R, Benzid R (2010) A blind rgb color image watermarking based on singular value decomposition. In: 2010 IEEE/ACS international conference on Computer systems and applications (AICCSA). IEEE, pp 1–5
12. Gonzalez RC, Wintz P (1977) Digital image processing(book). Reading, Mass., Addison-Wesley Publishing Co., Inc. (Applied Mathematics and Computation (13), pp 451
13. Guo JM, Prasetyo H (2014) False-positive-free SVD-based image watermarking. *J Vis Commun Image Represent* 25(5):1149–1163
14. Guo J, Zheng P, Huang J (2015) Secure watermarking scheme against watermark attacks in the encrypted domain. *J Vis Commun Image Represent* 30:125–135
15. Hu WC, Chen WH, Yang CY (2012) Robust image watermarking based on discrete wavelet transform-discrete cosine transform-singular value decomposition. *J Electron Imaging* 21(3):033005
16. Jia SL (2014) A novel blind color images watermarking based on svd. *Optik-Int J Light Electron Opt* 125(12):2868–2874
17. Kashyap N, Sinha G (2012) Image watermarking using 3-level discrete wavelet transform (dwt). *Int J Modern Educ Comput Sci* 4(3):50
18. Lee JS, Li B (2014) Self-recognized image protection technique that resists large-scale cropping. *IEEE MultiMed* 21(1):60–73
19. Lee TY, Lin SD (2008) Dual watermark for image tamper detection and recovery. *Pattern Recogn* 41(11):3497–3506
20. Lei BY, Soon Y, Li Z (2011) Blind and robust audio watermarking scheme based on svd–dct. *Signal Process* 91(8):1973–1984
21. Lin PL, Hsieh CK, Huang PW (2005) A hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recogn* 38(12):2519–2529
22. Lin SD, Shie SC, Guo JY (2010) Improving the robustness of DCT-based image watermarking against jpeg compression. *Comput Stand Interfaces* 32(1-2):54–60
23. Makbol NM, Khoo BE (2013) A hybrid robust image watermarking scheme using integer wavelet transform, singular value decomposition and arnold transform. In: International visual informatics conference. Springer, pp 36–47
24. Mallat SG (1989) A theory for multiresolution signal decomposition: the wavelet representation. *IEEE Trans Pattern Anal Mach Intell* 11(7):674–693
25. Patra JC, Phua JE, Bornand C (2010) A novel dct domain crt-based watermarking scheme for image authentication surviving jpeg compression. *Digit Signal Process* 20(6):1597–1611
26. Qin C, Chang CC, Chen PY (2012) Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism. *Signal Process* 92(4):1137–1150
27. Rawat S, Raman B (2011) A chaotic system based fragile watermarking scheme for image tamper detection. *AEU-Int J Electron Commun* 65(10):840–847
28. Run RS, Horng SJ, Lai JL, Kao TW, Chen RJ (2012) An improved svd-based watermarking technique for copyright protection. *Expert Syst Appl* 39(1):673–689
29. Singh SP, Rawat P, Agrawal S (2012) A robust watermarking approach using dct-dwt. *Int J Emerging Technol Adv Eng* 2(8):300–305
30. Su Q, Niu Y, Zhao Y, Pang S, Liu X (2013) A dual color images watermarking scheme based on the optimized compensation of singular value decomposition. *AEU-Int J Electron Commun* 67(8):652–664
31. Thakkar FN, Srivastava VK (2017) A blind medical image watermarking: Dwt-svd based robust and secure approach for telemedicine applications. *Multimed Tools Appl* 76(3):3669–3697
32. Trefethen LN, Bau D III (1997) Numerical linear algebra. Siam, vol 50
33. Wang X, Zhang D, Guo X (2013) A novel image recovery method based on discrete cosine transform and matched blocks. *Nonlinear Dyn* 73(3):1945–1954
34. Zheng P, Huang J (2013) Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain. *IEEE Trans Image Process* 22(6):2455–2468
35. Zheng P, Huang J (2018) Efficient encrypted images filtering and transform coding with Walsh-Hadamard transform and parallelization. *IEEE Trans Image Process* 27(5):2541–2556



**Peijia Zheng** received the B.S. degree in mathematics, in 2009, and the Ph.D degree in computer science, in 2014, from Sun Yat-sen University, Guangzhou, China.

He is currently a Lecturer with the School of Data and Computer Science, Sun Yat-Sen University, Guangzhou, China. He is also a member of the Guangdong Key Laboratory of Information Security and Technology. His research interests include multimedia security, image/video encryption, and secure image/video processing.



**Yonghong Zhang** received the B.S. degree from China University of Mining and Technology, Xuzhou, China, in 2018, where he is currently pursuing the master's degree at Sun Yat-sen University. His current research interests include multimedia security, signal/image processing in the encrypted domain.