Multimed Tools Appl (2018) 77:13197–13224
DOI 10.1007/s11042-017-4941-1

A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength

Xiao-bing Kang[1] · **Fan Zhao**[1] · **Guang-feng Lin**[1] · **Ya-jun Chen**[1]

Received: 19 November 2016 / Revised: 27 April 2017 / Accepted: 11 June 2017 /
Published online: 10 July 2017

Abstract To optimize the tradeoff between imperceptibility and robustness properties, this paper proposes a robust and invisible blind image watermarking scheme based on a new combination of discrete cosine transform (DCT) and singular value decomposition (SVD) in discrete wavelet transform (DWT) domain using least-square curve fitting and logistic chaotic map. Firstly cover image is decomposed into four subbands using DWT and the low frequency subband LL is partitioned into non-overlapping blocks. Then DCT is applied to each block and several particular middle frequency DCT coefficients are extracted to form a modulation matrix, which is used to embed watermark signal by modifying its largest singular values in SVD domain. Optimal embedding strength for a specific cover image is obtained from an estimation based on least-square curve fitting and provides a good compromise between transparency and robustness of watermarking scheme. The security of the watermarking scheme is ensured by logistic chaotic map. Experimental results demonstrate the better effectiveness of the proposed watermarking scheme in the perceptual quality and the ability of resisting to conventional signal processing and geometric attacks, in comparison with the related existing methods.

✉ Xiao-bing Kang
kangxb@xaut.edu.cn

Fan Zhao
vcu@xaut.edu.cn

Guang-feng Lin
lgf78103@xaut.edu.cn

Ya-jun Chen
chenyajun@xaut.edu.cn

[1] Department of Information Science, Faculty of Printing, Packaging Engineering and Digital Media Technology, Xi'an University of Technology, Xi'an, Shaanxi 710048, People's Republic of China

Keywords Robust blind watermarking · Discrete wavelet transform · Discrete cosine transform · Singular value decomposition · Least squares curve fitting · Logistic chaotic map

1 Introduction

With the development of digital media and Internet technology, multimedia contents are becoming more significant, popular and they enrich people's everyday life. However, this advantage of digital media content is also their major disadvantage in terms of copyright infringement and unauthorized use of data content. Digital watermarking [11, 14, 29] has been rapidly developed during the past two decades, which can provide efficient solutions for copyright protection, ownership identification, certification of data authenticity, tracking of digital content copies, copy and access controls, etc. In this paper, we concentrate our research topic on robust image watermarking technique for copyright protection and ownership authentication.

Digital image watermarking is a technique to embed a secret signal (watermark) within a specific image (cover image) and extract the secret message at the destination, thereby protecting the image from signal processing attacks during the transmission process. From visual perceptual aspect, image watermark technology can be classified as visible and invisible watermark. The visual watermark runs the risk of being removed. Currently the majority of techniques used fall into the class of invisible watermark. For the reason that the embedding locations are secret, the invisible watermarks are more secure and robust than the visible watermarks. The most important properties of image watermarking techniques include imperceptibility, robustness, security and data capacity. Many watermark methods have been proposed mainly to improve the former two. Owing to robustness and imperceptibility being in conflict with each other, how to maintain a balance between them is key issue in the watermark research activities. In addition original cover images or watermark signals are not always available, the watermark detection or extraction may be performed without the original data. Therefore, an effective robust and invisible blind watermarking scheme is still urged nowadays. Researchers seek to develop a novel watermark scheme that can preserve good imperceptibility while ensuring high security and resisting malicious attacks.

Image watermarking can be implemented in spatial or frequency domain. Spatial domain methods insert watermark signals in cover image by directly changing pixel values. In general, spatial domain schemes have the advantages of low complexity and easy implementation but they tends to be susceptible to attacks. Compared to spatial domain, transform domain schemes in which the watermark signals are hidden by altering frequency coefficients of a transformed image, are generally considered to be robust against attacks. However, their data capacities are very limited since the embedding of high-capacity watermark in the frequency domain would degrade the image quality significantly. The most widely used transforms include discrete cosine transform (DCT) [8, 17, 22–26, 28], discrete wavelet transform (DWT) [41, 42], discrete Fourier transform (DFT) [38–40], and singular value decomposition (SVD) [7, 10, 16, 37], etc. Transform domain methods are very popular for exploiting the spectral characteristics of image transforms and human visual perception. Das et al. [8] presented a novel blind watermarking algorithm in DCT domain using the correlation between two DCT coefficients of adjacent blocks in the same position. A robust blind watermarking technique based on DCT coefficient modification was proposed by Parah et al. [28], where the difference between two DCT coefficients of the adjacent blocks at the same position was needed to be calculated. Lin et al. [17] introduced an improved image watermarking technique in

which the watermark was embedded into a digital image by modifying the low-frequency coefficients in DCT frequency domain. A new approach based on CRT for watermarking of images in the DCT domain for authentication and copyright protection was addressed by Patra et al. [23]. Verma et al. [41] provided a new approach for watermark extraction using support vector machine (SVM) with principal component analysis (PCA) based feature reduction where the original cover image was decomposed up to three level using lifting wavelet transform (LWT) and low-pass sub-band was selected for data hiding purpose. The wavelet transform provides excellent spatial-frequency localization and multi-resolution properties. Energy compaction capability of DCT is useful for adjusting invisibility constraints. By reason of its own intrinsic properties, SVD is widely utilized as watermark embedding domain in the literature, especially in the key steps of watermark embedding. In watermark methods based on SVD, the watermark bits are usually inserted into the singular values or singular vectors of the cover signal. Su et al. [37] suggested a novel watermarking algorithm based on the improved compensation of SVD in which the watermark bit was embedded into 4×4 block by modifying the second row first column and the third row first column elements of U component. Chung et al. [7] developed a watermarking algorithm in which the watermark was embedded into U and V components of the SVD. Fan et al. [10] designed a watermarking scheme that the watermark is embedded by changing the relation between the second and third coefficients in the first column of U component of SVD. Lai [16] presented an improved SVD-based watermarking scheme where the watermark was embedded into the selected blocks by modifying the entries in U orthogonal matrix of each block.

In recent decades, various robust image watermark methods have been proposed. In these schemes, image transforms are indispensable. Transform domain watermark techniques are effective in terms of stronger robustness and higher imperceptibility. Some researchers have suggested the use of two or three transforms to develop new watermarking schemes. Multiple domain image watermarking of combining two or more transforms has been developed in the direction of providing more robust and imperceptible, such as DWT+SVD [1, 4, 5, 20, 21, 46], DWT+DCT [6, 13, 15, 27], DCT+SVD [3, 9, 18], DWT+DCT+SVD [12, 30–35, 44]. Zheng et al. [46] developed a blind watermark method of combining DWT and SVD where the watermark is embedded by modifying the singular values in U components of SVD. Makbol et al. [20] used DWT-SVD image transform and human visual system to improve performance of watermarking scheme where watermark was embedded by modifying several elements in its U matrix. Ahn et al. [4] introduced an image watermarking scheme where the watermark bits were embedded into the target blocks by modifying the first column coefficients of the left singular vector matrix of SVD decomposition. DWT and SVD were employed in a robust and secure watermarking scheme by Irshad et al. [5]. Agoyi et al. [1] developed a novel watermarking scheme based on DWT, chirp z-transform (CZT) and SVD. Kumar et al. [15] proposed a new watermarking algorithm for digital images by cascading of biorthogonal wavelet transforms (BWT) and DCT where embedding of watermark data was done in middle frequency component by comparison-based correlation technique. Ali et al. [3] described a digital image watermarking algorithm based on a combination of DCT and SVD, the advantage of the algorithm is that it automatically chooses the appropriate multiple scaling factors. Ling et al. [18] addressed a watermarking scheme based on a hybrid of SVD and DCT. Elayan and Ahmad [9] developed a DCT-SVD based digital image watermarking scheme that made use of Arnold transform with a view to improving the robustness against different types of attacks while preserving the perceptual quality. Singh et al. [34] presented a secure multiple watermarking method based on DWT, DCT and SVD, where the watermark was embedded in the singular values of DWT subbands. Singh [30] provided a new robust hybrid multiple

watermarking technique using fusion of DWT, DCT and SVD which provided extra level of security with the acceptable performance in terms of robustness and imperceptibility. Singh et al. [31] proposed a robust and blind watermarking scheme based on DWT-SVD and DCT with Arnold cat map encryption for copyright protection. Hu et al. [12] presented a novel scheme to implement blind image watermarking based on the feature parameters extracted from a composite domain including DWT, SVD and DCT. Singh et al. [32] developed a hybrid image watermarking technique based on DWT, DCT and SVD against signal processing attacks.

The main limitation of the existing image watermarking techniques for copyright protection is difficult to obtain a favorable trade-off between imperceptibility and robustness. To take full advantage of image transforms, we design a novel combination of DWT, DCT and SVD for robust and invisible blind image watermarking. More specifically, we select LL component in DWT domain for purpose of improving the robustness and transparency of watermarking using multiscale analysis. A number of particular middle frequency coefficients in DCT domain are chosen for watermark embedding considering the capacity of resistance to low-pass filtering, noise addition, JPEG compression, etc. and the visual quality of watermarked images according to human visual system (HVS). In SVD domain, The largest singular value is modified to embed the watermark bit for the robustness of watermarking against diversified image processing attacks. In recent literatures, most authors concentrated on embedding binary watermarking into the gray-level cover images for protecting multimedia data. For binary image watermark, there are generally two ways to implement the watermarking [13]. One is to map chosen frequency coefficients to a dichotomized field in accordance with the bit value. The quantization index modulation (QIM) [13] is the most common technique in this way. The other way is to modify specific coefficients into paired groups so that each binary bit is manifested by the relationship of the paired groups [8, 46]. In this work, we employ the latter for its universality and flexibility.

The main purpose of this work is to develop a DWT-DCT-SVD based robust and invisible blind image watermarking scheme for obtaining a better tradeoff between imperceptibility and robustness requirements. The use of selected medium-frequency DCT coefficients, optimal embedding strength and flexible embedding strategy provides better adaptability and greater robustness in resisting image processing operations. In the proposed scheme, the LL subband of cover image in DWT domain is segmented into 8×8 blocks and each block is processed by DCT transform. In each block of DCT coefficients, certain middle frequency coefficients are selected to compose a modulation matrix. And then the modulation matrix is decomposed by SVD transform, the largest singular value is made use of embedding watermark. Based on analyzing the relationship between the quality degradation of the watermarked image and the accuracy of the recovered watermark, the optimal watermark embedding strength is estimated using least squares curve fitting technique. The security of the proposed watermarking scheme is improved using logistic chaotic map. The main highlights of this paper are those a watermarking scheme based on a new blend of DCT and SVD in DWT domain is presented and it provides an alternative to optimizing embedding strength technique.

This paper is organized as follows. We present the fundamental concepts and theories in Section 2. Section 3 depicts the proposed watermarking scheme in detail. Section 4 provides the experimental results and analysis, shows the superiority in comparison with other existing techniques and briefly discusses with the proposed scheme. Section 5 summarizes and concludes the paper.

2 Background Theory

The proposed work based on DWT, DCT, SVD, logistic chaotic map and least-squares curve fitting requires certain mathematical concepts. Hence, a brief description of these mathematical theories is discussed as follows.

2.1 Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform is an important and powerful signal processing technique used to divide signals into 4 separate subbands, namely LL (approximation details), HL (horizontal details), LH (vertical details) and HH (diagonal details) sub-bands [36]. The process can be repeated to obtain multi-scale wavelet decomposition. An image may be filtered by 2D DWT into approximation and detail with multiple-levels, which reveals a multi-resolution perspective. The advantages of DWT include excellent localization in time and frequency domains, symmetric spread distributions, multi-resolution characteristics and in accord with the principle of HVS. DWT is widely applied to image processing. In this work, it helps us to achieve preferable robustness and invisibility properties of the proposed watermarking scheme.

2.2 Discrete Cosine Transform

The discrete cosine transform (DCT) was introduced by Ahmed et al. [2]. Considering the case of a gray-scale image f(x,y), $0 \le x, y \le N-1$. The forward two-dimensional DCT can be expressed as [19]:

$$F(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)\pi}{2N}u\right]\cos\left[\frac{(2y+1)\pi}{2N}v\right] \tag{1}$$

where u, v=0, 1, 2,... , N-1. The 2D DCT is a symmetric and orthogonal transformation. α(u), α(v) and the inverse 2D DCT are defined in (2) and (3).

$$\alpha(u) = \begin{cases} 1/\sqrt{N} & u = 0 \\ \sqrt{2/N} & u \neq 0 \end{cases} \quad \alpha(v) = \begin{cases} 1/\sqrt{N} & v = 0 \\ \sqrt{2/N} & v \neq 0 \end{cases} \tag{2}$$

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)F(u,v)\cos\left[\frac{(2x+1)\pi}{2N}u\right]\cos\left[\frac{(2y+1)\pi}{2N}v\right] \tag{3}$$

The DCT is better at providing energy compaction and decorrelation, and widely used in image compression and signal processing. The DCT helps separate an image into different frequency bands as low frequency (LF), medium frequency (MF) and high frequency (HF) of differing importance (with respect to the image's visual quality) as shown in Fig. 1. Their distributions are from top left to bottom right in a DCT coefficient block as illustrated in Fig. 1(b) and (c). It is observed that the most energy of an image is focused on the low frequency zone (bright region) and the high frequency components corresponding to darker area as shown in Fig. 1(b) have extremely small values and only contain a small ratio of total energy. The watermark signals embedded in DCT coefficients may produce different distortions. The objective image quality metrics mean squared

error (MSE) and peak signal-to-noise ratio (PSNR) are considered, they are inversely proportional to each other according to (16). Watermark embedding in DCT domain can be expressed as

$$F_s^{'} = F_s Q \tag{4}$$

where F_s and F_s' are the matrices of selected DCT coefficients for embedding and corresponding modified DCT coefficients, Q is a set of the weighting factors provided by the watermark signals. It is well known that low frequency coefficients in DCT domain are usually a great deal larger in magnitude than the terms of medium and high frequency regions, depicted by Fig. 1. The fact suggests that the low frequency components play a relatively more important role in the determining image quality. If F_s be from low frequency zone, the MSE of F_s' tends to become larger in value and the corresponding PSNR value tends to lower according to (4), (3) and (16), namely the modifications F_s' caused by same Q in the significant low frequency coefficients should induce more prominent visible impairments to the original image than ones in the unimportant high frequency components. Therefore, the low frequency coefficients are usually avoided in watermarking. On the other hand, if F_s comes from high frequency components with smaller magnitudes, they carry certain image details and can be filtered out easily by lossy JPEG compression and signal processing attacks, although the modifications of watermark embedding can cause insignificant image degradation, the robustness is very poor. Thus the high frequency components are also often omitted in watermarking. In order to achieve a good compromise between imperceptibility and robustness of the proposed scheme, that is with lesser effect on the visual perceptibility of the image and stronger resistance to common attacks, it follows that most adaptive DCT coefficients to be employed for embedding are those in medium frequency region, as displayed in Fig. 1(c) (marked by gray).

2.3 Singular Value Decomposition

For any m×n matrix $A \in R^{m\times n}$ with rank $r \leq \min(m,n)$, there exist two orthogonal matrices $U \in R^{m\times m}$ and $V \in R^{n\times n}$ such that

$$A = U \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}_{m\times n} V^T \tag{5}$$

where $D \in R^{r\times r}$ is a square diagonal matrix, namely $D=\mathrm{diag}(\sigma_1, \sigma_2, ..., \sigma_r)$, with positive diagonal entries called the singular values of A and arranged in decreasing order: $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_r > 0$. The orthogonal matrices U and V are not unique, but the singular values σ_i are. The columns of U and V

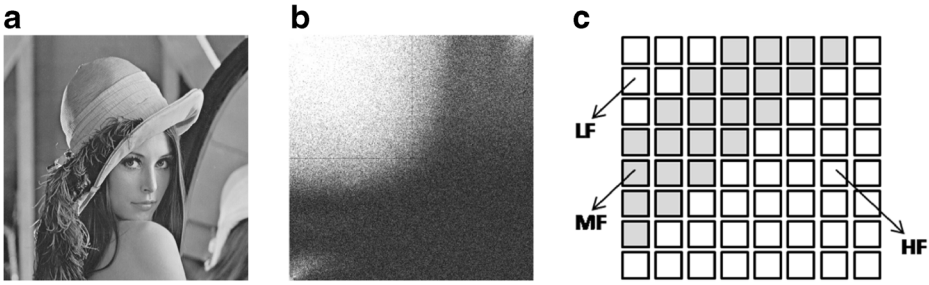


Fig. 1 2D DCT transform of a photograph 'lena'

are referred to as the left-singular vectors and right-singular vectors of A, respectively. SVD is a powerful tool for factorizing matrices that has been frequently applied to digital signal and image processing applications. SVD has particular characteristics, such as good stability. When a data matrix is distorted, the value of its elements or entries changes but the singular value of the matrix has little change. Moreover, singular value has the invariance to translation, zoom and mirror transformation. The stability of SVD, that is being invariant to small perturbations in an image, plays a vital role in signal processing. In watermarking techniques based on SVD, most of watermark embedding procedures are built on the use of singular values or singular vectors.

2.4 Image Encryption using Logistic Chaotic Map

To improve the security of the proposed watermarking scheme, watermark images should be encrypted before embedding. On account of the properties of highly sensitive to initial conditions and parameter values and the ergodicity, chaos maps are widely used in image encryption. Logistic map is a simple and broadly researched chaotic dynamic system. The one-dimensional logistic chaotic map is described as

$$L_{n+1} = \mu L_n(1-L_n) \tag{6}$$

Where L_n represents the population at any given generation n and branch parameter $\mu \in (0,4]$ represents the growth rate. Different sequence will be generated with different initial values and parameters. It has been found that the sequence iterated with an initial value $L_0 \in (0,1)$ for the values of parameter $\mu \in (3.5699456, 4]$ according to (6) is highly chaotic in nature, namely the sequence is neither periodic nor convergent. For this reason, the one-dimensional logistic chaotic map is adopted as in this paper. The encryption and decryption processes using logistic chaotic map are expressed as follows.

$$W_{en} = W_{or} \oplus CS \quad W_{or} = W_{en} \oplus CS \tag{7}$$

Where w_{en} and w_{or} are the encrypted and the original binary watermark sequence, respectively. $\oplus$ denotes XOR operation and CS is the binarization of a chaotic sequence generated from (6). The initial state value L_0 and parameters μ of logistic chaotic map are kept as the secret key. Image encryption using 1D chaotic logistic map is illustrated in Fig. 2. Fig. 2(a)-(c) show three examples including the original watermark images and their corresponding encrypted versions, respectively. As can be seen from them, encrypted watermark images exhibit excellent uncorrelated and random-like (non-periodic) properties.

2.5 Least-Squares Curve Fitting technique

The least squares curve fitting technique is to search the best-fitting curve for some discrete data points by minimizing the sum of the squares of the errors between actual

Fig. 2 Three examples of image encryption using logistic chaotic map

data and fitting function. The most general fitting function is polynomial and can be expressed as

$$\hat{y} = p(x) = C_0 + C_1x^1 + C_2x^2 + \ldots + C_kx^k = \sum_{j=0}^{k} C_jx^j \tag{8}$$

where C_j, j=0, 1, 2,..., k are polynomial coefficients for the best-fitting curve. Assuming that we have several discrete data (x_1, y_1), (x_2, y_2), ... , (x_n, y_n) and p(x) is a function for fitting a curve. The residual for each data point (x_i, y_i) is computed by the difference between the actual data y_i and the fitting function $p(x_i)$ as follows

$$r_i = y_i - p(x_i) = y_i - \sum_{j=0}^{k} C_jx_i^j \tag{9}$$

The least-squares solution gives the C_j, j=0, 1, 2,..., k that minimize $||r||_2^2$, namely

$$(C_0, C_1, \ldots, C_k) = \arg \min\left\{\sum_{i=1}^{n} r_i^2\right\} = \arg \min\left\{\sum_{i=1}^{n}\left(y_i - \sum_{j=0}^{k} C_jx_i^j\right)^2\right\} \tag{10}$$

where n is the number of data points (x_i, y_i) and k is the order number of assumed function.

3 Proposed watermarking scheme

In this section, The proposed watermarking scheme based on DWT-DCT-SVD hybrid domain is elaborated in details. Let *I* and *W* denote the gray-scale cover image of size *M*×*N* and the binary watermark image of size *L*×*L,* respectively. The proposed watermarking scheme mainly includes watermark encryption, watermark embedding, watermark extraction and watermark decryption.

3.1 Watermark encryption

Before embedding the watermark image into the original cover image, the original binary watermark image *W* with the size L×L is scrambled using logistic maps with certain secret key (L_0, μ) to generate a one-dimensional chaotic watermark sequence $W_{en}(i)$ for i=1, 2, . . . , L×L according to (6) and (7). This results in a watermark image without semantic meaning which comprises values of zeros and ones as shown in Fig. 2.

3.2 Watermark embedding process

The proposed watermark embedding procedure is shown in Fig. 3. It can be described in detail as follows:

Step 1: Perform first-level Haar 2D-DWT on the cover image *I* of size *M*×*N*. This produces an approximation coefficient matrix *LL* (low frequency subband) and three detail coefficient matrices *HL*, *LH*, and *HH* (high frequency subbands).

Step 2: Divide the *LL* coefficient matrix into non-overlapping blocks $\{B^k\}$ of size 8×8, k=1, 2, ..., (M/16×N/16).

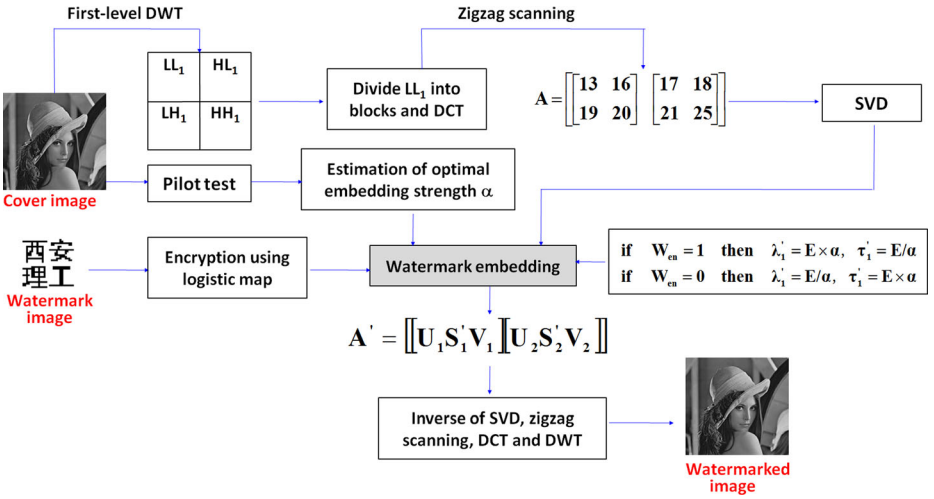


Fig. 3 Block diagram of the proposed watermark embedding process

Step 3: For each block B^k, k=1, 2, ..., (M/16×N/16):

(1) Implement forward 2D-DCT transform to obtain a coefficient matrix D.
(2) Zigzag scan coefficient matrix D to produce a vector a=[a_1, a_2,..., a_{64}] and its 8 components (13th, 16th, 17th, 18th, 19th, 20th, 21th, 25th) are extracted to construct a modulation matrix MM with 2 rows and 4 columns.

Zigzag scanning and mapping pattern of modulation matrix generation is shown in Fig. 4.

(3) Split modulation matrix MM into two same size submatrices MM_1 and MM_2 with 2 rows and 2 columns as shown in Fig. 4.
(4) Apply SVD transform to each of two submatrices and extract their largest singular values λ_1 and τ_1 as follows:

$$[U_i \quad S_i \quad V_i] = SVD(MM_i) \quad i = 1, 2 \tag{11}$$

$$S_1 = \begin{bmatrix} \lambda_1 & \\ & \lambda_2 \end{bmatrix} \quad S_2 = \begin{bmatrix} \tau_1 & \\ & \tau_2 \end{bmatrix} \tag{12}$$

(5) Assume the mean value of λ_1 and τ_1 is equal to E, i.e. E=(λ_1+τ_1)/2. The encrypted watermark sequence bits $W_{en}(i)$ for i=1, 2, . . . , L×L are embedded by modifying the largest singular values λ_1 and τ_1 according to the following criterion:

$$\begin{array}{llll} if & W_{en} = 1 & then & \lambda_1' = E \times \alpha \quad \tau_1' = E/\alpha \\ if & W_{en} = 0 & then & \lambda_1' = E/\alpha \quad \tau_1' = E \times \alpha \end{array} \tag{13}$$

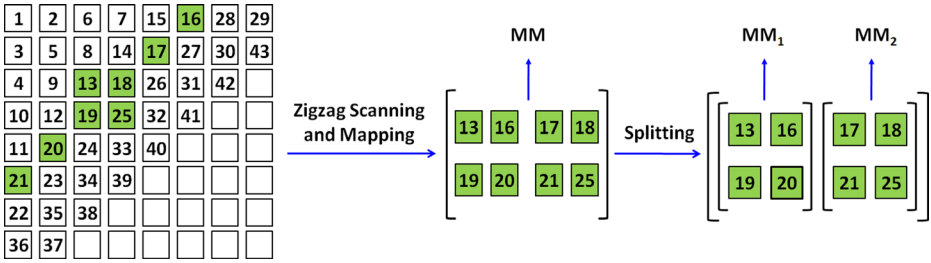


Fig. 4 Zig-zag scanning, mapping pattern and partitioning of selected coefficients (marked by green)

where λ'_1 and τ'_1 are the modified values of λ_1 and τ_1, respectively, the parameter α denotes the embedding strength factor of watermark. Through experiment, The value of α is usually restricted to [1 2].

(6) Two altered submatrices $MM_1^{'}$ and $MM_2^{'}$ are reconstructed by inverse SVD transform as follows:

$$MM_1 = U_1 \begin{bmatrix} \lambda_1^{'} & \\ & \lambda_2 \end{bmatrix} V_1^T \quad MM_2 = U_2 \begin{bmatrix} \tau_1^{'} & \\ & \tau_2 \end{bmatrix} V_2^T \tag{14}$$

then the changed modulation matrix MM' is obtained by merging them.

(7) All entries in the modulation matrix MM' are mapped back to their respective original positions in DCT coefficient matrix D, and then we obtain the altered coefficients matrix D'. A watermarked block $B^{k'}$ is obtained by performing inverse 2D-DCT transform on matrix $D^{'}$.

When all divided blocks $\{B^k\}$, k=1, 2, ..., M/16×N/16 are transformed into $\{B^{k'}\}$, k=1, 2, ..., (M/16)×(N/16) according to procedures (1)-(7), embedding of the encrypted watermark sequence bits $W_{en}(i)$ for i = 1, 2, ... , L×L, is finished. Here (L×L) is equal to (M/16)×(N/16).

Step 4: The modified coefficient matrix LL' is obtained by combining all blocks $\{B^{k'}\}$, k=1, 2, ..., (M/16×N/16).

Step 5: Apply inverse Haar 2D-DWT transform to obtain the watermarked image I' by utilizing above-mentioned three detail coefficient matrices *HL*, *LH*, and *HH* and the modified coefficient matrix LL'.

3.3 Watermark extraction process

The watermark extraction process requires only the watermarked image without the need for the original cover image and watermark image. The proposed watermark extraction procedure is shown in Fig. 5. The detailed watermark extraction procedure is depicted as follows:

Step 1: Perform the first-level Haar 2D-DWT transform on the grayscale watermarked image I' of size $M \times N$.

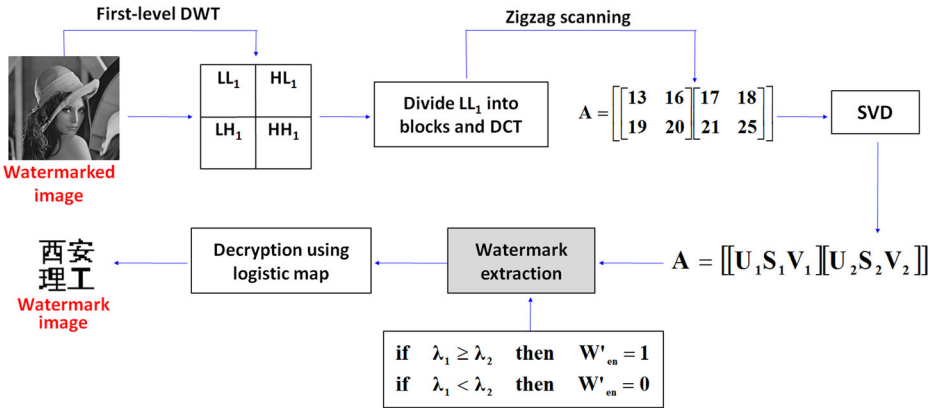


Fig. 5 Block diagram of the proposed watermark extraction process

Step 2: Divide the coefficient matrix *LL* into non-overlapping blocks $\{B^k\}$ with the size 8×8 pixels.

Step 3: For each block:

(1) Compute the forward DCT and produce a coefficient matrix D.

(2) Zigzag scan coefficient matrix D to generate a vector a=[a_1, a_2,..., a_{64}]. Then extract its 8 components (13th, 16th, 17th, 18th, 19th, 20th, 21th, 25th) to construct a modulation matrix MM with 2 rows and 4 columns.

Zigzag scanning and mapping pattern of matrix generation are shown in Fig. 4.

(3) Split a modulation matrix MM into two same size submatrices MM_1 and MM_2 with 2 rows and 2 columns as shown in Fig. 4, and then perform SVD transform on them to extract their largest singular values λ_1 and τ_1.

(4) The extraction of watermark bit $W_{en}(i)$ is performed according to the following criterion:

$$\begin{array}{llll} if & \lambda_1 \geq \tau_1 & then & W_{en} = 1 \\ if & \lambda_1 < \tau_1 & then & W_{en} = 0 \end{array} \tag{15}$$

where λ_1 and τ_1 are the largest singular values of two submatrices MM_1 and MM_2 respectively.

Step 4: When all blocks are processed by procedures (1)-(4), encrypted watermark sequence bits $W_{en}(i)$ for $i = 1, 2, \ldots, L\times L$, are extracted completely.

3.4 Watermark decryption

The process of decryption is similar to the encryption process. The logo watermark image *W* with the size $L\times L$ is acquired by decryption of watermark sequence $W_{en}(i)$ for $i = 1, 2, \ldots, L\times L$ using logistic chaotic map with secret key (L_0, μ) according to (7).

4 Experiment results and discussions

4.1 Experimental data sets

In this section, the performance of the proposed watermarking scheme is evaluated on some standard 8-bit gray-scale test images with size 512 × 512 pixels. They are shown in Fig. 6, used as cover images, namely 'Boat', 'Lena', 'Livingroom', 'Mandrill', 'Peppers', 'Pirate', 'Jetplane', and 'Lake'. Three 2-bit 32×32 binary logo images are selected to act as the watermark images, as shown in Fig. 7.

To demonstrate the efficiency of the proposed scheme, we selected some earlier important works [1, 3, 8, 9, 12, 17, 23, 28, 30, 31, 34, 35, 37, 41, 44] as comparison methods in terms of the robustness and imperceptibility, where their watermark embedding domains are shown in Table 1. All experiments are coded by Matlab R2015b.

4.2 Performance Measures

The performance of the proposed watermarking scheme can be evaluated on the basis of its robustness and imperceptibility. The imperceptibility is generally assessed by the image distortion induced between the watermarked and original images due to watermark embedding, and it is measured by Peak Signal-to-Noise Ratio (PSNR), Structural SIMilarity (SSIM) index [43] and Feature SIMilarity (FSIM) index [45] objectively. The PSNR is used to analyze the visual quality of watermarked images, and it can display the perceptual transparency of the watermarked image with respect to the original cover image. PSNR is depicted as follows:

$$PSNR = 10 \times \log_{10}\left(\frac{f_{peak}^2}{MSE}\right) = 10 \times \log_{10}\left(\frac{f_{peak}^2}{\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[f(i,j)-f'(i,j)\right]^2}\right) \text{dB} \quad (16)$$

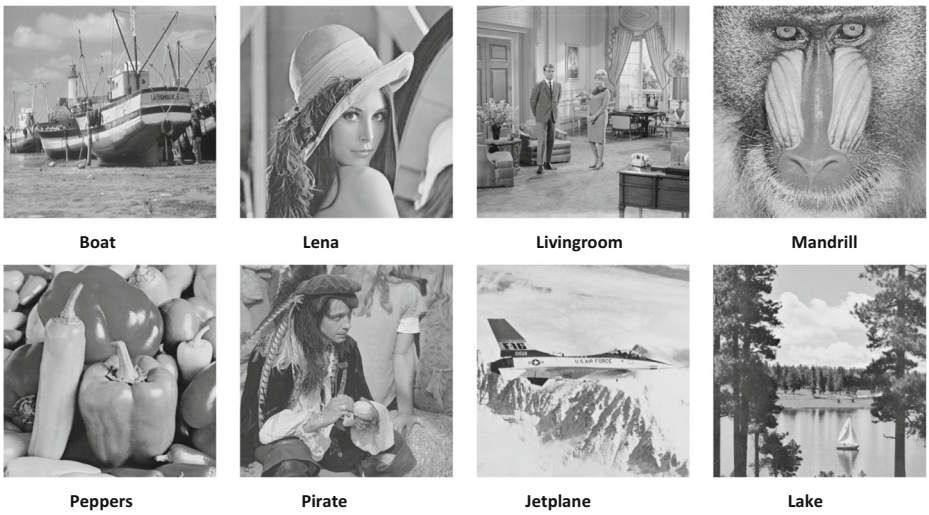


Fig. 6 Cover images for test

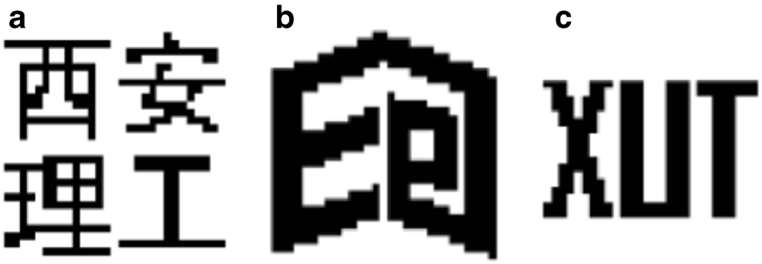


Fig. 7 Three binary watermark images used in experiment

where mean squared error (MSE) measures the average of the squares of the errors or deviations, f_{peak} represents the peak intensity level in the original image f, which is most commonly taken as 255 for an 8-bit gray-scale image, f(i,j) and f'(i,j) indicate the value of pixel (i,j) of original image and watermarked one respectively, and M,N denote the width and the height of cover image, respectively. High PSNR value implies less distortions induced and better invisibility. In general case, the quality of the watermarked image can be thought as acceptable when the PSNR value is above 30dB.

The SSIM [43] describes the luminance, contrast and structure attributes of the images for similarity measurement. It is defined as follows:

$$SSIM = \left[L\left(f,f^{'}\right)\right]^{\alpha} * \left[C\left(f,f^{'}\right)\right]^{\beta} * \left[S\left(f,f^{'}\right)\right]^{\gamma} \tag{17}$$

$$\begin{cases} L\left(f,f^{'}\right) = \dfrac{2\mu_f\mu_{f'} + C_1}{\mu_f^2 + \mu_{f'}^2 + C_1} \\ C\left(f,f^{'}\right) = \dfrac{2\sigma_f\sigma_{f'} + C_2}{\sigma_f^2 + \sigma_{f'}^2 + C_2} \\ S\left(f,f^{'}\right) = \dfrac{\sigma_{ff'} + C_3}{\sigma_f\sigma_{f'} + C_3} \end{cases} \tag{18}$$

where three functions L(f,f'), C(f,f'), and S(f,f') are the luminance, the contrast and the structure comparison functions respectively, $\alpha>0$, $\beta>0$ and $\gamma>0$ are parameters used to adjust the relative importance of the three components, f and f' are the original and the watermarked images, respectively. μ_f, $\mu_{f'}$, σ_f, $\sigma_{f'}$ and $\sigma_{ff'}$ are the corresponding mean luminance values, standard deviations and cross-covariance of two images f and f' separately. C_1、C_2 and C_3 are constant terms with smaller values. If $\alpha = \beta = \gamma = 1$ and $C_3 = C_2/2$, the SSIM index simplifies to:

$$SSIM\left(f,f^{'}\right) = \frac{\left(2\mu_f\mu_{f'} + C_1\right)\left(2\sigma_{ff'} + C_2\right)}{\left(\mu_f^2 + \mu_{f'}^2 + C_1\right)\left(\sigma_f^2 + \sigma_{f'}^2 + C_2\right)} \tag{19}$$

Based on the fact that human visual system (HVS) understands an image mainly according to its low-level features, the feature similarity (FSIM) index [45] is proposed for full-reference Image quality assessment. Two important local features, phase congruency (PC) and gradient magnitude (GM) play complementary roles in characterizing the image local quality for FSIM.

Table 1 Comparison methods and their watermark embedding domains

Methods	[8]	[17]	[37]	[9]	[41]	[34]	[30]	[44]
Domains	DCT	DCT	SVD	DCT+SVD	LWT+SVM+PCA	DWT+DCT+SVD	DWT+DCT+SVD	DWT+DCT+SVD
Methods	[28]	[23]	[1]	[3]	[35]	[31]	[12]	Proposed
Domains	DCT	DCT	DWT+SVD	DCT+SVD	NSCT+DCT+MSVD	DWT+DCT+SVD	DWT+DCT+SVD	DWT+DCT+SVD

The FSIM index between two images $f_1(x)$ and $f_2(x)$ is defined as

$$FSIM = \frac{\sum_{x\in\Omega} S_L(x)\cdot PC_m(x)}{\sum_{x\in\Omega} PC_m(x)} \tag{20}$$

$$PC_m(x)^m = \max\{PC_1(x), PC_2(x)\}, S_L(x) = [S_{PC}(x)]^{\alpha}\cdot[S_{GM}(x)]^{\beta} \tag{21}$$

$$S_{GM}(x)^{GM} = \frac{2GM_1(x)\cdot GM_2(x) + T_2}{GM_1^2(x)\cdot GM_2^2(X) + T_2}, S_{PC}(x)^{PC} = \frac{2PC_1(x)\cdot PC_2(x) + T_1}{PC_1^2(x)\cdot PC_2^2(X) + T_1} \tag{22}$$

Where Ω indicates the whole image spatial domain, α and β are parameters used to adjust the relative importance of PC and GM features, we set α=β=1 for simplicity. T_1 and T_2 are two positive constants depending on the dynamic ranges of PC and GM values respectively.

The robustness means the capability that the watermarked image can withstand various attacks, which include two groups: signal processing such as filtering, noise addition, lossy compression, and geometric transformations such as scaling, cropping, etc. It is assessed by Bit Error Rate (BER) and Normalized Correlation (NC) between the original watermark and the extracted one. The BER is defined as ratio between number of error bits and total number of bits. It is depicted as follows:

$$BER = \frac{1}{P_W \times Q_W}\sum_{i=1}^{P_W}\sum_{j=1}^{Q_W}\left[W(i,j)\oplus W'(i,j)\right] \times 100\% \tag{23}$$

where W(i,j) and W'(i,j) are original watermark and extracted one, respectively, with same size of $P_W \times Q_W$. ⊕ indicates the exclusive-or (XOR) operation. The lower the BER value is, the better the robustness is. The NC is used to evaluate the similarity and difference between the extracted watermark and the original watermark. It is computed as follows:

$$NC = \frac{\sum_{i=1}^{P_W}\sum_{j=1}^{Q_W}\left[W(i,j)\times W'(i,j)\right]}{\sqrt{\sum_{i=1}^{P_W}\sum_{j=1}^{Q_W} W^2(i,j)}\sqrt{\sum_{i=1}^{P_W}\sum_{j=1}^{Q_W} W'^2(i,j)}} \tag{24}$$

where W and W' are the original and extracted watermarks with same size of $P_W \times Q_W$, respectively. The NC value generally lies between 0 and 1. If the value of NC is closer to 1, it indicates there is lesser difference or very high similarity between the two images.

4.3 Estimation of watermark embedding strength

Before the formal experiments, a pilot test including watermark embedding and extracting process is conducted to estimate an optimal embedding strength α in accordance with the content of a cover image. As known, embedding the watermark signals into an image will degrade the visual quality of the image. In addition to that, the embedded data can be immune to signal processing or manipulation attacks to some extent. This determines that the robustness and imperceptibility compose a conflicting relation. Too high imperceptibility in embedding the watermark may lead

to decreasing the robustness, vice versa. Considering these metrics of performance, high PSNR and SSIM values between the original and watermarked image usually signal good imperceptibility, low BER values or high NC values between the original and extracted watermark also indicate strong robustness. For SSIM and NC, representing the imperceptibility and the robustness respectively, although they all are similarity measurement between two images and range from 0 to 1, they are usually opposite, that is when the SSIM value is high, the corresponding NC value tend to be low, and vice versa. It is a very important issue to seek the best balance between the two variables. Fig. 8(a) and Fig. 8(c) show the PSNR and SSIM values under different embedding strength α for image 'mandrill', respectively. Fig. 8(b) and Fig. 8(d) show the relationshop between the corresponding averaged BER and NC values under four kinds of typical attacks and watermark embedding strength α, severally. These representative attacks include Gaussian noise (mean=0 and variance = 0.005), JPEG compression (QF=30), Gaussian filtering (sigma=1.0) and histogram equalization. As can been seen from Fig. 8, the larger watermark embedding strength α is, the worse the quality of the watermarked image becomes while the better the robustness of watermark scheme is. If a suitable embedding strength α is chosen, the PSNR/SSIM of the watermarked image and the BER/NC of the extracted watermark are acceptable. Especially for SSIM and NC, they have not only a same data range, but also similar changing trend in addition to opposite direction. A best embedding strength α may be found out by pre-embedding and pre-extracting process for a specific cover image, which can balance well both imperceptibility and robustness. Once the pre-embedding and pre-extracting process are performed, two relational graph can be drawn, one displays the relationship between SSIM and watermark embedding strength α, the other shows the correlation

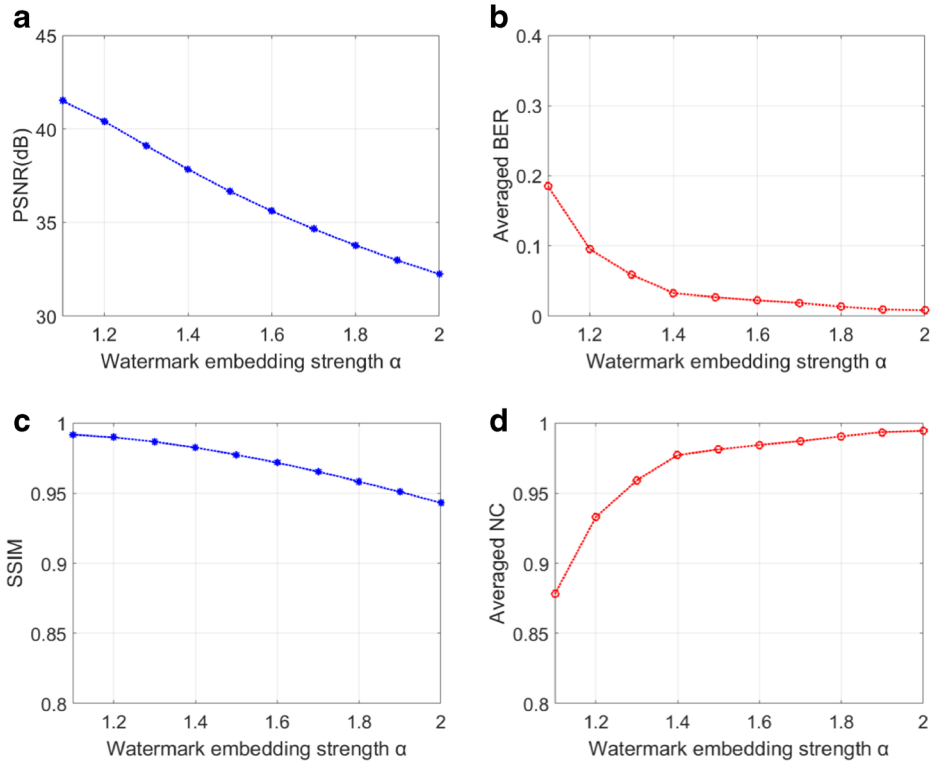


Fig. 8 The relationshop between PSNR/SSIM, BER/NC and watermark embedding strength α

between NC and watermark embedding strength α. They represent the imperceptibility and robustness of the proposed scheme, respectively.

In order to achieve the best trade-off between the imperceptibility and robustness, the optimal embedding strength value α can be estimated by minimizing absolute difference between SSIM and NC as follows:

$$\alpha_{optimal} = \arg \min_{\alpha \in [t_1, t_2]} \{|p_{SSIM} - p_{NC}|\} \tag{25}$$

subject to

$$\{BER \in [0, ET_1]\} \cap \{PSNR \in [ET_2, \propto]\} \tag{26}$$

Where p_{SSIM} and p_{NC} are polynomial fitting functions of SSIM and NC respectively, according to (8), (9) and (10). ET_1 and ET_2 are two experience thresholds, which depend on watermarking applications. In this paper, embedding strength $\alpha \in [1.1, 2.0]$, ET_1=0.05 and ET_2=34 dB.

According to above-mentioned method, the SSIM and mean value of NC under various conventional attacks for eight cover images (as shown in Fig. 6) all can be fitted with different polynominal functions and are shown in Fig. 9(a)-(h). For embedding strength $\alpha \in [1.1, 2.0]$, the former function is monotone decreasing while the latter function is monotonic increasing. In order to achieve a balance between image quality and resistance to attacks, we seek optimal embedding strength α by minimizing absolute difference between the two functions. As shown in Fig. 9(a), when the NC and SSIM values are all 0.9795, the value of optimal embedding strength α is 1.46 conformed by the constraint PSNR=37.14 dB and BER=0.0294.

4.4 Imperceptibility analysis

For assessing the imperceptibility, we utilize PSNR and SSIM/FSIM to measure the similarity between the original cover image and the watermarked one. We have evaluated the proposed scheme on eight cover images *Boat*, *Lena*, *Livingroom*, *Mandrill*, *Peppers*, *Pirate*, *Jetplane* and *Lake* as shown in Fig. 6. At respective optimal embedding strength α, the PSNR and the corresponding SSIM/FSIM values of eight different watermarked images are graphically presented in Fig. 10 and Fig. 11. The average values of three metrics are 38.63dB, 0.9662 and 0.9757, respectively, which signify high image quality. In addition, the PSNR values for test images 'Mandrill' and 'Lena' obtained by the proposed scheme have been compared with five previous methods Lin et al. [17], Agoyi et al. [1], Elayan et al. [9], Ali et al. [3] and Singh et al. [30] as shown in Fig. 12(a) and (b). In this experiment for perceptual transparency verification, the proposed scheme achieves superior perceptual quality of watermarked image than other methods [1, 3, 9, 17, 30].

4.5 Robustness analysis

In this subsection BER and NC values between the original watermark and the extracted watermark are computed for evaluating the robustness of the proposed scheme against different kinds of image attacks. The image attacks can be categorised into signal processing and geometrical transform. Signal processing attacks include image compression, addition of white Gaussian noise, salt and pepper noise and speckle noise, median filtering, Gaussian low-pass filtering, average filtering, histogram equalization, sharpening and contrast adjustment.

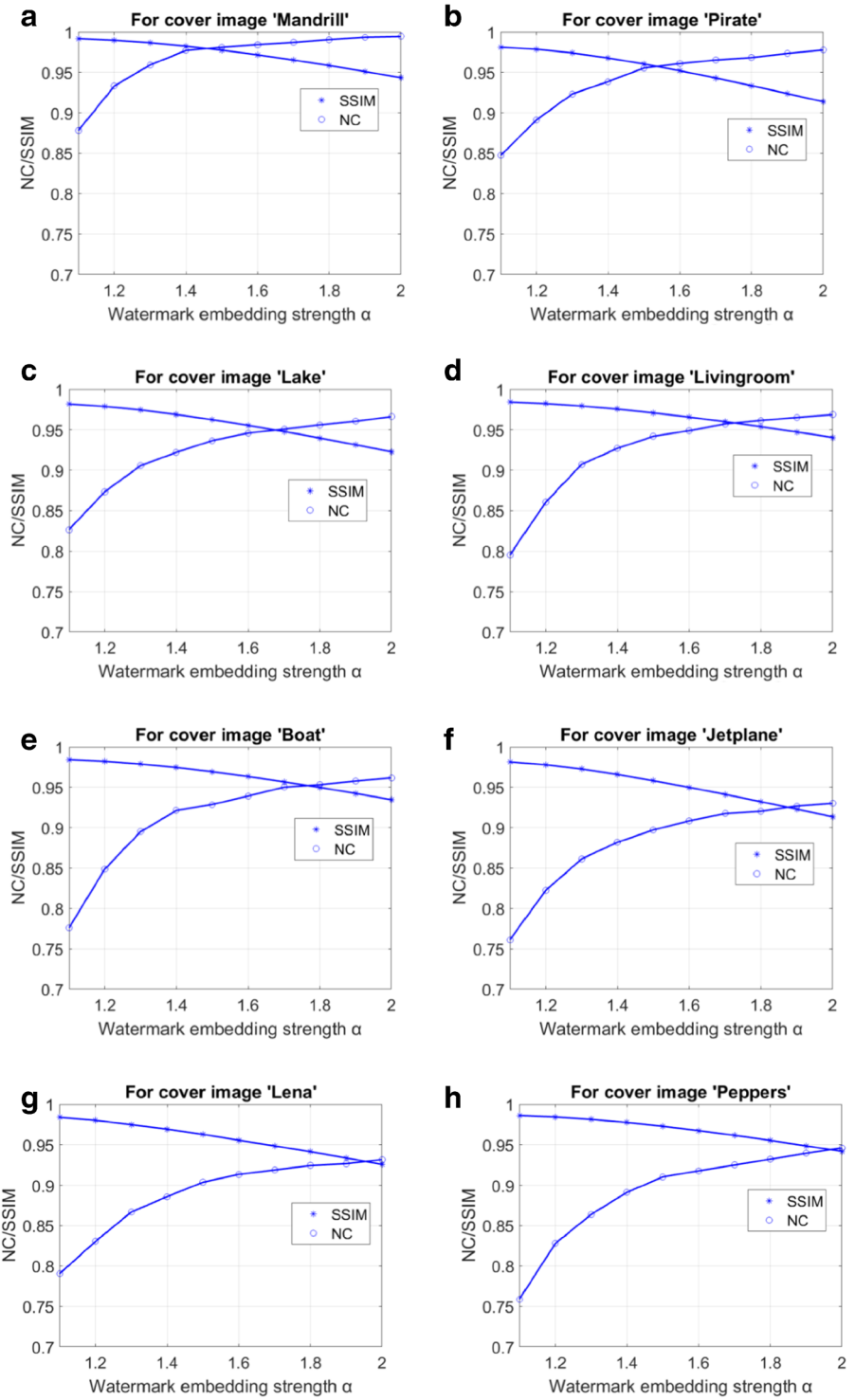


Fig. 9 The relationship between robustness and imperceptibility

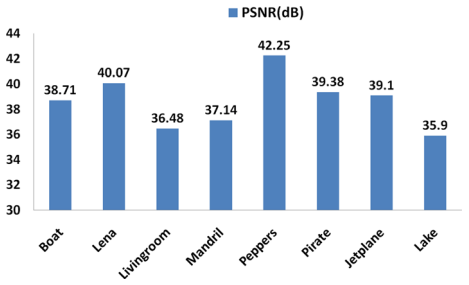


Fig. 10 PSNR values of eight watermarked images for assessing the transparency

Geometrical transform attacks contain image resizing and cropping. The types of image attacks considered in this work are detailed as follows:

1. JPEG compression: JPEG compression with quality factor (QF) chosen from {70, 50, 30, 20, 10} is applied to the watermarked image.

2. JPEG2000 compression: JPEG2000 with compression ratio (CR) chosen from {2, 4, 8} is applied to the watermarked image.

3. Gaussian noise: Gaussian noise with the mean (m=0) and variance (v) set at {0.005, 0.01, 0.015} is added to the watermarked image.

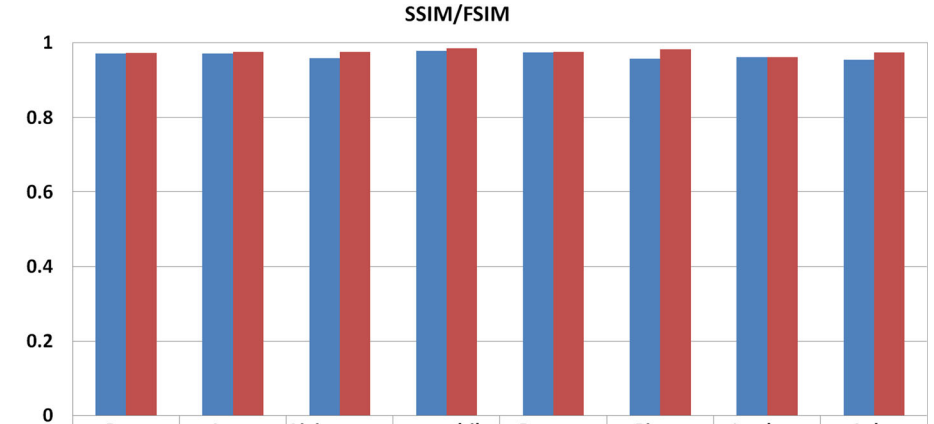
4. Salt-and-pepper noise: The watermarked image is corrupted by the salt-and-pepper noises with 1% and 2% density.

5. Speckle noise: multiplicative speckle noise with the variance v chosen from {0.01, 0.02, 0.05} is added to the watermarked image.

6. Median filtering: The watermarked image is filtered by a median filter with a 3×3 or 5×5 mask.

7. Average filtering: The watermarked image is filtered by an average filter with a 3×3 or 5×5 mask.

8. Gaussian filtering: The watermarked image is filtered by a Gaussian filter with sigma chosen from {0.5, 1.0, 1.5}.



	Boat	Lena	Livingroom	mandril	Peppers	Pirate	Jetplane	Lake
SSIM	0.9714	0.972	0.9585	0.9795	0.9747	0.9572	0.9613	0.955
FSIM	0.9728	0.9758	0.9759	0.9857	0.9759	0.9836	0.9618	0.9741

Fig. 11 SSIM/FSIM values of eight watermarked images for assessing the transparency

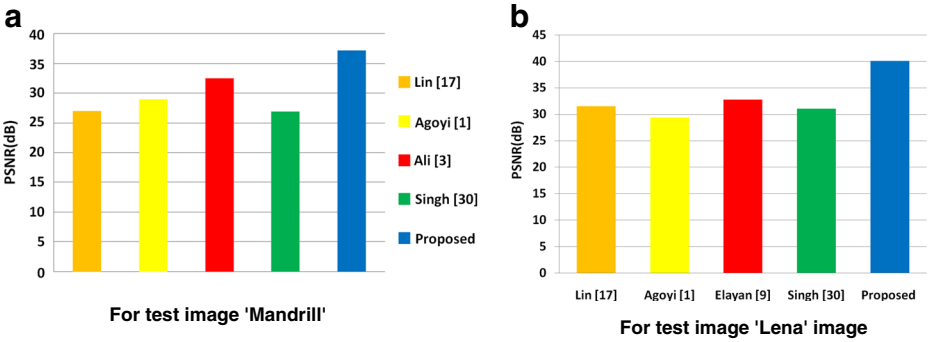


Fig. 12 PSNR comparison

9. Histogram equalization: The watermarked image is processed by histogram equalization or adaptive histogram equalization.

10. Contrast adjustment: The watermarked image is processed by contrast adjustment.

11. Scaling: The size of the watermarked image above is reduced from 512×512 to 256×256 pixels and subsequently enlarged from 256×256 to 512×512 pixels, or enlarged from 512×512 to 1024×1024 pixels and reduced from 1024×1024 to 512×512 pixels.

12. Cropping: The watermarked image is cropped by 25% or 50% on the upper left corner.

13. Sharpening: The watermarked image is filtered by a highpass filter.

The NC and BER values of the extracted watermark for test images under various attacks are listed in Table 2. Some watermarked images attacked by the most common signal processing and geometric operations and the corresponding extracted watermarks for test image 'Mandrill' are shown in Fig. 13. It can be observed from it that the proposed scheme can obtain satisfactory results. As can be seen from Table 2, most of the NC values of the extracted watermarks are greater than 0.9 and the corresponding BER values are lesser than 0.1. It demonstrates the stronger performance of the proposed scheme in terms of robustness against most common attacks including image JPEG compression, JPEG2000 compression, filtering, contrast adjustment, histogram equalization, scaling, sharpening, and so on.

JPEG and JPEG2000 are the two widely used image compression standards. The BER and NC values of the extracted watermarks under JPEG and JPEG2000 image compression attacks are shown in Fig. 14. For JPEG lossy compression attacks, the range domain of quality factor (QF) is from 10 to 100, whereas for JPEG2000 compression attacks, the compression ratio (CR) is varied from 1 to 10. It is easy to note that for JPEG compression QF > 50, the NC values approach 1 and the corresponding BER values appear close to 0%, while for JPEG2000 compression CR < 5, the NC values are greater than 0.96 and the corresponding BER values are less than 5%. For QF > 20 or CR<9, all NC and BER values are considered acceptable. The proposed watermarking scheme shows excellent robustness against JPEG compression and JPEG2000 compression attacks.

In order to show the advantage of the proposed scheme in terms of robustness, the NC and BER comparison for test image 'Pirate', 'Mandrill ' and 'Lena' under different attacks with other seven different approaches are shown in Fig. 15-17. Singh et al. [31] and Verma et al. [41] work fairly well in resistance to image JPEG compression. Fig. 15(a) & (b) show the NC values of the proposed scheme from the extracted watermarks attacked by JPEG compression at various levels comparing with the two methods, respectively. From Fig. 15(a) & (b), as shown comparative results for the test image 'Pirate' and 'Mandrill', it is clear that the

Table 2 NC and BER values of extracted watermarks under various attacks

Attacks	Mandrill		Pirate		Lake		Livingroom		Peppers		Jetplane		Lena	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
No attack	1.0000	0	1.0000	0	1.0000	0	1.0000	0	1.0000	0	1.0000	0	1.0000	0
JPEG compression(QF=10)	0.9195	0.1143	0.8701	0.1836	0.8797	0.1709	0.8698	0.1826	0.7913	0.2861	0.8260	0.2402	0.8382	0.2266
JPEG compression(QF=20)	0.9751	0.0361	0.9268	0.1045	0.9170	0.1191	0.9393	0.0879	0.8842	0.1641	0.8452	0.2148	0.8502	0.2070
JPEG compression(QF=30)	0.9947	0.0078	0.9628	0.0537	0.9302	0.0996	0.9653	0.0508	0.9325	0.0977	0.8885	0.1572	0.8867	0.1582
JPEG compression(QF=50)	0.9980	0.0029	0.9792	0.0303	0.9609	0.0566	0.9907	0.0137	0.9826	0.0254	0.9395	0.0869	0.9449	0.0791
JPEG compression(QF=70)	0.9993	0.0010	0.9913	0.0127	0.9778	0.0322	0.9953	0.0068	0.9967	0.0049	0.9697	0.0439	0.9859	0.0205
JPEG2000 compression(CR=2)	0.9993	0.0010	0.9967	0.0049	0.9906	0.0137	0.9973	0.0039	0.9993	0.0010	0.9913	0.0127	0.9980	0.0029
JPEG2000 compression(CR=4)	0.9987	0.0020	0.9859	0.0205	0.9624	0.0547	0.9887	0.0166	0.9906	0.0137	0.9819	0.0264	0.9893	0.0156
JPEG2000 compression(CR=8)	0.9940	0.0088	0.9637	0.0527	0.9296	0.1025	0.9646	0.0518	0.9557	0.0645	0.9343	0.0957	0.9492	0.0732
Gaussian filtering(sigma=0.5)	1.0000	0	1.0000	0	1.0000	0	1.0000	0	1.0000	0	1.0000	0	1.0000	0
Gaussian filtering(sigma=1.0)	0.9954	0.0068	0.9907	0.0137	0.9920	0.0117	0.9894	0.0156	0.9940	0.0088	0.9947	0.0078	0.9914	0.0127
Gaussian filtering(sigma=1.5)	0.9488	0.0762	0.9506	0.0742	0.9585	0.0615	0.9548	0.0664	0.9606	0.0576	0.9735	0.0391	0.9651	0.0518
Median filtering (3×3)	0.9953	0.0068	0.9913	0.0127	0.9853	0.0215	0.9880	0.0176	0.9765	0.0342	0.9987	0.0020	0.9967	0.0049
Median filtering (5×5)	0.9029	0.1436	0.9083	0.1357	0.9283	0.1064	0.8972	0.1504	0.9073	0.1367	0.9455	0.0791	0.9486	0.0752
Average filtering (3×3)	0.9880	0.0176	0.9873	0.0186	0.9765	0.0342	0.9552	0.0645	0.9723	0.0400	0.9682	0.0459	0.9641	0.0518
Average filtering (5×5)	0.8858	0.1660	0.9172	0.1201	0.9073	0.1357	0.8668	0.1885	0.8926	0.1533	0.9038	0.1377	0.9006	0.1426
Gaussian noise(m=0, v=0.005)	0.9338	0.0947	0.8693	0.1836	0.8945	0.1494	0.8974	0.1445	0.8439	0.2158	0.8344	0.2285	0.8470	0.2100
Gaussian noise(m=0, v=0.01)	0.9227	0.1104	0.8318	0.2324	0.8517	0.2070	0.8365	0.2266	0.8052	0.2666	0.8072	0.2627	0.8142	0.2529
Gaussian noise(m=0, v=0.02)	0.8562	0.1982	0.7739	0.3037	0.8096	0.2598	0.7958	0.2783	0.7787	0.2988	0.7888	0.2861	0.7580	0.3223
Salt & pepper noise(d=0.01)	0.9609	0.0566	0.9269	0.1045	0.9029	0.1377	0.9311	0.0986	0.8941	0.1494	0.8889	0.1572	0.8817	0.1650
Salt & pepper noise(d=0.02)	0.9271	0.1035	0.8609	0.1924	0.8850	0.1621	0.8960	0.1465	0.8544	0.2012	0.8314	0.2334	0.8386	0.2217
Speckle noise (v=0.01)	0.9594	0.0586	0.9289	0.1016	0.9141	0.1221	0.9287	0.1016	0.9096	0.1289	0.8307	0.2334	0.8683	0.1826
Speckle noise (v=0.02)	0.9263	0.1055	0.9081	0.1309	0.8910	0.1533	0.8849	0.1621	0.8642	0.1904	0.8105	0.2578	0.8384	0.2217
Speckle noise (v=0.05)	0.8970	0.1487	0.8409	0.2217	0.8760	0.1748	0.8458	0.2129	0.8166	0.2510	0.7818	0.2949	0.8075	0.2598
Adaptive histogram equalization	0.9993	0.0010	0.9933	0.0098	0.9859	0.0205	0.9913	0.0127	0.9993	0.0010	0.9933	0.0098	0.9960	0.0059
Histogram equalization	0.9953	0.0068	0.9934	0.0098	0.9866	0.0195	0.9874	0.0186	0.9960	0.0059	0.9886	0.0166	0.9953	0.0068
Contrast adjustment	0.9993	0.0010	0.9953	0.0068	0.9927	0.0107	0.9987	0.0020	0.9437	0.0830	0.8738	0.1982	0.9502	0.0732
Sharpening	0.9993	0.0010	0.9953	0.0068	0.9973	0.0039	0.9973	0.0039	0.9993	0.0010	0.9973	0.0039	0.9993	0.0010
Cropping (25%)	0.9557	0.0693	0.9526	0.0742	0.9525	0.0742	0.9557	0.0693	0.9588	0.0645	0.9554	0.0693	0.9574	0.0664
Cropping (50%)	0.9307	0.1133	0.9087	0.1543	0.9212	0.1309	0.9087	0.1543	0.9094	0.1533	0.9061	0.1582	0.9105	0.1504
Resizing (512→256→512)	0.9987	0.0020	0.9886	0.0166	0.9847	0.0225	0.9873	0.0186	0.9987	0.0020	0.9993	0.0010	0.9987	0.0020
Resizing (512→1024→512)	0.9993	0.0010	0.9960	0.0059	0.9900	0.0146	0.9987	0.0020	1.0000	0	1.0000	0	1.0000	0

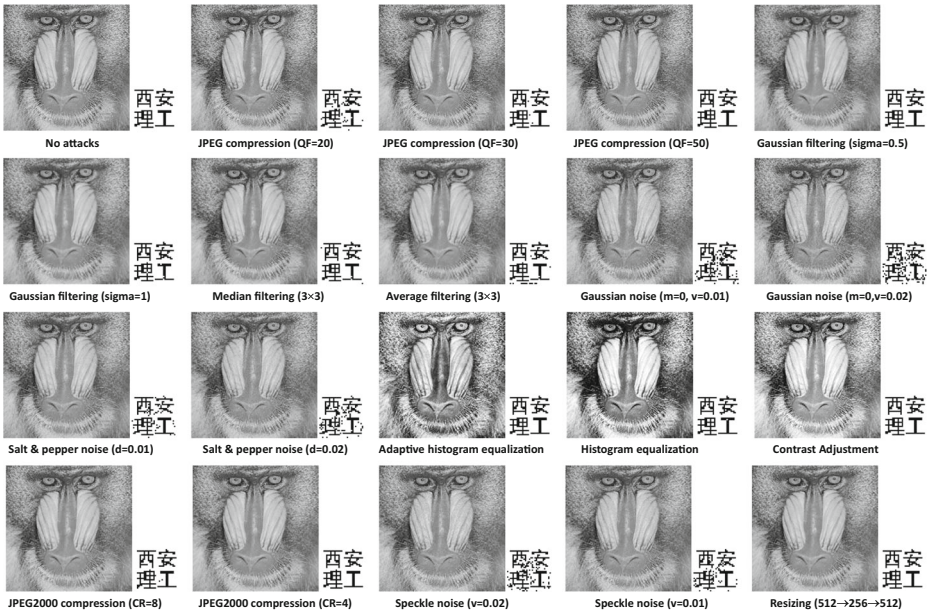


Fig. 13 Watermarked images under different kinds of attacks and the corresponding extracted watermark images for cover image 'Mandrill'

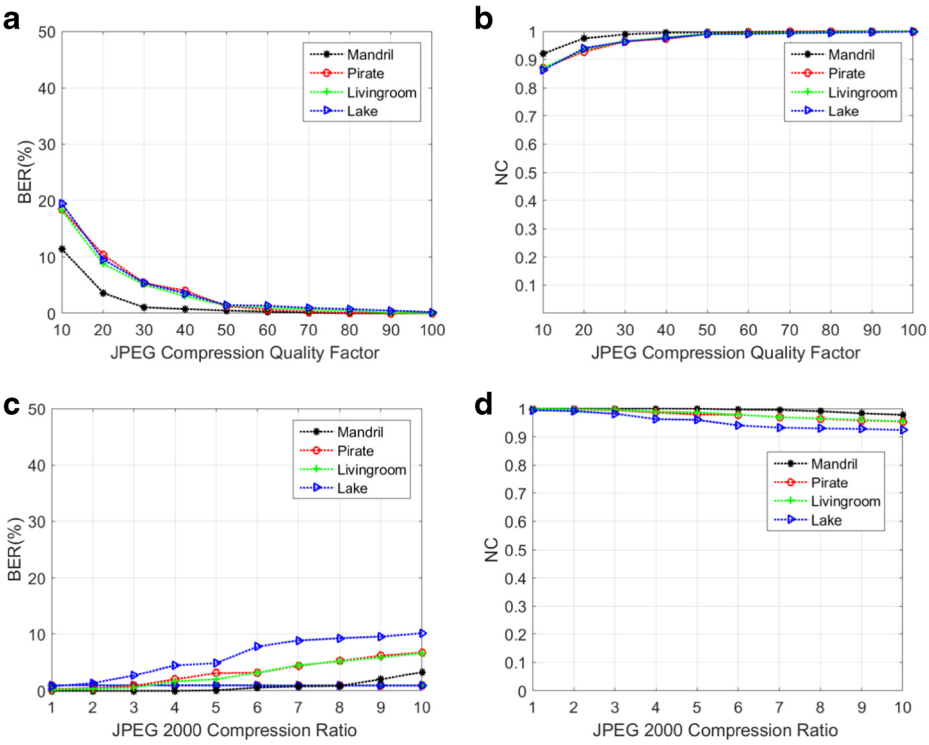


Fig. 14 Robustness against image compression attacks. (a)-(b) JPEG lossy compression. (c)-(d) JPEG2000 compression

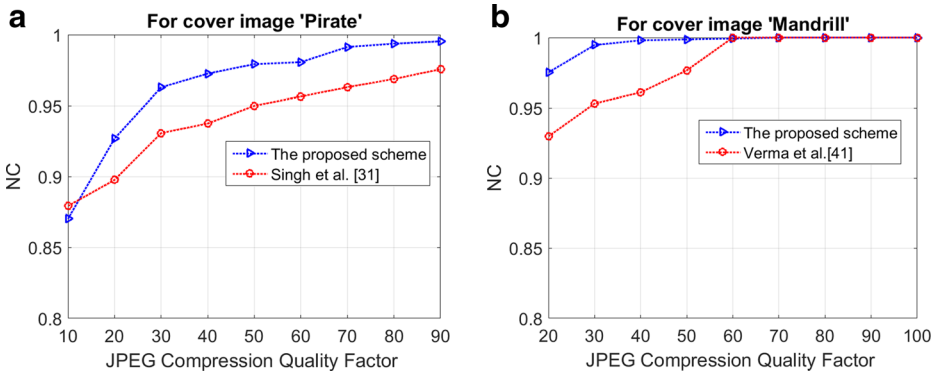
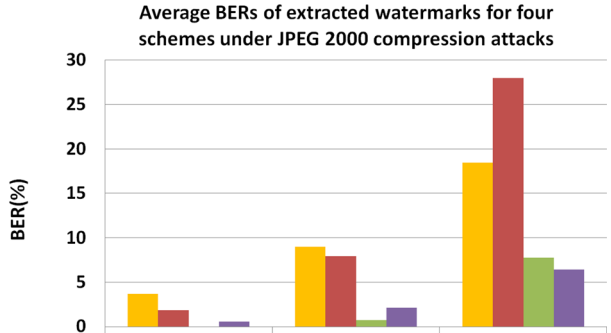


Fig. 15 Robustness comparison of the proposed scheme in term of NC values

robustness performance of the proposed watermark scheme against JPEG compression attacks is better in comparison to the two methods [31] and [41]. Fig. 16 presents the average BER values (in percentage) of extracted watermarks for eight test images under JPEG2000 compression attack, respectively obtained by the compared methods [12, 23, 37]. As shown in Fig. 16, Hu et al's scheme [12] shows a little advantage to the proposed in the case of CR=2 and 4. In addition to this, the robustness of these three methods against JPEG2000 compression is evidently inferior to the proposed scheme's. From Fig. 14-16, the proposed scheme exhibits exceptional robustness against JPEG compression and JPEG2000 compression.

The robustness of the proposed scheme has been also examined for other common signal processing attacks. The BER values obtained from the proposed scheme under various attacks for the test image 'lena' have been compared with those of Das [8] and Parah [28] as shown in Fig. 17. These attacks include salt and pepper noise addition (density = 0.01), Gaussian noise addition (mean = 0, variance = 0.001), median filtering (filter size 3x3), histogram equalization and sharpening (radius=1.5 and amount=1.5). In addition to Gaussian noise attack, where the BER of the proposed scheme is a little bit higher than Parah's [28], the BERs of the proposed scheme under other attacks are lower than other methods'. It is easy to reach the conclusion from Fig. 17 that the proposed scheme based on hybrid domain performs better than other methods for single domain [8] and [28] in resistance to common signal processing attacks.

Fig. 16 Average BER values for various schemes



	CR=2	CR=4	CR=8
Patra [23]	3.69	9.02	18.42
Su [37]	1.82	7.95	27.93
Hu [12]	0	0.71	7.74
Proposed	0.57	2.13	6.41

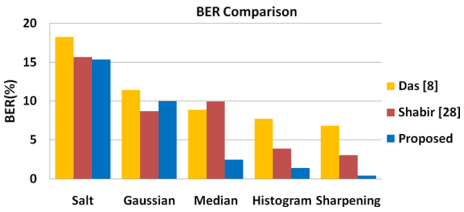


Fig. 17 BER comparison for 'Lena' image

Moreover, some common signal processing attacks are provided to verify the advantage of the proposed watermarking scheme in hybrid domain. Table 3 shows comparison results of NC values with other multi-domain approaches [34, 35, 44] for cover image 'mandrill'. As indicated in Table 3, the proposed scheme is superior to Singh AK's [34] and Zear A' [44] methods for almost all listed attacks only slightly worse than Singh AK's [34] on resisting Gaussian noise (m= 0, v=0.01). In comparison to Singh S's method [35], our method is better than it in the aspect of JPEG compression, median filtering and histogram equalization, however it has its advantages in terms of average filtering, Gaussian noise and salt & peppers noise.

From experimental and comparative results in Fig. 10-17 and Table 2-3, it is derived that the proposed scheme based on DWT-DCT-SVD hybrid domain shows better imperceptibility and robustness. The utilization of spectral characteristics of image transforms, human visual perception properties and optimal embedding strength makes the proposed scheme more imperceptible and robust as compared to the state-of-art techniques.

The main contribution of this work are: (1) the proposed watermarking scheme combines the advantages of three popular transforms DWT, DCT and SVD and provides a better compromise between the imperceptibility and robustness as compared to existing certain DWT, DCT and SVD applied individually or blend of DWT-SVD, DCT-SVD and DWT-DCT-SVD, (2) the optimal embedding strength is adaptively determined according to a compromise between the imperceptibility and robustness of watermarking technique by least squares curve fitting.

5 Conclusions

In this paper, a new robust and invisible blind watermarking scheme based on a combination of DCT and SVD in DWT domain has been proposed to improve the imperceptibility and the robustness. Low frequency subband (LL) which contains the maximum energy of an image is

Table 3 Comparison results of NC values against some signal processing attacks

Attacks	Singh S [35]	Singh AK [34]	Zear A [44]	Proposed
JPEG Compression (QF=50)	0.9935	0.9785	-	0.9980
JPEG Compression (QF=30)	0.9920	-	0.9803	0.9947
Average filtering [3 3]	0.9951	-	0.9869	0.9880
Median filtering (3 3)	0.9939	0.9752	-	0.9953
Gaussian noise (m= 0, v=0.001)	-	0.9754	0.9466	0.9893
Gaussian noise (m= 0, v=0.01)	0.9828	0.9365	-	0.9227
Gaussian noise (m= 0, v=0.5)	0.8481	0.6565	0.6576	0.6627
Gaussian filtering(sigma=1.0)	-	0.9913	0.9883	0.9954
Salt & Pepper noise(d=0.01)	0.9867	-	0.7747	0.9609
Histogram equalization	0.9943	0.9208	0.9404	0.9953

selected to embed the watermark signal and improve the robustness against image processing operations in DWT domain. In DCT domain, specific middle frequency coefficients are chosen to achieve the appropriate perception for human vision. Embedding the watermark is executed by modifying singular values of cover image into discrepant paired groups in SVD domain. The optimal embedding strength is estimated using least-square curve fitting in a preliminary experiment and provides a good balance between the imperceptibility and robustness. Logistic chaotic map is employed to increase the security of the watermarking scheme.

The main aim of this work is to develop an effective watermarking scheme for protecting digital images against various signal processing attacks with high image quality. By comparing with some existing important methods, experimental results demonstrate better visual imperceptibility and robustness of the proposed scheme against variety of attacks, especially JPEG/JPEG2000 compression, average filtering, histogram equalization, median filtering and Gaussian filtering, etc. Future direction that need to be scheduled in the area of image watermarking is to seek a new algorithm which is invariant to geometrical attacks such as rotation and translation.

Acknowledgments This work was supported by the Scientific Research Program Funded by Shaanxi Provincial Education Department (Program No.15JK1504), the National Natural Science Foundation of China (Grant No. 61671376 & 61671374) and the Natural Science Basic Research Plan in Shaanxi Province of China (Program No.2016JM6045).

References

1. Agoyi M, Çelebi E, Anbarjafari G (2014) A watermarking algorithm based on chirp z-transform, discrete wavelet transform, and singular value decomposition. SIViP. doi:10.1007/s11760-014-0624-9
2. Ahmed N, Natarajan T, Rao KR (1974) Discrete cosine transform. IEEE Transactions on Computers C-23: 90–93
3. Ali M, Ahna CW, Pant M (2014) A robust image watermarking technique using SVD and differential evolution in DCT domain. Optik 125:428–434
4. Ali M, Chang WA, Pant M, Siarry P (2015) An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. Information Sciences 301:44–60
5. Ansari IA, Pant M, Chang WA (2016) PSO optimized and secured watermarking scheme based on DWT and SVD. Proceedings of fifth international conference on soft computing for problem solving, Advances in Intelligent Systems and Computing 437:411–424
6. Benoraira A, Benmahammed K, Boucenna N (2015) Blind image watermarking technique based on differential embedding in DWT and DCT domains. EURASIP Journal on Advances in Signal Processing 2015(1):55
7. Chung KL, Yang WN, Huang YH et al (2007) On SVD-based watermarking algorithm. Applied Mathematics and Computation 188:54–57
8. Das C, Panigrahi S, Sharma VK, Mahapatra KK (2014) A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. Int J Electron Commun 68:244–253
9. Elayan MA, Ahmad MO (2016) Digital watermarking scheme based on Arnold and anti-Arnold transforms. Image and Signal Processing. ICISP 2016. Lecture Notes in Computer Science 9680:317–327. doi:10.1007/978-3-319-33618-3_32
10. Fan MQ, Wang HX, Li SK (2008) Restudy on SVD-based watermarking scheme. Applied Mathematics and Computation 203(2):926–930
11. Hsu CT, Wu JL (1999) Hidden digital watermarks in images. IEEE Trans. Image Process 8(1):58–68
12. Hu HT, Hsu LY (2015) Exploring DWT-SVD-DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. Computers and Electrical Engineering 41:52–63
13. Hu HT, Hsu LY (2017) Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics. Multimed Tools Appl. 76(5):6575–6594. doi:10.1007/s11042-016-3332-3

14. Huang HC, Chu CM, Pan JS (2009) Genetic watermarking for copyright protection. Information Hiding and Applications, the series Studies in Computational Intelligence 227:1–19
15. Kumar A, Agarwal P (2016) Choudhary A (2016) A digital image watermarking technique using cascading of DCT and biorthogonal wavelet transform. Proceedings of International Conference on Recent Cognizance in Wireless Communication & Image Processing:21–29
16. Lai CC (2011) An improved SVD-based watermarking scheme using human visual characteristics. Optics Communications 284:938–944
17. Lin SD, Shie S-C, Guo JY (2010) Improving the robustness of DCT-based image watermarking against JPEG compression. Comput Standards Interfaces 32(1-2):54–60
18. Ling HC, Phan CW, Heng SH (2012) On the security of a hybrid SVD-DCT watermarking method based on LPSNR. Advances in Image and Video Technology Lecture Notes in Computer Science 7087:257–266
19. Madhuri AJ, Mehul SR, Yogesh HD, Kalyani RJ, Shilpa PM (2015) Image and video compression fundamentals, techniques, and applications. CRC Press Taylor & Francis Group, Boca Raton
20. Makbol NM, Khoo BE, Rassem TH (2016) Block-based discrete wavelet transform singular value decomposition image watermarking scheme using human visual system characteristics. IET Image Process 10(1):34–52
21. Mishra A, Agarwal C, Sharma A, Bedi P (2014) Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. Expert Systems with Applications 41:7858–7867
22. Parah SA, Sheikh JA, Akhoon JA et al (2016) Information hiding in edges: A high capacity information hiding technique using hybrid edge detection. Multimed Tools Appl. doi:10.1007/s11042-016-4253-x
23. Patra JC, Phua JE, Bornand C (2010) A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. Digital Signal Process 20:1597–1611
24. Qin C, Chang CC, Hsu TJ (2015) Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimed Tools Appl 74(15):5861. doi:10.1007/s11042-014-1894-5
25. Rabie T (2016) Color-secure digital image compression. Multimed Tools Appl. doi:10.1007/s11042-016-3942-9
26. Rabie T, Kamel I (2017) Toward optimal embedding capacity for transform domain steganography: a quad-tree adaptive-region approach. Multimed Tools Appl 76(6):8627–8650. doi:10.1007/s11042-016-3501-4
27. Roy S, Pal AK (2016) A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling. Multimed Tools Appl. doi:10.1007/s11042-016-3902-4
28. Shabir AP, Javaid AS, Nazir AL, Ghulam MB (2016) Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. Digital Signal Process 53:11–24
29. Shieh CS, Huang HC, Wang FH, Pan JS (2004) Genetic watermarking based on transform domain techniques. Pattern Recognit. 37(3):555–565
30. Singh AM (2017) Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimed Tools Appl. 76(6):8881–8900. doi:10.1007/s11042-016-3514-z
31. Singh D, Singh SK (2016) DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimed Tools Appl. doi:10.1007/s11042-016-3706-6
32. Singh AK, Dave M, Mohan A (2013) A hybrid algorithm for image watermarking against signal processing attacks. Multi-disciplinary Trends in Artificial Intelligence (MIWAI). Lecture Notes in Computer Science (LNCS) 8271:235–246
33. Singh AK, Dave M, Mohan A (2014) Hybrid technique for robust and imperceptible image watermarking in DWT-DCT-SVD domain. National Academy Science Letters 37(4):351–358
34. Singh AK, Dave M, Mohan A (2016) Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl. 75(14):8381–8401
35. Singh S, Rathore VS, Singh R (2017) Hybrid NSCT domain multiple watermarking for medical images. Multimed Tools Appl 76(3):3557–3575. doi:10.1007/s11042-016-3885-1
36. Srdjan S, Irena O and Ervin S (2016) Multimedia Signals and Systems: Basic and Advanced Algorithms for Signal Processing (Second Edition). Springer International Publishing, Switzerland
37. 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 67:652–664
38. Su Q, Niu Y, Wang G, Jia S, Yue J (2014) Color image blind watermarking scheme based on QR decomposition. Signal Process 94:219–235
39. Tao P, Eskicioglu AM (2006) An adaptive method for image recovery in the DFT domain. J Multimed 1(6):36–45
40. Tsui TK, Zhang XP, Androutsos D (2008) Color image watermarking using multidimensional fourier transforms. IEEE Trans Inform Forensics Security 3(1):16–28
41. Verma VS, Jha RK, Ojha A (2015) Digital watermark extraction using support vector machine with principal component analysis based feature reduction. J Vis Commun Image R 31:75–85
42. Wang Y, Doherty JF, Van Dyck RE (2002) A wavelet-based watermarking algorithm for ownership verification of digital images. IEEE Trans Imag Process 11(2):77–88

43. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: From error visibility to structural similarity. IEEE Transactions on Image Processing 13(4):600–612
44. Zear A, Singh AK, Kumar P (2016) A proposed secure multiple watermarking technique based on DWT. DCT and SVD for application in medicine. Multimed Tools Appl. doi:10.1007/s11042-016-3862-8
45. Zhang L, Zhang L, Mou X, Zhang D (2011) FSIM: A Feature Similarity Index for Image Quality Assessment, IEEE Trans. Image Processing 20(8):2378–2386
46. Zheng PP, Feng J, Li Z, Zhou MQ (2014) A novel SVD and L S-SVM combination algorithm for blind watermarking. Neurocomputing 142:520–528

Xiao-bing Kang is currently working as an associate professor in the Department of Information Science, Faculty of Printing, Packaging Engineering and Digital Media Technology, Xi'an University of Technology, Xi'an, China. He received his B.E. Degree in University of Science and Technology Beijing, China, his M.E. and Ph.D. degrees in Northwestern Polytechnical University, Xi'an, China, respectively. He is a member of the IEEE, the ACM and the CCF. His main research interests include Signal and Image Processing, Multimedia Forensics and Security, Machine Learning.

Fan Zhao received a Ph.D. in Information and Communication Engineering from Xi'an Jiaotong University, Xi'an, China, in 2009. She worked as a postdoctoral fellow in the Department of Computer Science and Engineering, Xi'an Jiaotong University from July 2010 to April 2012. She is now an associate professor in the Department of Information Science at Xi'an University of Technology, Xi'an, China, Her research interests include image processing, object tracking, and pattern recognition. (E-mail: vcu@xaut.edu.cn).

Guang-feng Lin received the B.E. degree in mechatronic engineering from Xi'an Institute of Technology in 2001, the M.E. degree in traffic information engineering and control from Chang'an University in 2005 and the Ph.D. in control theory and control engineering from Xi'an University of Technology in 2013. From September 2014 to September 2015, he have completed postdoctoral research about heterogenous structure fusion for classification in Visual Computing and Image Processing Lab (VCIPL) at Oklahoma State University. He is currently a lectorate of Department of Information Science at the Xi'an University of Technology. His research interests focus on digital image processing and pattern recognition. He is CCF professional member, ACM member and IEEE CS member.

Ya-jun Chen was born in 1980. He is currently an associate professor of the Department of Information Science, Xi'an University of Technology, China. He received his B.S. degree in mechanical engineering, M.S. degree in signal and information processing and PhD degree in control theory and control engineering, all from Xi'an University of Technology, Xi'an, China, in 2002, 2006 and 2015, respectively. He is a member of the CCF. His research interests cover digital image processing and machine vision, and intelligent information processing.