An entropy-based image watermarking scheme by improving robustness in shearlet and wavelet domain

Yujian Zhuang
Hainan University
Xiaoyi Zhou (xy.zhou.xy@gmail.com)
Hainan University https://orcid.org/0000-0003-3777-9479
Sheng Liu
Hainan University

Research

Keywords:

Posted Date: August 24th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-63616/v1

An entropy-based image watermarking scheme by improving robustness in shearlet and wavelet domain

Yujian Zhuang[1], Xiaoyi Zhou [1,*], Sheng Liu[1]

1 School of Computer and Cyberspace Security, Hainan University, China; zyujian@hainanu.edu.cn, shengliu681@gmail.com;

* Correspondence: xy.zhou.xy@gmail.com;

Abstract

The existing robust digital watermarking schemes mainly embed information in the fixed positions or with fixed embedding strength, while seldom considering adaptive adjustment based on the characteristics of the cover image, thus it reduces the imperceptibility and the robustness of watermarking. Aiming at these issues, we propose a scheme which can be able to dynamically adjust the watermark embedding position and strength. Furthermore, it guarantees the trade-off between robustness and imperceptibility. The appropriate embedding positions are dynamically selected for the watermark by comparing the image entropy, and the embedding strength of the image blocks are adaptively adjusted according to the entropy and the JND model in the HVS-based wavelet domain. SVD is performed on the image blocks to ensure the resistant ability of geometric attacks. The experimental results show that the scheme has good imperceptibility as well as strong robustness against various attacks. The robustness in common attacks is improved by at least 1% compared with similar watermarking schemes.

Keywords: Robust Watermarking; Entropy; Just Noticeable Difference; Fast Finite Shearlet Transform; Discrete Wavelet Transform

1. Introduction

Digital watermarking is an information hiding technology, it commonly used for copyright protection, ownership identification and authentication applications. From the anti-attack ability, the watermark technology can be classified into three categories: fragile, semi-fragile and robust. Among them, robust watermarking enables the watermarked image not only resistant to non-malicious attacks, but also malicious attacks within a certain range of distortions, even general image processing hardly affects the detection of the watermarks [1].

Imperceptibility and robustness are the two main characteristics of robust digital watermarking[2]. Imperceptibility refers to the visibility and quality of the watermarked image, while robustness is the ability of a watermark being effectively extracted and detected from a watermarked image under various attacks. Most watermarking schemes are difficult to achieve both features for they are mutually exclusive [3]. Therefore, robust watermarking researches generally focus on achieving a good balance between imperceptibility and robustness. The watermark can be embedded in spatial and transform domain of cover image. The former technology hides a large amount of data into the cover image, but its robustness is worse than the schemes based on transform domain [4]. The latter one embeds a watermark via converting cover image into a transform domain and then change its coefficients and shows good robustness under geometric attacks such as rotation, scaling, and panning [5]. Discrete Fourier transform (DFT), discrete wavelet transform (DWT) and discrete cosine transform (DCT) are commonly used in a watermark technology.

In recent years, some researchers consider to combine the plural transform methods for obtaining the advantage of each transform domain to improve the performance. Araghi et al. [6] utilized the advantage of the wavelet domain and SVD and proposed a hybrid robust digital watermarking scheme. Wavelet domain better reflects the HVS, and SVD has strong anti-geometric attack ability. Thanki et al. [7] proposed a digital watermarking scheme with redundant discrete wavelet transform (RDWT) and discrete curvelet transform (DCuT). In their scheme, after carrying out the DCuT of the original cover image, vertical wavelet coefficients are modified by two pseudo-random noise (PN) sequences according to scrambled watermark. Singh et al. [8] proposed a scheme based on DCT-SVD. The nonlinear chaotic map is used to randomly select the embedding position of the watermark in the DCT domain, it enhances the security of the watermark scheme and solves the false alarm detection problem by using a verification operation. Vali et al. [9] proposed an algorithm named self-adaptive differential evolution (SADE) based on RDWT and SVD to optimize the embedding strength. The scheme embeds a gray-scale watermark image into the singular values of RDWT subbands after multiplying by a scaling factor. Although the above watermarking schemes combine the advantages of multiple transformation, they embed a watermark with fixed embedding strength or in fixed position, and it is hard to achieve the trade-off between the robustness and imperceptibility.

How to dynamically select the suitable embedding position and strength is one of the challenges to optimize the watermarking scheme. To solve this issue, information entropy, which is commonly used to describe the randomness of image data, is introduced in this research. The higher entropy of an image, the higher the pixel complexity. In other words, selecting the region with higher information entropy as the embedding

position can effectively improve the imperceptibility of the scheme. [10] applies the quantization method to control the embedding strength of watermark, selects some image blocks with high information entropy as the embedding positions, and utilizes just noticeable difference (JND) model to calculate the maximum embedding strength of each singular value matrix coefficient, thus it solves the trade-off between the imperceptibility and robustness. Experiments show that the scheme has good robustness owing to JND model. JND is the minimum perceptual threshold of the human eye when the image changes. Since the transform domain-based JND model has the advantages of low computational complexity and adaptability to HVS, it can achieve better robustness and imperceptibility than using a fixed embedding strength scheme, thus it is a suitable tool for controlling the embedding strength. Tikariha et al. [11] proposed a DWT-DCT-SVD robust digital watermarking scheme based on effective JND model. They combine many transformation domains and the JND model to improve the robustness of the overall watermarking scheme. Similarly, Hu et al. [12] proposed a robust blind digital watermarking scheme based on DCT-PSAMM. By combining the JND model and the LQI in the cosine domain, the watermarked image still cannot be observed obvious distortion even at a high embedding strength.

In the above digital watermarking schemes, the methods based on wavelet domain have achieved good performances. However, the two-dimensional discrete wavelet is composed of wavelet tensor accumulation, its basis function only has three directions of horizontal, vertical and diagonal, thus it cannot represent the edge information of image optimally. Therefore, some researchers put forward the multi-scale geometric analysis methods to develop an "optimal" representation method for high-dimensional data. The multi-scale geometric analysis methods applied in digital watermarking include ridgelet transform[13,14], contourlet transform[15-17], bandelet transform[18], shearlet transform[19-23] and so on. Among them, discrete shearlet transform (DST) [24] is a new multi-scale geometric transformation proposed in 2008. It overcomes the imperfections of limited direction selection of wavelet transform and anisotropy of base function, and has good directionality and multi-resolution representation for images. DST is widely used in image processing, and the research of digital image watermarking based on DST is gradually increasing in recent years [21-23]. However, most of the existing DST-based schemes have high computational complexity, which is not conducive to real-time embedding of the watermarks. Fast finite shearlet transform (FFST) [25] is a simple version of DST which translates the shearlets over the full grid at each scale and for each direction. And the use of fast Fourier transform speeds up the implementation of the algorithm, which makes it more suitable for the application of watermarking schemes. In consequence, we selected FFST to optimize the time complexity compared with traditional shearlet transforms.

In this paper, a robust hybrid watermarking scheme based on shearlet domain and wavelet domain is proposed. **Table 1** shows the comparison between the proposed scheme and some state-of-the-art methods. The proposed scheme utilizes a multi-scale analysis method to analyze the cover image and get the optimal representation, improving the ability of watermark to resist general attacks and geometric attacks by using the existing DWT-SVD watermarking schemes. Information entropy is adopted in embedding position selection and improves the imperceptibility. Compared with the similar algorithms, it is not limited to select a part of the high entropy region as the embedding position. Instead, the whole region can be used to embed watermarks through quantitative comparison of the embeddable regions, so as to increase the capacity of watermarks. In terms of embedding strength, the HVS-based JND model is used to select the best embedding strength. The trade-off between robustness and imperceptibility is achieved by adjusting the information entropy. Experimental results show that the identifiable watermark can still be extracted after the watermarked image being not seriously distorted.

The rest of the paper is organized as follows. In Section 2, the preliminaries briefly describe the discrete shearlet transform, JND model and image encryption with ergodic matrix,. Section 3 describes the proposed watermarking scheme in detail. And the experimental results are presented in Section 4. Finally, Section 5 contains the conclusion of the paper.

Table 1 Comparison of state-of-the-art methods with the proposed scheme.

Scheme	Proposed	[6]	[26]	[9]	[8]	[27]	[28]	[29]	[10]	[30]	[20]	[31]	[32]
MGA	Yes	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
Security	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No
Fixed embedding location	No	Yes	Yes	Yes	No	No	Yes	No	No	Yes	No	Yes	Yes
Fixed embedding strength	No	Yes	Yes	No	Yes	Yes	Yes	No	No	No	No	Yes	Yes

2. Preliminaries

2.1 Discrete shearlet transform:

In Multi-scale Geometric Analysis (MGA), the high-dimensional function is represented by the set of functions in the low-dimensional function space, and the optimal or "thinnest" function representation method is obtained. With more and more research and application, its ability to optimize the representation of images makes it important in the field of digital image processing. Discrete shearlet transform is a novel image

analysis of MGA with the ability to perform multi-scale and multi-directional analysis of data [32].

The image decomposition based on shearlet transform is mainly divided into two steps: ①decompose the cover image by Laplacian pyramid to obtain the high-pass and low-pass sub-bands of the image. ②perform a suitable transform on the sub-bands to obtain the multi-scale and multi-directional representations, as shown in **Fig. 1**. Here, the details of the DST is described briefly as follows.

For a function f, the shearlet transform can be mapped according to formula (1), which requires several parameters: the scale $a > 0$, the direction s∈R, the location $t \in \mathbb{R}^2$

$$f \to \mathrm{SH}_\psi f(a,s,t) = \langle f, \psi_{a,s,t} \rangle \tag{1}$$

Let $a = 2^{-j}$, $s = -l$, Each generation function $\psi \in L^2(R^2)$ of the discrete shearlet transform can be defined as formula (2):

$$\psi_{j,l,k} = |det\ A|^{\frac{j}{2}} \psi\left(B_0{}^l A_0{}^j - k\right);\ j,l \in \mathbb{Z}, k \in \mathbb{Z}^2 \tag{2}$$

Where A and B are 2 × 2 invertible matrices, representing anisotropic expansion and shear.

The criteria for discrete shearlet transformation are as shown in formula (3):

$$A_0 = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix},\ B_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{3}$$

Then apply the discrete Fourier transform, of which the target image $f \in L^2(R^2)$ of the N × N size can be defined as:

$$\langle f, \psi_{j,l,k}^{(d)} \rangle = 2^{\frac{3j}{2}} \int_{\Re^2} \hat{f}(\xi) \overline{V(2^{-2j}\xi) W_{j,l}^{(d)}(\xi)} e^{2\pi i \xi A_d^{-j} B_d^{-l} k}\, d\xi, d \in \{0,1\};\ \xi \in \Re^2 \tag{4}$$

Where $\widehat{f}(\xi)$ is a function evaluation of 2D-DFT. $V(\xi)$ is a pseudo-polar coordinate, and $W_{j,l}^{(d)}(\xi)$ is a window function located on a pair of trapezoids.

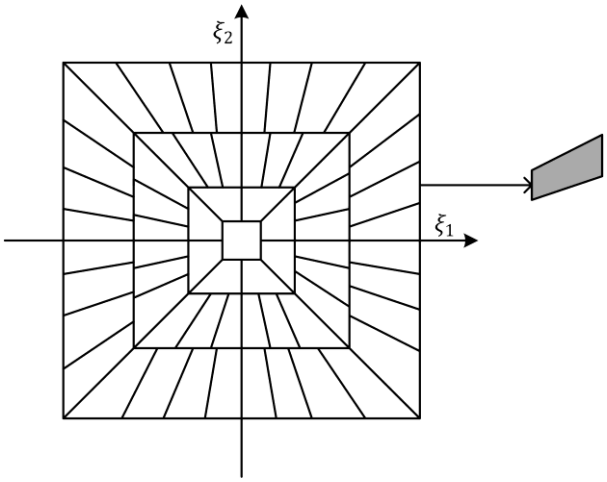


Fig. 1 The tiling of frequency plane and frequency support of a shearlet.

2.2 Just noticeable threshold model on wavelet domain

Barni et al. [33] proposed a noticeable threshold model in the wavelet domain, which has been considered as a suitable tool for controlling the embedding strength of watermark in each DWT coefficient of a cover image and a solution to balance the robustness and imperceptibility of the watermarking scheme. The model using three major characteristics of human visual system: Frequency masking $F_{s,l}$, Brightness masking $\tilde{L}_l(i,j)$ and Texture masking $T_l(i,j)$. The entire JND model is calculated according equation (5):

$$JND(i,j) = F_{s,l} \times \tilde{L}_l(i,j) \times T_l(i,j)^{0.02} \tag{5}$$

Among them, l, s are respectively the decomposition scale and direction of the discrete wavelet transform. Three characteristics based on the human visual system are mathematically defined as equation (6-9):

$$F_{s,l} = \begin{cases} \sqrt{2}, & if\ s = LL \\ 1, & otherwise \end{cases} \times \begin{cases} 1.00, & if\ l = 0 \\ 0.32, & if\ l = 1 \\ 0.16, & if\ l = 2 \\ 0.10, & if\ l = 3 \end{cases} \tag{6}$$

$$\tilde{L}_l(i,j) = 1 + \begin{cases} 1 - L_l(i,j), & if\ L_l(i,j) < 0.5 \\ L_l(i,j), & otherwise \end{cases} \tag{7}$$

$$L_l(i,j) = \frac{1}{256} I_3^{LL}\left(1 + \left\lfloor \frac{i}{2^{3-l}} \right\rfloor, 1 + \left\lfloor \frac{j}{2^{3-l}} \right\rfloor\right) \tag{8}$$

$$T_l(i,j) = \sum_{k=0}^{3-l} \frac{1}{16^{-k}} \sum_{s}^{LL,LH,HL,HH} \sum_{a=0}^{1}\sum_{b=0}^{1} \left(I_{k+l}^{s}\left(a + \frac{i}{2^k}, b + \frac{j}{2^k}\right)\right)^2 \cdot var(I_3^{LL}(x + a + \frac{i}{2^{3-l}}, y + b + \frac{j}{2^{3-l}}))_{\substack{x=0,1 \\ y=0,1}} \tag{9}$$

It can be seen from the above equations that the JND model of the wavelet domain is proposed by pixel-based masking. These characteristics are calculated in relatively small 2 × 2 neighborhood pixels, representing small local features of the image, and it ignores the effect of global features of the image on HVS. Block-based image processing is a common method that can be used to weigh the effects of global and local characteristics of target images on HVS. Therefore, a block-based digital image watermarking scheme is proposed in this research. The cover image and the watermark image are decomposed into non-overlapping image blocks before the embedding process. Then the entropy of each image block is calculated to represent the global features of the image block, and finally the imperceptibility of the watermarking scheme is improved by combining with JND.

2.3 Image Encryption with Ergodic Matrix

For ensuring the security of the digital watermarking scheme, an image encryption with ergodic matrix is applied before the watermark embedding process.

Ergodic matrix was introduced by Zhao et al. [34,35]. The basic idea can be briefly described as below:

Let $\mathbb{F}_{n\times n}^{q}$ be a set of all n×n matrices over the finite field $\mathbb{F}^q$, ($\mathbb{F}_{n\times n}^{q}$, +, ×) form a 1-ring, here + and × are addition and multiplication over $\mathbb{F}^q$, respectively. We randomly generate two nonsingular matrices Q_1, $Q_2 \in \mathbb{F}_{n\times n}^{q}$, then:

($\mathbb{F}_{n\times n}^{q}$, ×) is a monoid, its identity element is $I_{n\times n}$.

($\langle Q_1\rangle$, ×) and ($\langle Q_2\rangle$, ×) are Abelian groups, their identity elements are also $I_{n\times n}$. Here Q_1, Q_2 are nonsingular and Q_1, $Q_2 \in \mathbb{F}_{n\times n}^{q}$, and for any $m_1, m_2 \in \mathbb{F}_{n\times n}^{q}$, generally $m_1 \times m_2 \neq m_2 \times m_1$. i.e. the multiplication is not commutative in $\mathbb{F}_{n\times n}^{q}$.

Ergodic matrix has the following definitions and properties [34,35]:

Definition 1: Given $Q \in \mathbb{F}_{n\times n}^{q}$ if $\forall v \in \mathbb{F}_{n\times 1}^{q} \backslash \{0\}$, $\{Qv, Q^2v, \ldots, Q^{q^n-1}v\}$ just takes

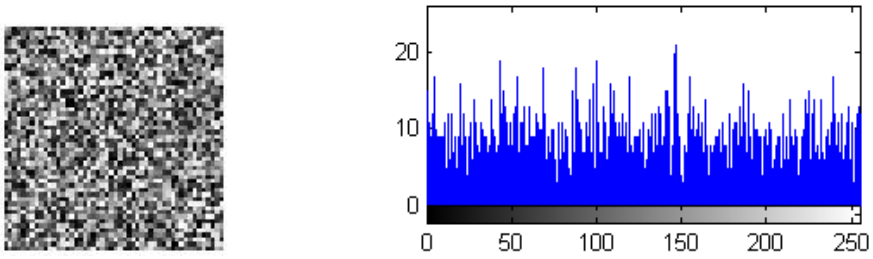
over $\mathbb{F}_{n\times 1}^{q}\backslash\{0\}$, then Q is what so-called ergodic matrix over finite field $\mathbb{F}^{q}$. (Here 0=[0 0 … 0]^{T}).

Definition 2: Given $Q\in\mathbb{F}_{n\times n}^{q}$, if $\langle Q\rangle = \{ Qx|x = 1, 2, 3,\ldots\}$, then $\langle Q\rangle$ is the generating set of Q over $\mathbb{F}_{n\times n}^{q}$.

Theorem 1: $Q\in\mathbb{F}_{n\times n}^{q}$ is an ergodic matrix if and only if the order of Q is (q^n-1) after the multiplication of Q over finite field $\mathbb{F}^{q}$.

Theorem 2: Given $Q\in\mathbb{F}_{n\times n}^{q}$ is an ergodic matrix, then for $\forall v\in\mathbb{F}_{n\times 1}^{q}\backslash\{0\}$, $\{v^{T}Q, v^{T}Q^{2}, \ldots, v^{T}Q^{q^{n}-1}\}$ just takes over $\{ v^{T}| v\in\mathbb{F}_{n\times 1}^{q}\}\backslash\{0^{T}\}$.

From the theorems above, over finite field $\mathbb{F}^{q}$, all $n \times n$ ergodic matrices have the same order and their generating sets have the same size, which are larger than that of any other $n \times n$ non-ergodic matrices. Take a random ergodic matrix $Q\in\mathbb{F}_{50\times 50}^{256}$ as an example, then the image of the matrix and the histogram is shown in **Fig. 2.**



(1) Image of a Random 50×50 Ergodic Matrix (2) Histogram of a Random Ergodic Matrix

Fig. 2 Image of a Random Ergodic Matrix and the Corresponding Histogram

This figure shows that an ergodic matrix is almost uniformly distributed and can be used to encrypt an image.

Zhou et al. [36] and Zhang et al. [37] apply ergodic matrix in the image encryption scheme and obtain a good result. It is demonstrated that an ergodic matrix with proper parameters [36,37] can be employed to completely shuffle the original image and has an immense key space of at least3.08×10^{5898}. Therefore, the same method is used in watermark preprocessing in our research. For preprocessing is not our main concern, interested readers can refer to [36,37] .

3. The proposed scheme

In order to provide effective protection for digital images, a hybrid robust digital watermarking scheme based on shearlet and wavelet domain is proposed. The owner of the digital image is verified during the extraction process by using a secret key. The multiple transformation on the cover image is to improve the overall effect for the scheme. The embedding position and embedding strength are adaptive and optimized in this scheme, which guarantees the trade-off between the transparency and robustness. In this section, the process of digital watermark embedding and extraction is illustrated in Sections 3.1 and 3.2, respectively. Section 3.3 uses an example to describe the proposed scheme in details.

3.1 Watermark embedding process

1. Read the cover image I of size $M \times N$ and decompose it into k sub-bands by α-FFST, as shown in equation (10).

$$[S_1, S_2, \dots, S_k] = FFST_\alpha(I) \tag{10}$$

2. Calculate the entropy of each sub-band and select the sub-band with the largest entropy value for b-DWT to get four sub-bands: LL_b, HL_b, LH_b and HH_b.

$$I_s = DWT_b(S_{k'}) \quad s = LL_b, HL_b, LH_b, HH_b \tag{11}$$

3. Combine four sub-bands into a coefficient matrix of size $\frac{M}{2^{b-1}} \times \frac{N}{2^{b-1}}$ and divide them into small pieces $I_s^{X,Y}$ of size $\frac{M}{2^{b+1}} \times \frac{N}{2^{b+1}}$. $I_s^{X,Y}$ is denoted equation (12).

$$I_s^{X,Y} = Divide(I_s) \tag{12}$$

Where X, Y represent the row and column of the image in which the sub-block is located.

4. Read the watermark image W, and the watermark image is encrypted by ergodic matrix (Section 2.3), and the encrypted watermark information W' is also decomposed into small blocks $w^{O,P}$ of size $\frac{M}{2^{b+1}} \times \frac{N}{2^{b+1}}$ by equation (13).

$$w^{O,P} = Divide(W') \tag{13}$$

5. Calculate the entropy of the sub-block $I_s^{X,Y}$ and $w^{O,P}$ separately. At the same time, in order to reduce the entropy error between sub-blocks, the entropy of each sub-block is divided by the minimum sub-block entropy. The specific embedding position of the watermark information is determined by the index after sorting the entropy values of $I_s^{X,Y}$ and $w^{O,P}$.

$$E_s^{X,Y} = IE\left(I_s^{X,Y}\right) \tag{14}$$

$$\tilde{E}_s^{X,Y} = \frac{E_s^{X,Y}}{\min\left(E_s^{X,Y}\right)} \tag{15}$$

$$[(x,y);(o,p)] = index\left(sort\left[\tilde{E}_s^{X,Y}; IE(w^{O,P})\right]\right) \tag{16}$$

6. As shown by the equation (17), $\beta_s^{x,y}$ represents the embedding strength of the x-th column of the row y corresponding to the sub-block, which is obtained by the block-based JND model and entropy:

$$\beta_s^{x,y} = \lambda \cdot \tilde{E}_s^{x,y} \cdot F_{s,b-1} \cdot mean\left(\sum_i \sum_j \tilde{L}_{s,b-1}^{x,y}(i,j)\, T_{b-1}^{x,y}(i,j)^{0.02}\right) \tag{17}$$

where λ is a scaling factor ranging from 0 to 1.

7. Decompose $I_s^{x,y}$ into three matrices by SVD: Left singular matrix $U_s^{x,y}$, singular value matrix $\Sigma_s^{x,y}$ and right singular matrix $V_s^{x,y}$. Then change the value of $\Sigma_s^{x,y}$ by the following equation (19) to embed the watermark information into the cover image:

$$SVD\left(I_s^{x,y}\right) = U_s^{x,y}, \Sigma_s^{x,y}, V_s^{x,y} \tag{18}$$

$$\bar{\Sigma}_s^{x,y}(i,j) = \Sigma_s^{x,y}(i,j) + \beta_s^{x,y} \cdot w^{o,p}(i,j) \tag{19}$$

8. The changed singular value matrix $\bar{\Sigma}_s^{x,y}$ is again decomposed by SVD into $\bar{\bar{U}}_s^{x,y}$, $\bar{\bar{\Sigma}}_s^{x,y}$ and $\bar{\bar{V}}_s^{x,y}$ by equation (20), and then used the following equation (21) to get the image block after embedding the watermark:

$$SVD\left(\bar{\Sigma}_s^{x,y}\right) = \bar{\bar{U}}_s^{x,y}, \bar{\bar{\Sigma}}_s^{x,y}, \bar{\bar{V}}_s^{x,y} \tag{20}$$

$$I'^{x,y}_s = U_s^{x,y} \cdot \bar{\bar{\Sigma}}_s^{x,y} \cdot V_s^{x,y^T} \tag{21}$$

9. In the end, b-IDWT and α-IFFST are performed on the combined coefficient matrix

in order to obtain the image I_w after the watermark is embedded. I_w is denoted as equation (22).

$$I_w = IDST\left(IFFST\left(Splice(I'^{x,y}_s)\right), S_i\right) \quad i \in [1,2,\dots,k] \quad i \neq k' \tag{22}$$

3.2 Watermark extraction process

Fig. 3 and **4** show the embedding and extraction processes of watermark information, respectively. The extraction process is the reverse process of the embedding process, the steps are as follows:

1. The watermarked image I'_w is processed with α-FFST and b-DWT, and four sub-bands are obtained as in steps 1 and 2 of the embedding process.

2. Decompose the four sub-bands into $\frac{M}{2^{b+1}} \times \frac{N}{2^{b+1}}$ small blocks $I'^{x,y}_s$, and find the corresponding embedding position of the watermark information by using the index obtained in step 5 of the embedding process.

3. Perform SVD on the watermarked image $I'^{x,y}_s$ which may have been attacked. Then put its singular value matrix $\Sigma'^{x,y}_s$ with the previous $\bar{\bar{U}}^{x,y}_s$ and $\bar{\bar{V}}^{x,y}_s$ to perform I-SVD (inverse SVD). The equation (23-24) is as follows:

$$SVD\left(I'^{x,y}_s\right) = U'^{x,y}_s, \Sigma'^{x,y}_s, V'^{x,y}_s \tag{23}$$

$$\Sigma''^{x,y}_s = \bar{\bar{U}}^{x,y}_s \cdot \Sigma'^{x,y}_s \cdot \bar{\bar{V}}^{x,y^T}_s \tag{24}$$

4. Extract encrypted watermark block information according to the following equation (25):

$$w'^{o,p} = \frac{\Sigma''^{x,y}_s - \bar{\bar{\Sigma}}^{x,y}_s}{\beta^{x,y}_s} \tag{25}$$

5. The watermark information is decrypted using the secret key to obtain the final watermark information.

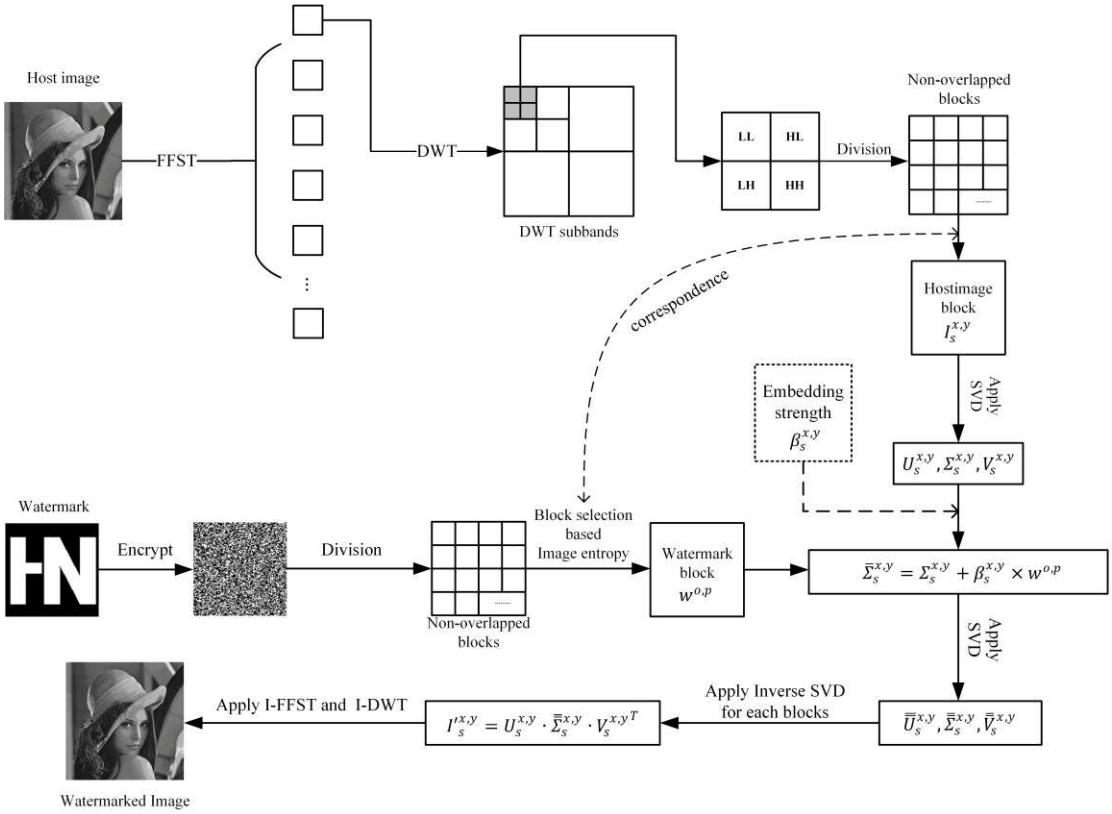


Fig. 3 The watermark embedding procedure.

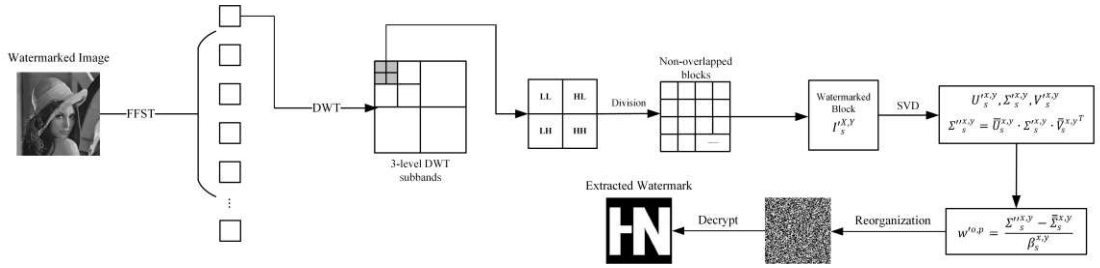


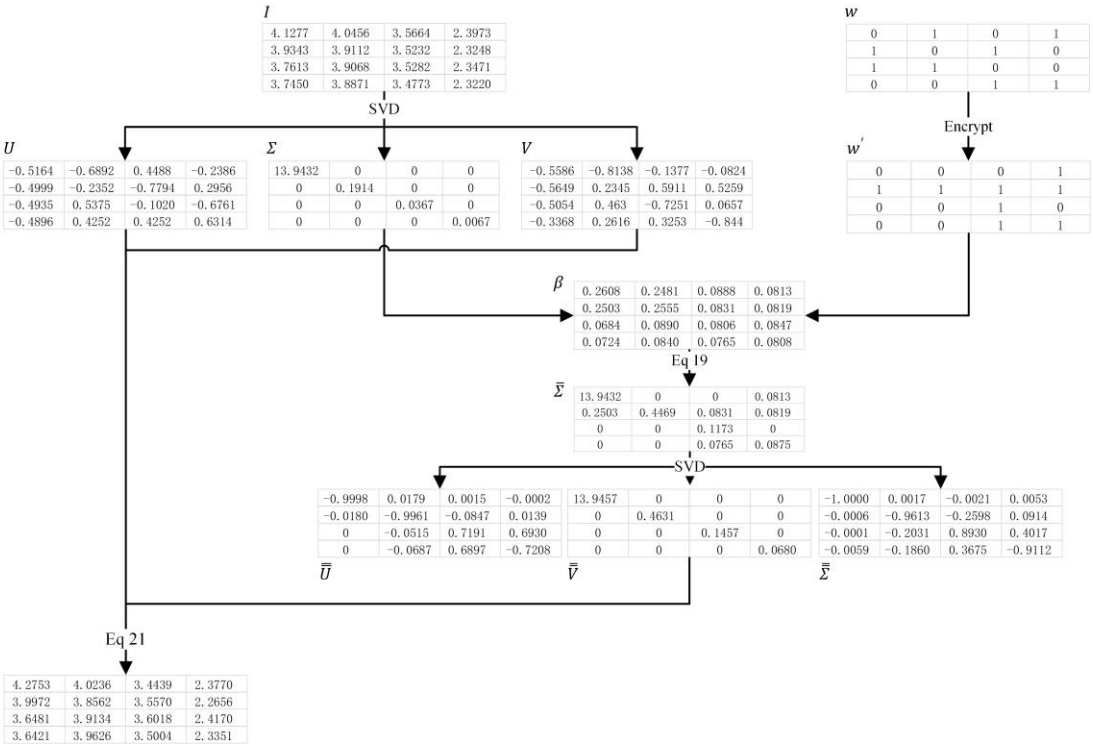
Fig. 4 The watermark extraction procedure.

3.3 Discussion and analysis

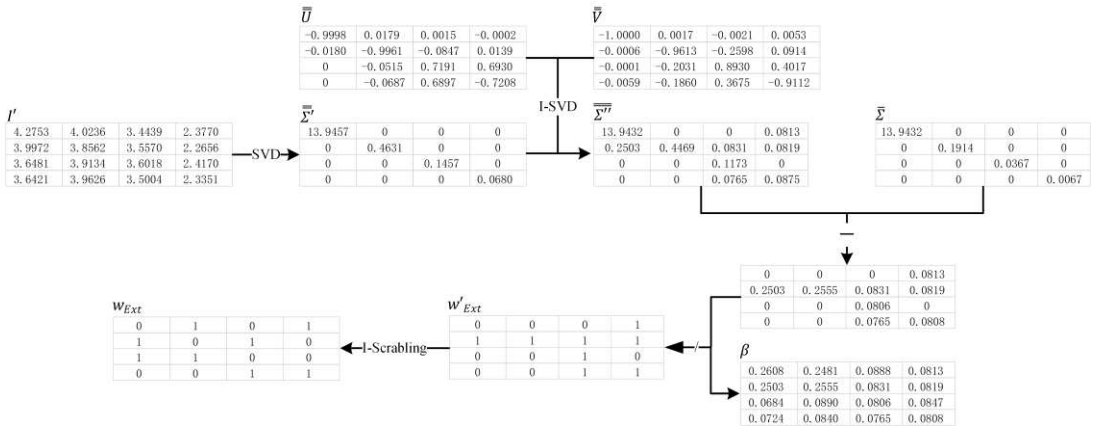
To elaborate the proposed scheme, two examples are given and they are discussed in more details. In **Example 1**, for a more convenient representation, a 4 × 4 matrix I is selected as a cover image to perform FFST-DWT. U, Σ and V are three matrices of I after SVD, where the singular value matrix Σ is used for watermark embedding. Ergodic matrix encrypts the original watermark w of size 4 × 4, and the obtained matrix w' is taken as the information to be embedded. β is an embedded intensity matrix of size 4 × 4 calculated by the formula (17). Using the equation (19), the w' is inserted into the singular value matrix Σ, and the singular value matrix $\bar{\Sigma}$ containing the watermark information is obtained. Then SVD is used to obtain the left singular matrix $\bar{\bar{U}}$,

the right singular matrix $\bar{\bar{V}}$ and the singular value matrix $\bar{\bar{\Sigma}}$. The coefficient matrix I' after embedding the watermark by I-SVD is used on $\bar{\bar{\Sigma}}$ with the previous U and V. In this example, the initial values of the coefficient matrices for positions (1, 1), (1, 2), and (1, 3) are 4.1277, 4.0456, and 3.5664, respectively. And they change to 4.2753, 4.0236 and 3.4439 after embedding the watermark. It can be seen that the impact of the watermark information on the original coefficient matrix I is minimal, and all the coefficients have changed to a certain extent, which increases the imperceptibility of the watermark and reduces the blockiness of the image after embedding the watermark.

Example 2 shows how to extract watermark information from the coefficient matrix after the watermark is embedded. For the extracting process, the secret key, the embedding position and the embedding strength of the watermark information are indispensable. Therefore, the illegal extractor often lacks the proper data information and cannot extract the information correctly $\bar{\bar{\Sigma}}'$ is a singular value matrix obtained by performing SVD on I' and multiplied by $\bar{\bar{U}}$ and $\bar{\bar{V}}^T$ obtained $\bar{\bar{\bar{\Sigma}}}''$ when the watermark is embedded. It can be seen, without the watermarked image being attacked, all the values in $\bar{\bar{\bar{\Sigma}}}''$ are equal to the value of $\bar{\bar{\Sigma}}$ and no change has taken place. $\bar{\bar{\Sigma}}$ in **Example 1** is subtracted by $\bar{\bar{\bar{\Sigma}}}''$ and divided by the embedded intensity matrix β to obtain the encrypted watermark w'_{Ext}. w_{Ext} is the watermark of the inverse of encrypted watermark, and the matrix coefficient is completely equal to the embedded watermark w. In attack simulation, w_{Ext} may be an arbitrary floating-point number. In this research, we take a floating-point number of ≥0.5 as an integer 1, and a floating-point number of <0.5 as an integer 0.



Example 1



Example 2

4. Experimental results

The scheme was tested on Matlab R2016a and a computer with i7-4710MQ and 8GB of memory. The experimental results are presented and analyzed in this section. Eight nature images are selected for discussion in this section, which are Airplane, Baboon, Boat, House, Lena, Man, Peppers and Sailboat. **Fig. 5** shows the cover images and a binary image used as a watermark image. The size of the cover image and the watermark image are 512 × 512 and 128 × 128, respectively. The watermark embedding parameters of our algorithm are α=1, b=3 and λ=0.12.

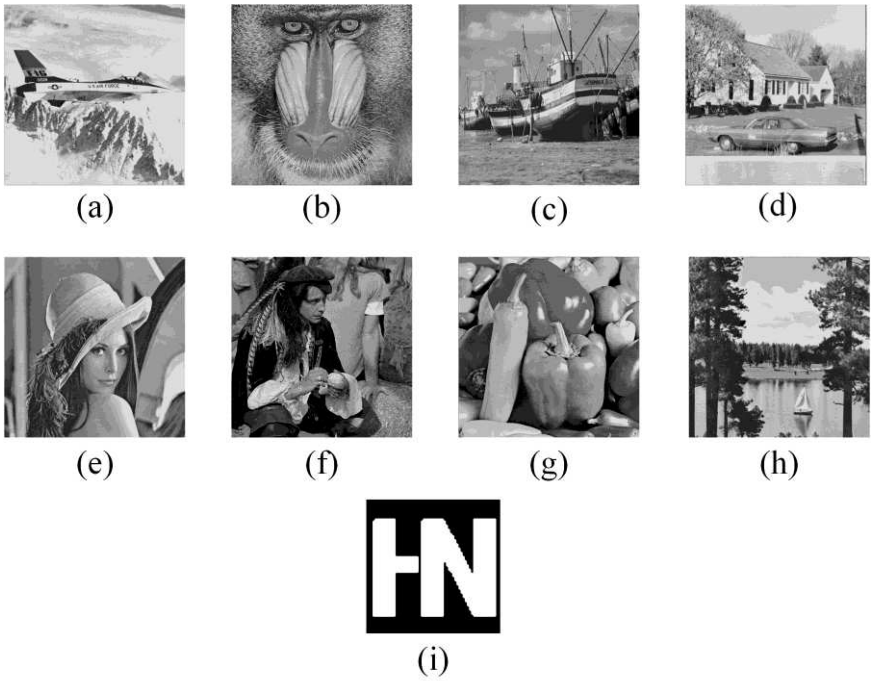


Fig. 5 Cover and watermark images (a) Airplane (b) Baboon (c) Boat (d) House (e) Lena (f) Man (g) Peppers (h) Sailboat (i) Watermark logo.

4.1 The imperceptibility test of proposed scheme

One of the most commonly used objective evaluation criterions to evaluate the image quality is peak signal to noise ratio (PSNR). The other one is SSIM, this serves as a subjective evaluation standard for images based on HVS. In this study, the imperceptibility of the watermarking scheme is discussed in combination with the above two evaluation criteria.

PSNR considers pixel-level errors and can be defined as equation (26-27):

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{26}$$

$$MSE = \frac{1}{m \times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - I'(i,j)]^2 \tag{27}$$

Where I and I' represent the original image and the image after embedding the watermark, the size is $m \times n$.

SSIM reflects people's subjective feelings relative to PSNR, and similarity evaluation is performed on three aspects of two images: brightness, contrast and structure. Its equation is as equation (28):

$$\mathrm{SSIM}(X,Y) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)} \tag{28}$$

Where μ_X and μ_Y are the mean values of the images X and Y, respectively. σ_X and σ_Y are the variances of the images X and Y, respectively. σ_{XY} represents the covariance of the images X and Y. C_1 and C_2 are defined constants.

In most cases, if the PSNR value is not less than 40 dB and the SSIM value is not lower than 0.9, it indicates that there is no obvious difference between the two images. **Fig. 6** shows that the PSNR value is larger than 45 dB and the SSIM value is not lower than 0.99. Therefore, Human beings cannot perceive changes in digital images through the naked eye. It indicates the proposed scheme satisfies the requirement of the imperceptibility. In addition, we compared the histograms of the four original cover images with the watermarked images (**Fig. 7**), the results prove that the grayscale distribution of the two images is similar. In summary, we can clearly conclude that the watermarking scheme has good imperceptibility.

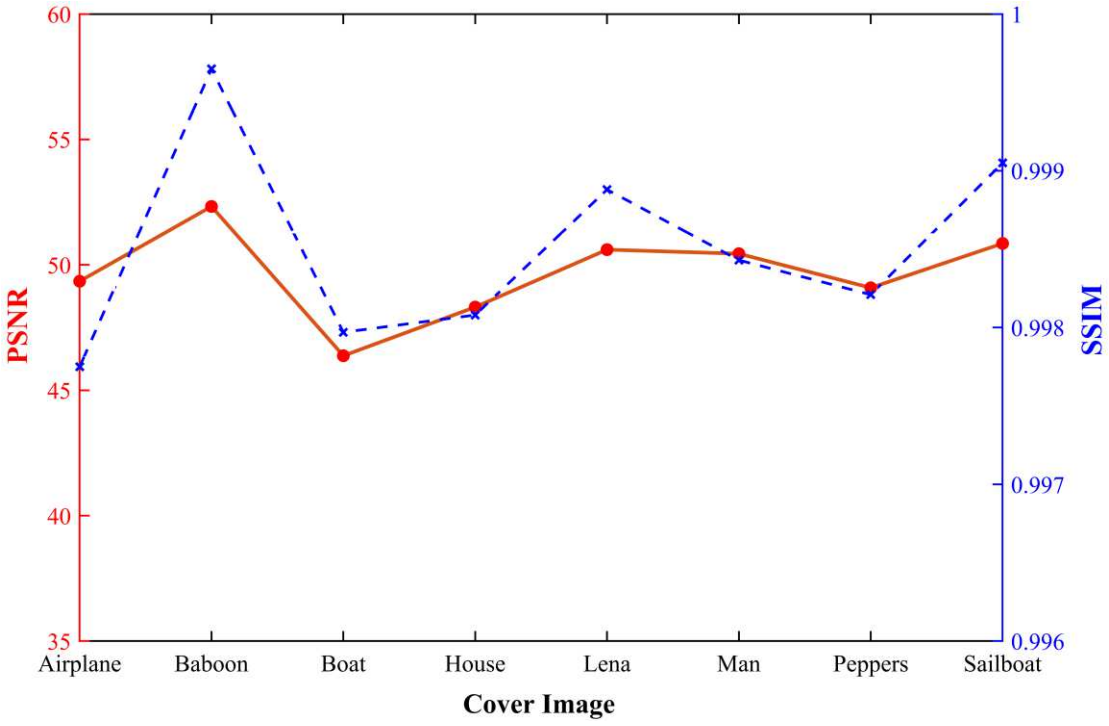


Fig. 6 The imperceptibility of proposed scheme

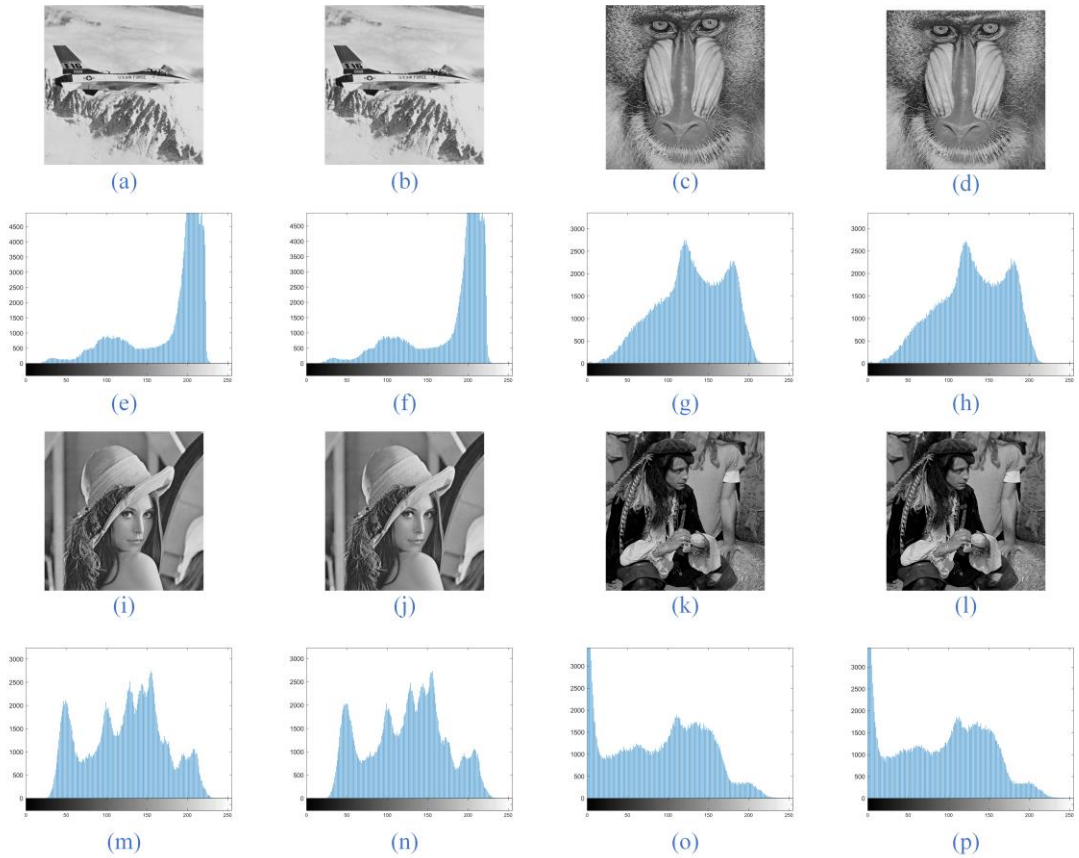


Fig. 7 Histogram comparison of original image and watermarked image: Original Image (a), (c), (i), (k); Watermarked Image (b), (d), (j), (l); Histogram Information of original image (e), (g), (m), (o); Histogram Information of watermarked image (f), (h), (n), (p).

4.2 The robustness test of proposed scheme

When the watermarked image is transmitted over the Internet, the watermark may be changed under general attacks and geometric attacks. Noise, filtering, JPEG compression, and histogram equalization are general attacks, while geometric attacks include scaling, rotation, clipping, and panning. The robustness of the scheme under various attacks is measured by the normalized correlation coefficient (NC) and the bit error rate (BER). The high NC and low BER represent the high similarity between the original watermark information and the extracted watermark information. Where NC can be calculated by equation (29):

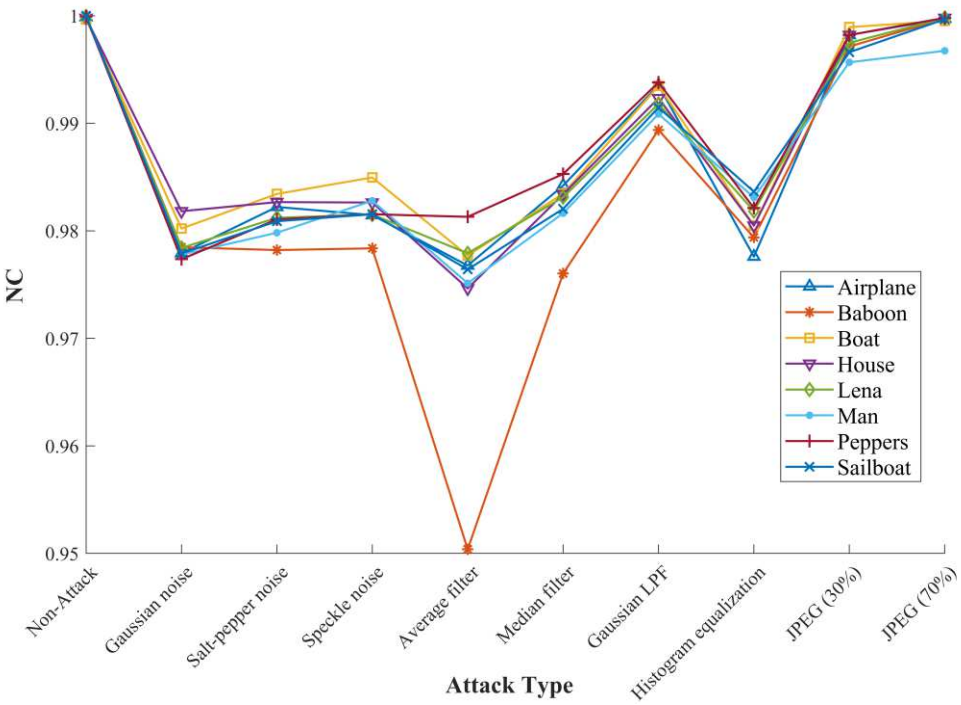
$$NC(W, W') = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} W(i,j) \times W'(i,j)}{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[W(i,j)]^2} \tag{29}$$

Where W and W' denote the original watermark information and the extracted watermark information, respectively. Both of their size is $m \times n$ .When the NC value is closer to 1, the two images are more similar. **Fig. 8** shows the NC values of eight images under general attacks and geometric attacks.

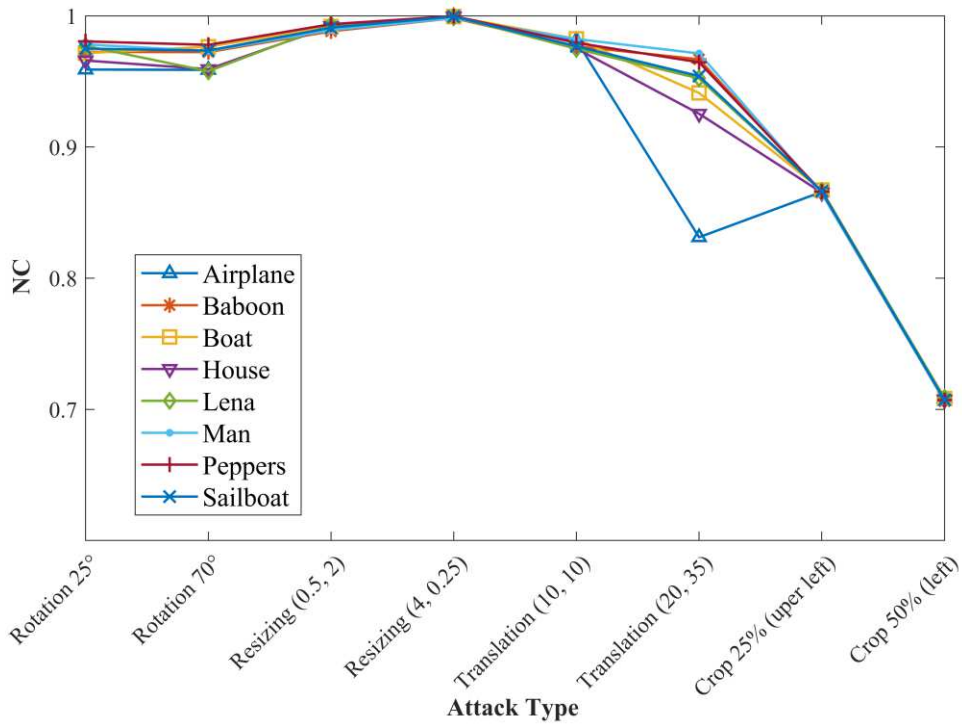
The equation for BER is as equation (30):

$$\mathrm{BER} = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} W(i,j) \otimes W'(i,j) \tag{30}$$

Where $\otimes$ represents an exclusive OR operation, W and W' represent the original watermark and the extracted watermark of size $m \times n$, respectively. When the BER value is closer to 0, the similarity between the two watermark pictures is higher. **Table 2** shows the watermarked image of Lena after 25 attacks and the extracted watermark, as well as its BER and NC values.



(a)



(b)

Fig. 8 The robustness of proposed scheme (a) General attack (b) Geometric attack

Table 2. Attacked image and extracted watermark.

Attack Type	**Gaussian noise (σ= 5%)**	**Salt-pepper noise (den = 5%)**	**Speckle noise (5%)**	**Average filter (5×5)**	**Median filter (5×5)**
Attacked Image					
Extracted Watermark					
NC	**0.9795**	**0.9833**	**0.9832**	**0.9779**	**0.9837**
BER	**0.0180**	**0.0133**	**0.0165**	**0.0201**	**0.0145**
Attack Type	**Gaussian filter (5×5)**	**Rotation (25°)**	**Rotation (70°)**	**Resizing (0.5,2)**	**Resizing (4,0.25)**

Attacked Image					
Extracted Watermark					
NC	**0.9933**	**0.9771**	**0.9577**	**0.9932**	**0.9993**
BER	**0.0061**	**0.0212**	**0.0386**	**0.0062**	**0.0006**
Attack Type	**Translation (10,10)**	**Translation (20,35)**	**Histogram equalization**	**Image darken**	**Crop (25%)**
Attacked Image					
Extracted Watermark					
NC	**0.9748**	**0.9522**	**0.9818**	**0.9859**	**0.8653**
BER	**0.0232**	**0.0435**	**0.0172**	**0.0129**	**0.1146**
Attack Type	**Lossy JPEG (QF = 90%)**	**Lossy JPEG (QF = 70%)**	**Lossy JPEG (QF = 50%)**	**Lossy JPEG (QF = 30%)**	**Lossy JPEG (QF = 10%)**
Attacked Image					
Extracted Watermark					
NC	**1**	**0.9998**	**0.9988**	**0.9975**	**0.9878**
BER	**0**	**0.0002**	**0.0011**	**0.0023**	**0.0112**

The process of data transmission is inevitably affected by noise. The noise may be caused by the source sensor equipment or added artificially. As a result, the ability to resist noise attacks is a basic requirement for a robust digital watermarking scheme. Common noises include Gaussian noise, salt and pepper noise, and speckle noise. Salt and pepper noise, also known as impulse noise, affects the extraction of watermark information by randomly changing the partial pixel value of the image to black and white. Gaussian noise refers to a kind of noise whose probability density function obeys

Gaussian distribution, and speckle noise is common in radar and sonar image processing. **Fig. 9(a)** shows the robustness of the scheme under noise attack. It can be seen from the **Fig. 9(a)** that the BER value of the watermark information extracted under the noise attack is not more than 0.04. That is, at most 4 bits out of 100 watermark bits are incorrect, so the human eye can easily distinguish the extracted watermark information.

In image processing, filtering is a common method for preprocessing images, it can eliminate image noise and achieve image smoothing and blurring. General filter processing includes mean filtering, median filtering and Gaussian filtering. Mean filtering can be taken as the average of surrounding pixels for each pixel. Median filtering replaces each pixel with the sorted median value of surrounding pixels, while Gaussian filtering refers to the gray value obtained after multiplying surrounding pixels by Gaussian distribution weight for each pixel. Recently, the popular method of extracting image features in the convolutional neural network (CNN) is to continuously carry out convolution operations, similar to filtering operations on images. The robustness of the scheme under filtering attacks is shown in **Fig. 9(b)**.

Geometric attacks make it impossible to do relevant watermark detection or restore the embedded watermark by destroying the synchronization of the carrier data and the watermark. Common geometric attacks include zoom, rotate, cut, and pan. It's easy to know that the proposed scheme has good robustness under the resizing, rotation and translation attacks in **Fig. 9(c)**. Moreover, the NC under cropping is still as high as 0.7, and the information contained in the watermark image can still be correctly recognized by the naked eye.

JPEG compression is the most vulnerable artificial attack when images are propagated in the network by removing redundant information from the image to affect the extraction of watermark. From the experimental results in **Fig. 9(d)**, the NC values of the proposed scheme under histogram equalization, brightness reduction and JPEG compression are all above 0.98, which means that the scheme has good robustness against these attacks.

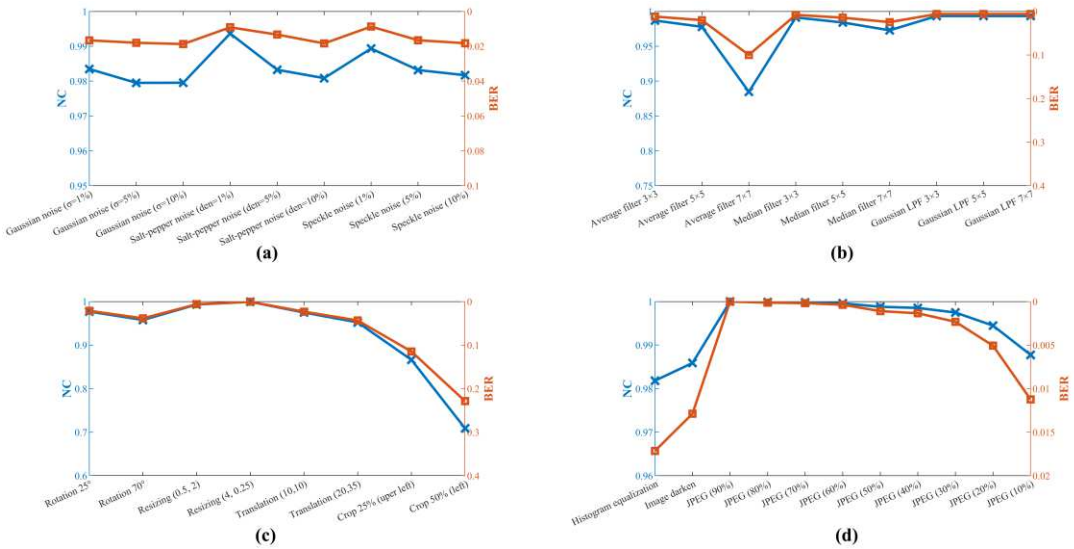


Fig. 9 NC and BER of extracted watermark extracted from the watermarked Lena image under various attacks (a) noise attacks (b) filter attacks (c) geometric attacks (d) other attacks.

4.3 Experimental comparison

In order to prove the superiority of the proposed scheme in terms of robustness, several latest robust watermarking schemes [26,9,16,31] are selected for comparison. The comparison results of NC values under various attacks is shown in **Fig. 10** and **Table 3**, and the cover image is Lena. As can be seen from **Table 3**, the robustness in JPEG compression, Gaussian noise, salt and pepper noise, speckle noise, median filtering 3×3, Gaussian filtering, resizing (0.5,2) is significantly better than other schemes. Moreover, the NC value is not lower than 0.95 under most attacks, which illustrates that the overall robustness of the scheme is very good, and it can meet the robustness requirements under most conditions.

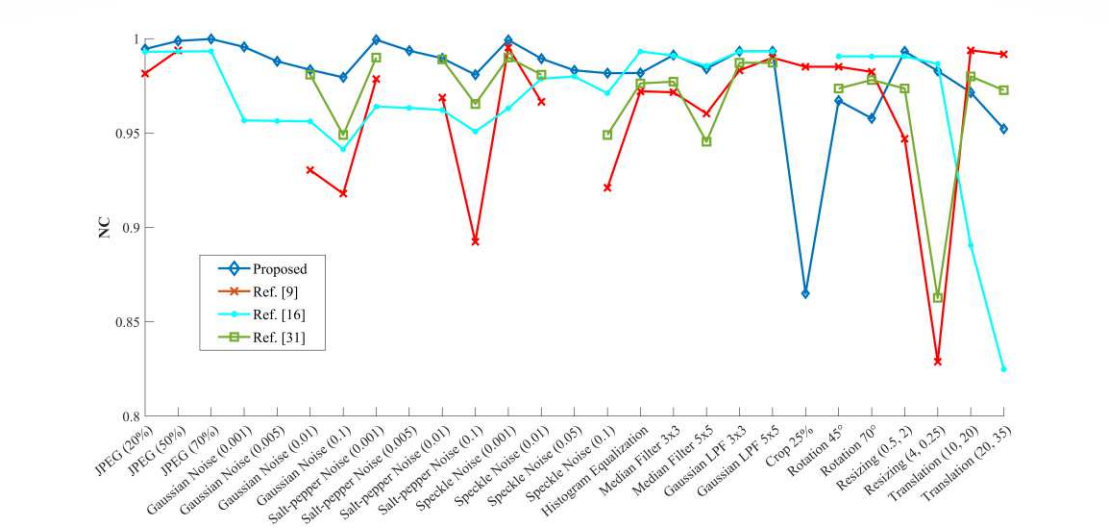


Fig. 10 The NC comparison of the proposed scheme with the existing non-blind robust watermarking schemes.

Table 3 Comparison of the proposed scheme with the existing similar schemes in term of robustness

Attack type	**Attack degree**		**Proposed**	**[26]**	**[9]**	**[16]**	**[31]**
JPEG Compression	QF	20%	**0.9945**	-	0.9815	0.9930	0.9872
		50%	**0.9988**	0.9639	0.9938	0.9932	-
		70%	**0.9998**	0.9837	-	0.9933	-
Gaussian Noise	Var	0.001	**0.9956**	0.9837	0.9838	0.9567	0.9900
		0.005	**0.9880**	0.9922	-	0.9564	-
		0.01	**0.9835**	0.9500	0.9304	0.9562	0.9809
		0.1	**0.975**	0.6827	0.9179	0.9414	0.9490
Salt-pepper Noise	Density	0.001	**0.9994**	0.9831	0.9786	0.9640	0.9900
		0.005	**0.9936**	0.9934	-	0.9633	-
		0.01	**0.9896**	0.9843	0.9688	0.9622	0.9890
		0.1	**0.9809**	0.8314	0.8924	0.9508	0.9654
Speckle Noise	Var	0.001	**0.9993**	-	0.9953	0.9631	0.9900
		0.01	**0.9894**	-	0.9666	0.9788	0.9809
		0.05	**0.9832**	-	-	0.9799	-

		0.1	**0.9817**	-	0.9210	0.9711	0.9490
Histogram Equalization	N/A		0.9818	0.9904	0.9721	**0.9932**	0.9763
Median Filter	Window size	3 × 3	**0.9913**	0.4576	0.9716	0.9910	0.9772
		5 × 5	0.9841	0.1656	0.9603	**0.9855**	0.9454
Gaussian LPF	Window size	3 × 3	**0.9933**	0.9916	0.9832	0.9932	0.9872
		5 × 5	**0.9933**	0.9916	0.9899	0.9932	0.9872
Crop 25%	Mean		0.8651	0.9795	**0.9851**	-	-
Rotation	Angle	45°	0.9672	0.4798	0.9851	**0.9906**	0.9736
		70°	0.9578	0.6629	0.9824	**0.9906**	0.9781
Resizing	Scale	0.5, 2	**0.9932**	0.5051	0.9470	0.9906	0.9736
		0.25, 4	0.9829	-	0.8289	**0.9866**	0.8627
Translation	Scale	10, 20	0.9715	-	**0.9938**	0.8906	0.9800
		20, 35	0.9522	-	**0.9917**	0.8249	0.9727

5. Conclusion

In this paper, a robust entropy-based image watermarking scheme in shearlet and wavelet domain is proposed. The multi-scale analysis method FFST is used to decompose the cover image, and the sub-band with the maximum entropy value is selected for DWT transformation, thus to improve the imperceptibility. By changing the coefficient of singular value matrix, the watermark is embedded to improve its ability to resist geometric attacks. Adaptive embedding position and embedding strength is optimized to make the watermarking scheme achieve "optimal". Information entropy is adopted as the criterion for embedding position selection, and the dynamic embedding intensity is obtained for each image block by combining the JND model of wavelet domain, which balances the imperceptibility and the robustness.

Availability of data and material

The datasets used or analysed during the current study are available from the corresponding author on reasonable request.

Competing interests

The authors have declared that no competing interests exist

Funding

The research was supported in part by Hainan Province Basic and Applied Basic Research Program (Natural Science Field) High-level Talent Project (Grant No. 2019RC044), and in part by Research project of Education and Teaching Reform of Hainan University (Grant No. hdjy2053), Funding Scheme to Outstanding Scientific and Technological Programs by Chinese Students Abroad (Grant No. Human Society Notice [2015]192 and [2016]176-2).

Authors' contributions

Xiaoyi Zhou contributed to the conception of the study;

Yujian Zhuang performed the experiment, the data analyses and wrote the manuscript; Sheng Liu helped perform the analysis with constructive discussions.

Acknowledgements

The research was supported in part by Hainan Province Basic and Applied Basic Research Program (Natural Science Field) High-level Talent Project (Grant No. 2019RC044), and in part by Research project of Education and Teaching Reform of Hainan University (Grant No. hdjy2053), Funding Scheme to Outstanding Scientific and Technological Programs by Chinese Students Abroad (Grant No. Human Society Notice [2015]192 and [2016]176-2).

References

1. Cox IJ, Miller ML, Bloom JA, Honsinger C (2002) Digital watermarking, vol 53. Springer,

2. Cox IJ, Kilian J, Leighton T, Shamoon T Secure spread spectrum watermarking for images, audio and video. In: Proceedings of 3rd IEEE International Conference on Image Processing, 1996. IEEE,

pp 243-246

3. Thulasidharan PP, Nair MS (2015) QR code based blind digital image watermarking with attack detection code. AEU - International Journal of Electronics and Communications 69 (7):1074-1084. doi:10.1016/j.aeue.2015.03.007

4. Van Schyndel RG, Tirkel AZ, Osborne CF A digital watermark. In: Proceedings of 1st International Conference on Image Processing, 1994. IEEE, pp 86-90

5. Makbol NM, Khoo BE (2013) Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. AEU-International Journal of Electronics and Communications 67 (2):102-112

6. Araghi TK, Manaf AA, Araghi SK (2018) A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. Expert Systems with Applications 112:208-228. doi:10.1016/j.eswa.2018.06.024

7. Thanki R, Kothari A, Trivedi D (2019) Hybrid and blind watermarking scheme in DCuT – RDWT domain. Journal of Information Security and Applications 46:231-249. doi:10.1016/j.jisa.2019.03.017

8. Singh SP, Bhatnagar G (2018) A new robust watermarking system in integer DCT domain. Journal of Visual Communication and Image Representation 53:86-101. doi:10.1016/j.jvcir.2018.03.006

9. Vali MH, Aghagolzadeh A, Baleghi Y (2018) Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition. Expert Systems with Applications 114:296-312

10. Liu J, Wu S, Xu X (2018) A Logarithmic Quantization-Based Image Watermarking Using Information Entropy in the Wavelet Domain. Entropy 20 (12):945

11. Tikariha M, Dey AK (2015) An efficient JND based digital image watermarking using hybrid DWT-DCT-SVD approach. INTERNATIONAL JOURNAL OF SCIENTIFIC PROGRESS AND RESEARCH (IJSPR) 10 (1):11-20

12. Hu H-T, Chang J-R, Hsu L-Y (2016) Robust blind image watermarking by modulating the mean of partly sign-altered DCT coefficients guided by human visual perception. AEU-International Journal of Electronics and Communications 70 (10):1374-1381

13. Campisi P, Kundur D, Neri A (2004) Robust digital watermarking in the ridgelet domain. IEEE signal processing letters 11 (10):826-830

14. Kalantari NK, Ahadi SM, Vafadust M (2009) A robust image watermarking in the ridgelet domain using universally optimum decoder. IEEE Transactions on circuits and systems for video technology 20 (3):396-406

15. Rabizadeh M, Amirmazlaghani M, Ahmadian-Attari M (2016) A new detector for contourlet

domain multiplicative image watermarking using Bessel K form distribution. Journal of Visual Communication and Image Representation 40:324-334. doi:10.1016/j.jvcir.2016.07.001

16. Najafi E, Loukhaoukha K (2019) Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform. Journal of Information Security and Applications 44:144-156. doi:10.1016/j.jisa.2018.12.002

17. Wang X-y, Zhang S-y, Wen T-t, Yang H-y, Niu P-p (2019) Coefficient difference based watermark detector in nonsubsampled contourlet transform domain. Information Sciences 503:274-290

18. Niu P-P, Wang X-Y, Jin H-B, Lu M-Y (2011) A feature-based robust digital image watermarking scheme using bandelet transform. Optics & Laser Technology 43 (3):437-450

19. Mardanpour M, Chahooki MAZ (2016) Robust transparent image watermarking with Shearlet transform and bidiagonal singular value decomposition. AEU-International Journal of Electronics and Communications 70 (6):790-798

20. Wang X-y, Liu Y-n, Xu H, Wang A-l, Yang H-y (2016) Blind optimum detector for robust image watermarking in nonsubsampled shearlet Domain. Information Sciences 372:634-654. doi:10.1016/j.ins.2016.08.076

21. Ahmaderaghi B, Kurugollu F, Rincon JMD, Bouridane A (2018) Blind Image Watermark Detection Algorithm Based on Discrete Shearlet Transform Using Statistical Decision Theory. IEEE Transactions on Computational Imaging 4 (1):46-59

22. Subramani S, Omprakash Narayanan L, Kamalanathan C, Panda S, Sreenivas B (2020) Design of robust image watermarking technique based on shearlet transform and QR matrix decomposition. Journal of Interdisciplinary Mathematics 23 (1):163-174

23. Xiang-yang W, Tao-tao W, Xin S, Pan-pan N, Hong-ying Y (2020) A New Watermark Decoder in DNST Domain Using Singular Values and Gaussian-Cauchy Mixture-Based Vector HMT. Information Sciences

24. Easley G, Labate D, Lim W-Q (2008) Sparse directional image representations using the discrete shearlet transform. Applied and Computational Harmonic Analysis 25 (1):25-46

25. Häuser S, Steidl G (2012) Fast finite shearlet transform. arXiv preprint arXiv:12021773

26. Thanki R, Kothari A, Trivedi D (2019) Hybrid and blind watermarking scheme in DCuT–RDWT domain. Journal of Information Security and Applications 46:231-249

27. Sangeetha N, Anita X (2018) Entropy based texture watermarking using discrete wavelet transform. Optik 160:380-388. doi:10.1016/j.ijleo.2018.01.136

28. Singh G, Goel N Entropy based image watermarking using discrete wavelet transform and singular value decomposition. In: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016. IEEE, pp 2700-2704

29. Abdelhakim AM, Abdelhakim M (2018) A time-efficient optimization for robust image watermarking using machine learning. Expert Systems with Applications 100:197-210. doi:10.1016/j.eswa.2018.02.002

30. Hu H-T, Chang J-R, Hsu L-Y (2016) Robust blind image watermarking by modulating the mean of partly sign-altered DCT coefficients guided by human visual perception. AEU - International Journal of Electronics and Communications 70 (10):1374-1381. doi:https://doi.org/10.1016/j.aeue.2016.07.011

31. Mardanpour M, Chahooki MAZ (2016) Robust transparent image watermarking with Shearlet transform and bidiagonal singular value decomposition. AEU - International Journal of Electronics and Communications 70 (6):790-798. doi:https://doi.org/10.1016/j.aeue.2016.03.004

32. Wang X-y, Xu H, Zhang S-y, Liang L-l, Niu P-p, Yang H-y (2018) A Color Image Watermarking Approach Based on Synchronization Correction. Fundamenta Informaticae 158 (4):385-407

33. Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixel-wise masking. IEEE transactions on image processing 10 (5):783-791

34. Zhou X, Ma J, Du W, Zhao B, Petridis M, Zhao Y BMQE system: a MQ equations system based on ergodic matrix. In: 2010 International Conference on Security and Cryptography (SECRYPT), 2010. IEEE, pp 1-5

35. Zhou X, Ma J, Du W, Zhao B, Chen M, Zhao Y Cryptanalysis of the bisectional MQ equations system. In: 2010 10th IEEE International Conference on Computer and Information Technology, 2010. IEEE, pp 1038-1043

36. Zhou X, Cao C, Ma J, Wang L (2018) Adaptive digital watermarking scheme based on support vector machines and optimized genetic algorithm. Mathematical Problems in Engineering 2018

37. Zhang J, Zhou X, Yang J, Cao C, Ma J (2019) Adaptive Robust Blind Watermarking Scheme Improved by Entropy-Based SVM and Optimized Quantum Genetic Algorithm. Mathematical Problems in Engineering 2019

Figures

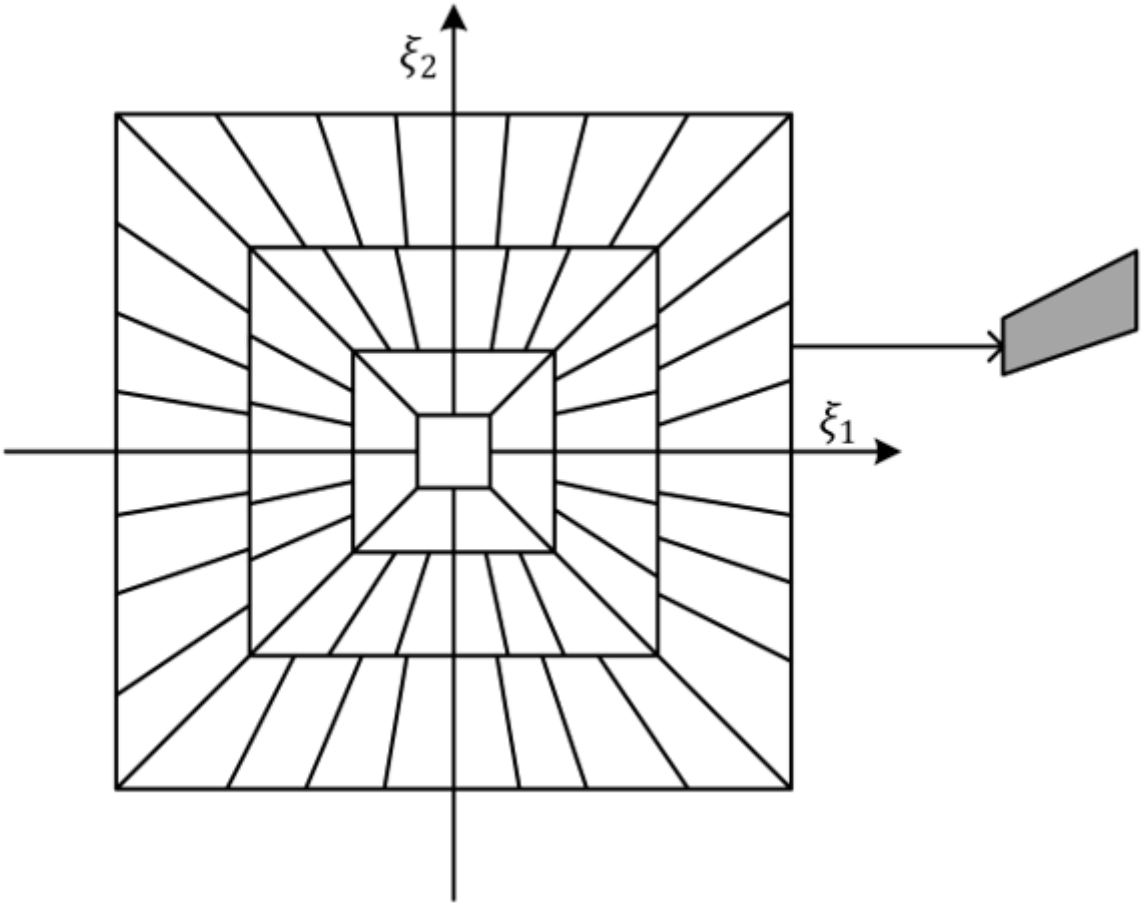
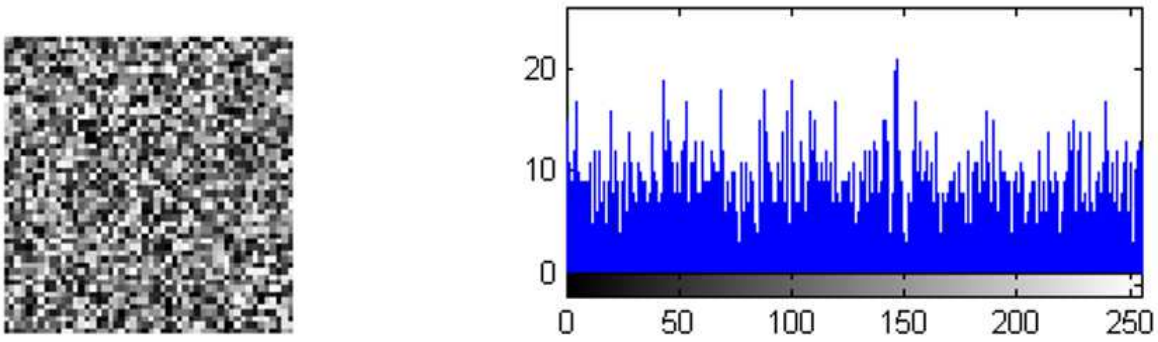


Figure 1

The tiling of frequency plane and frequency support of a shearlet.



(1) Image of a Random 50×50 Ergodic Matrix (2) Histogram of a Random Ergodic Matrix

Figure 2

Image of a Random Ergodic Matrix and the Corresponding Histogram

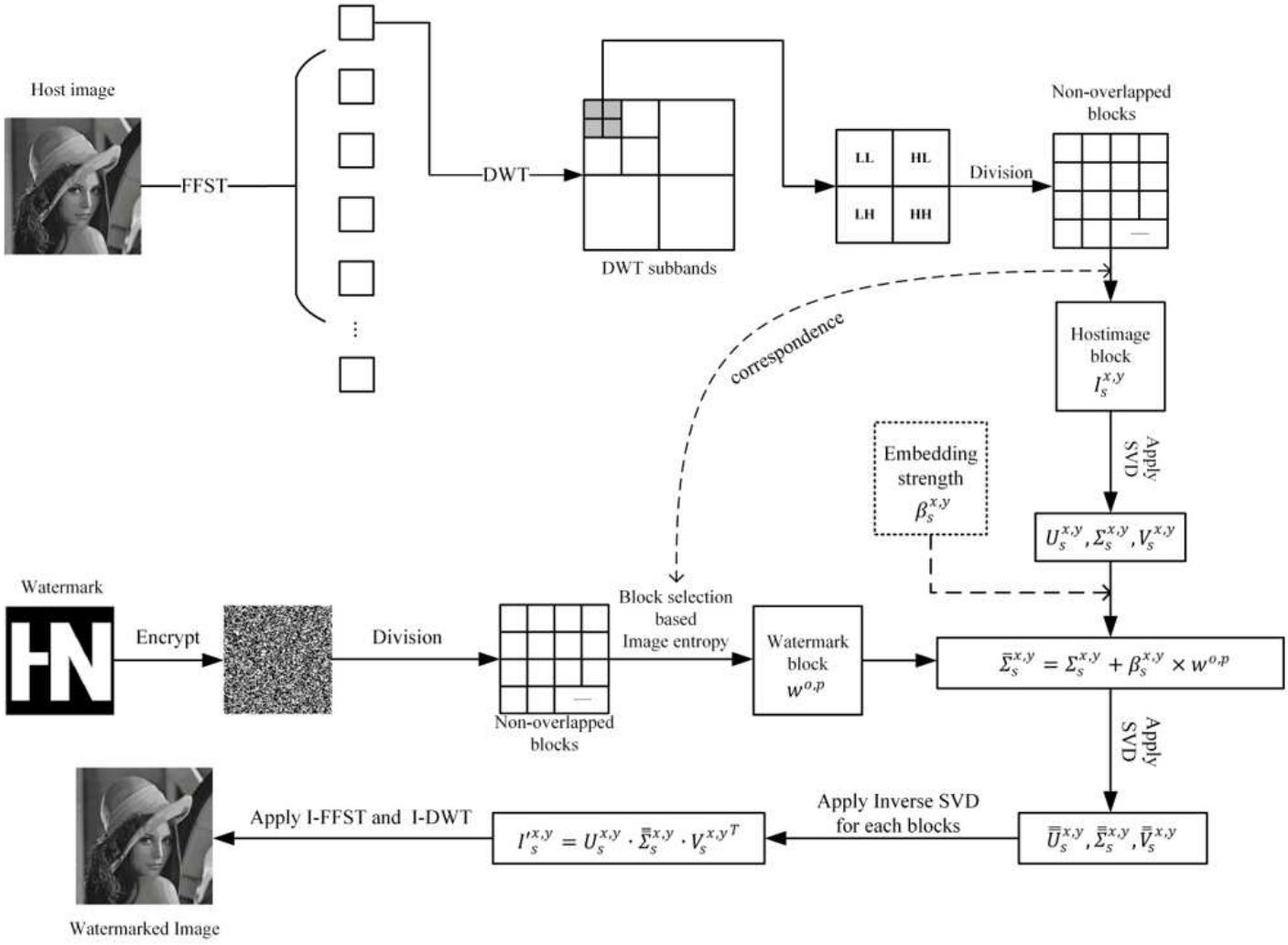


Figure 3

The watermark embedding procedure.

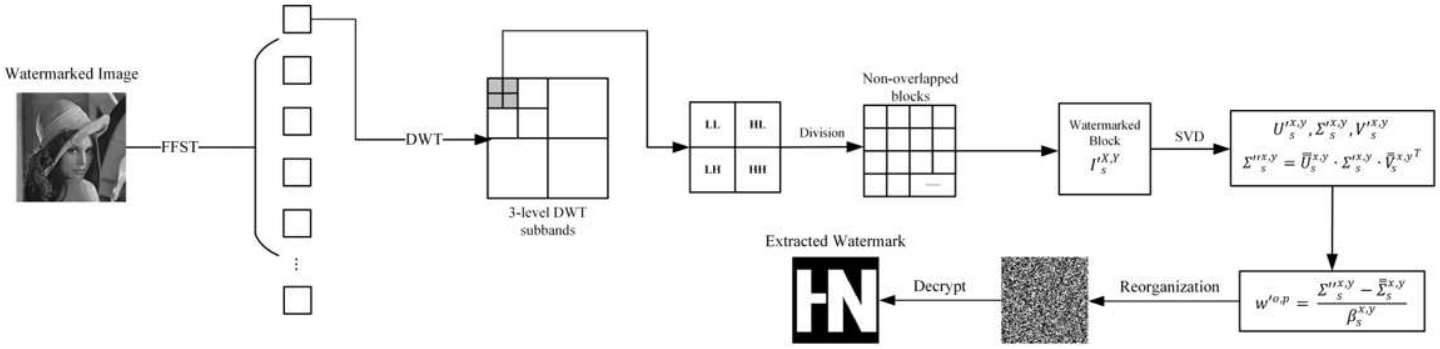


Figure 4

The watermark extraction procedure.

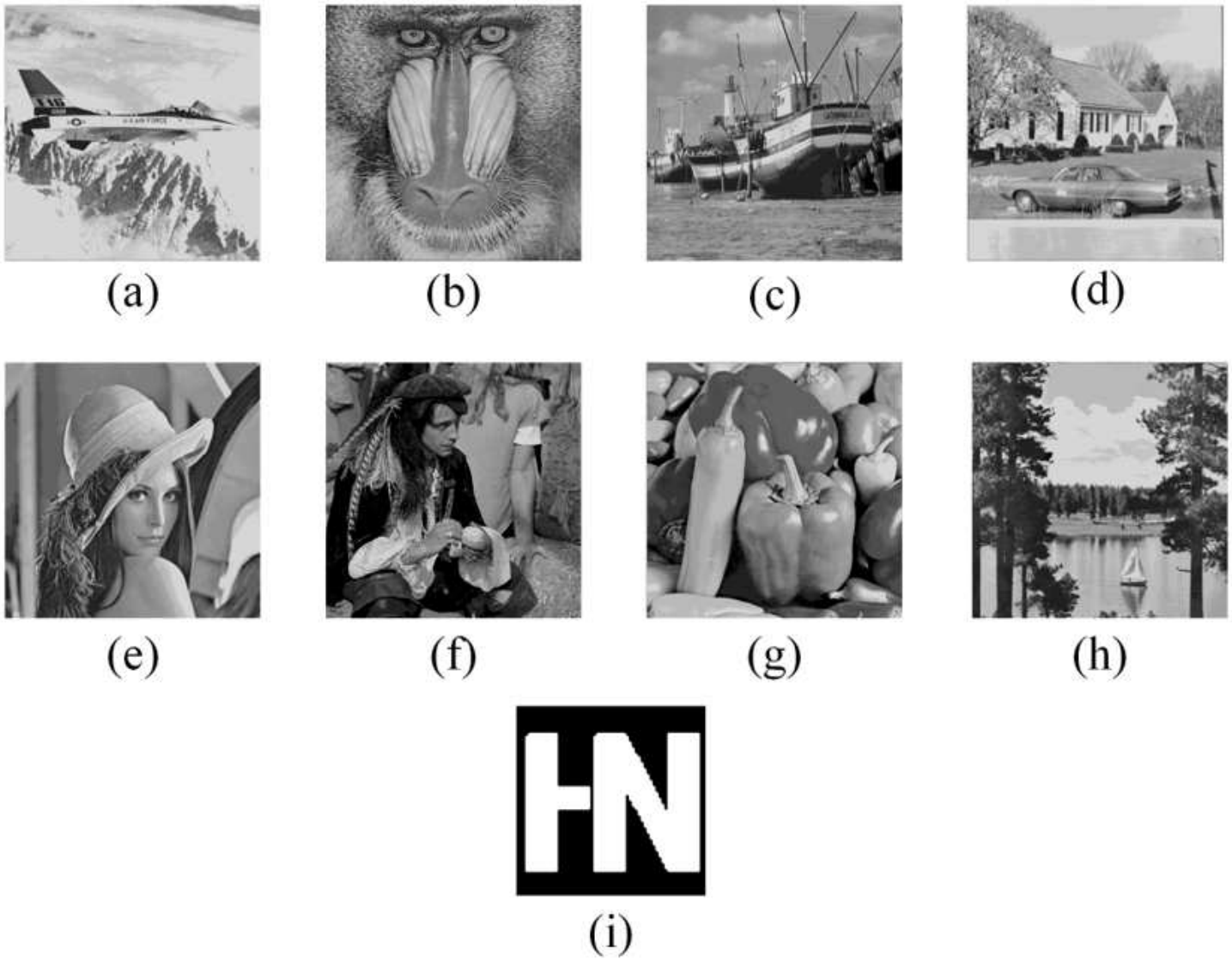


Figure 5

Cover and watermark images (a) Airplane (b) Baboon (c) Boat (d) House (e) Lena (f) Man (g) Peppers (h) Sailboat (i) Watermark logo.

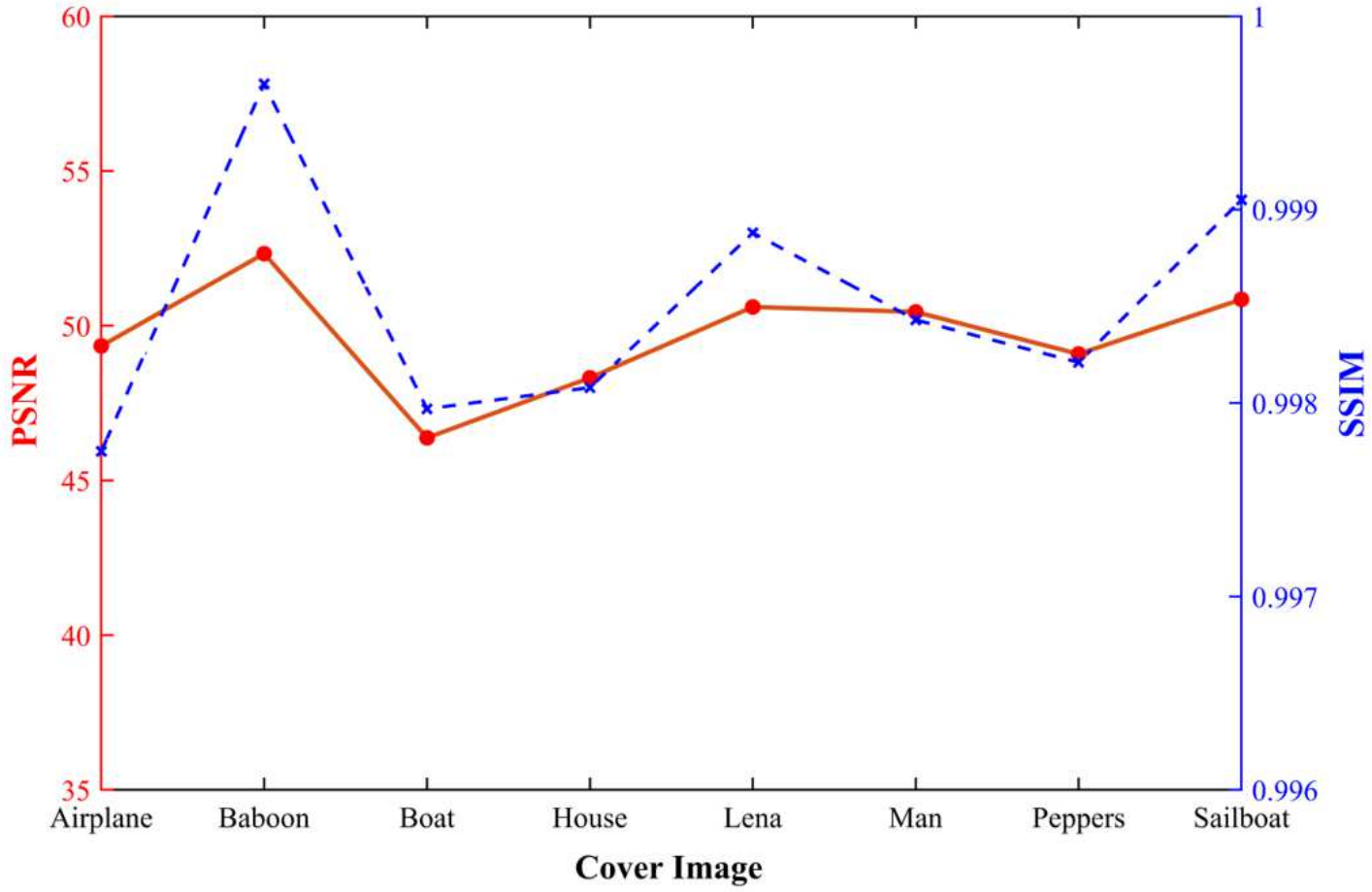


Figure 6

The imperceptibility of proposed scheme

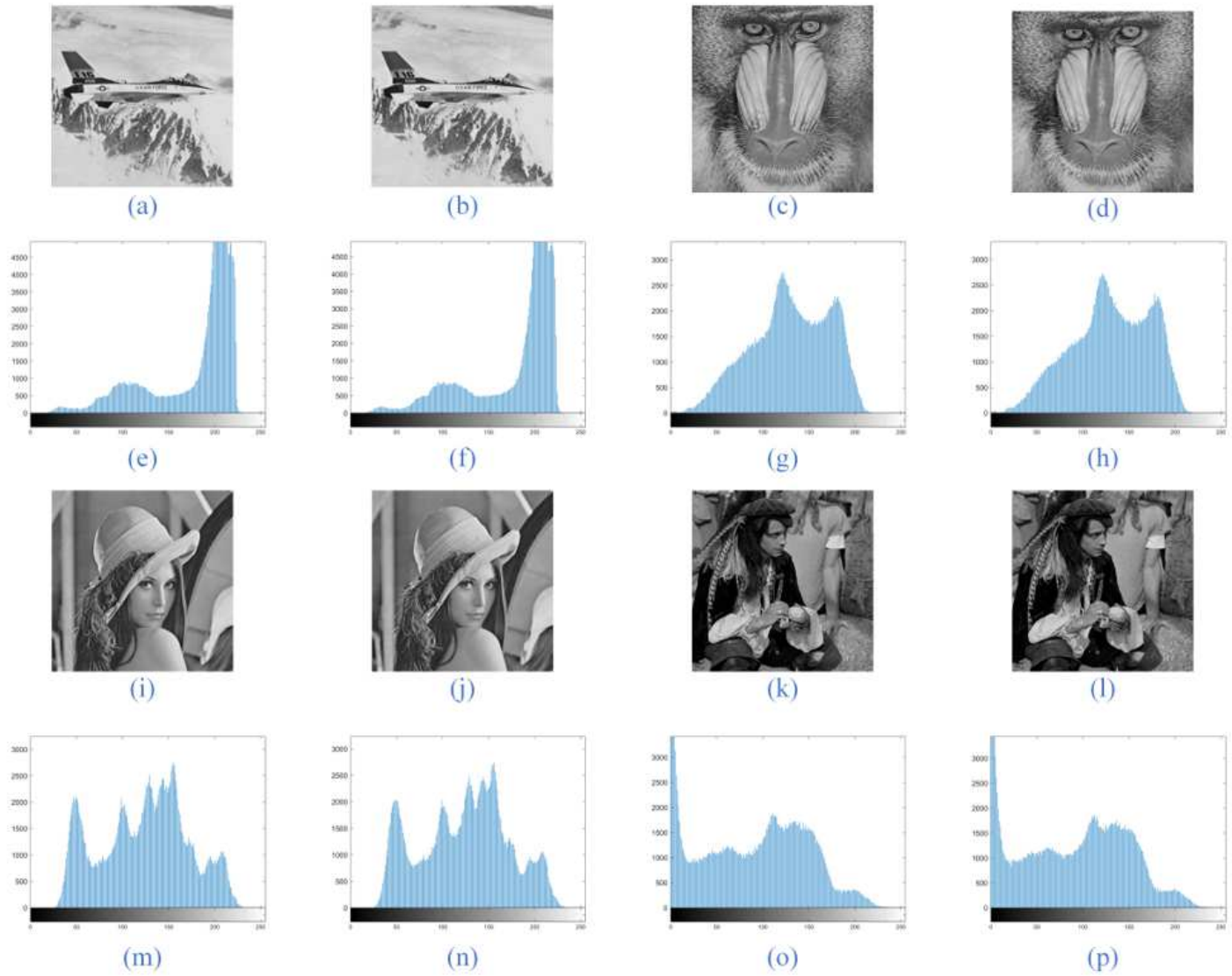


Figure 7

Histogram comparison of original image and watermarked image: Original Image (a), (c), (i), (k); Watermarked Image (b), (d), (j), (l); Histogram Information of original image (e), (g), (m), (o); Histogram Information of watermarked image (f), (h), (n), (p).

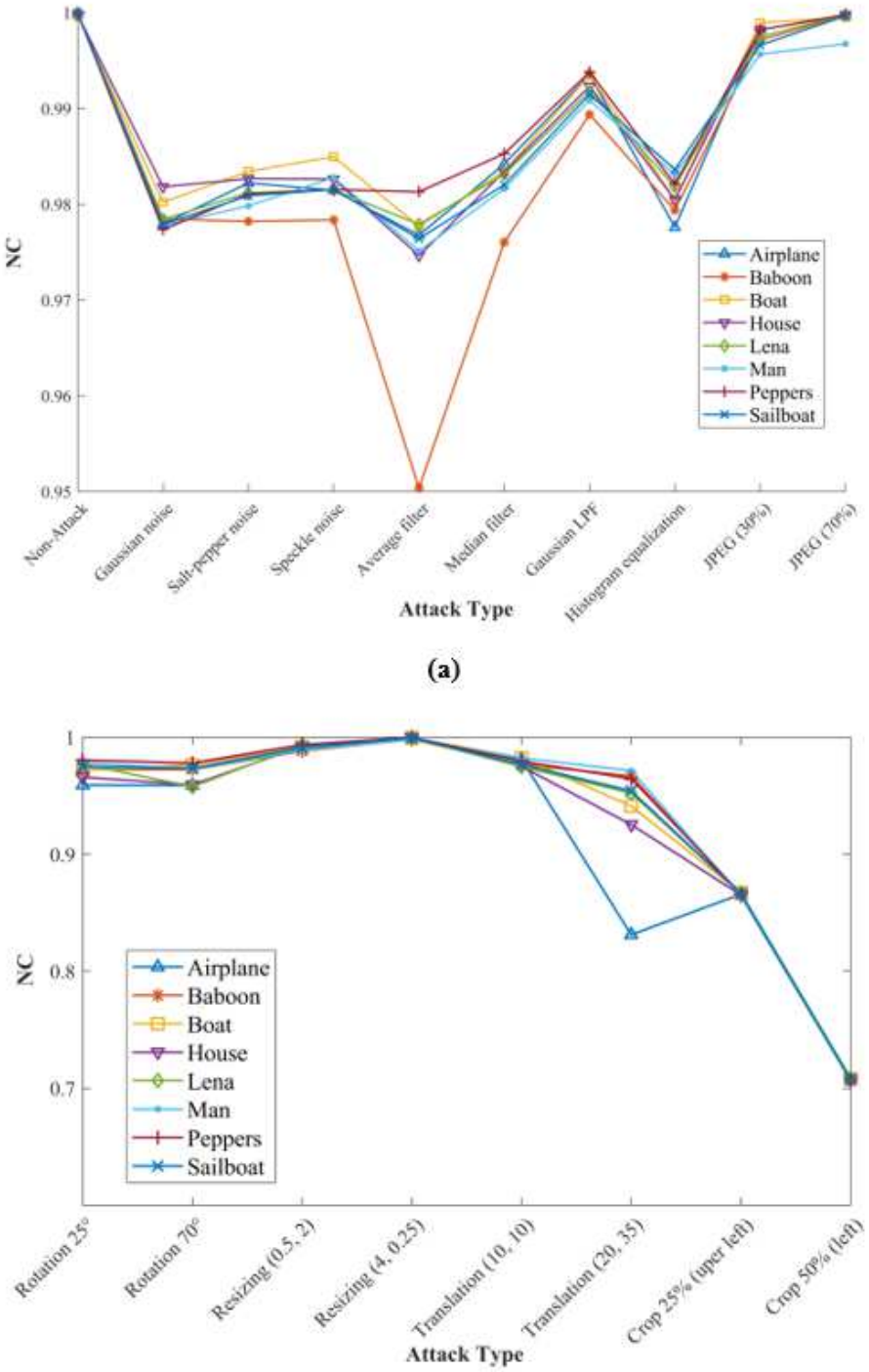


Figure 8

The robustness of proposed scheme (a) General attack (b) Geometric attack

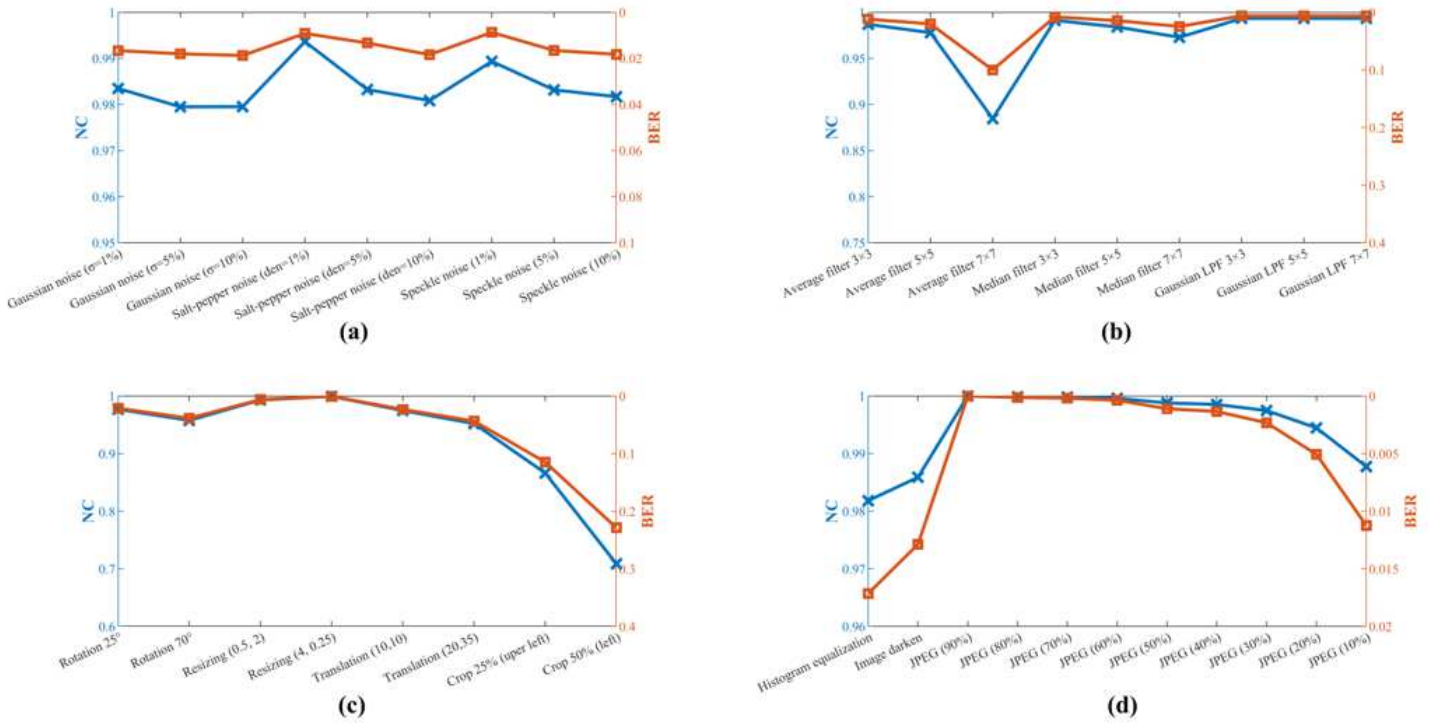


Figure 9

NC and BER of extracted watermark extracted from the watermarked Lena image under various attacks (a) noise attacks (b) filter attacks (c) geometric attacks (d) other attacks.

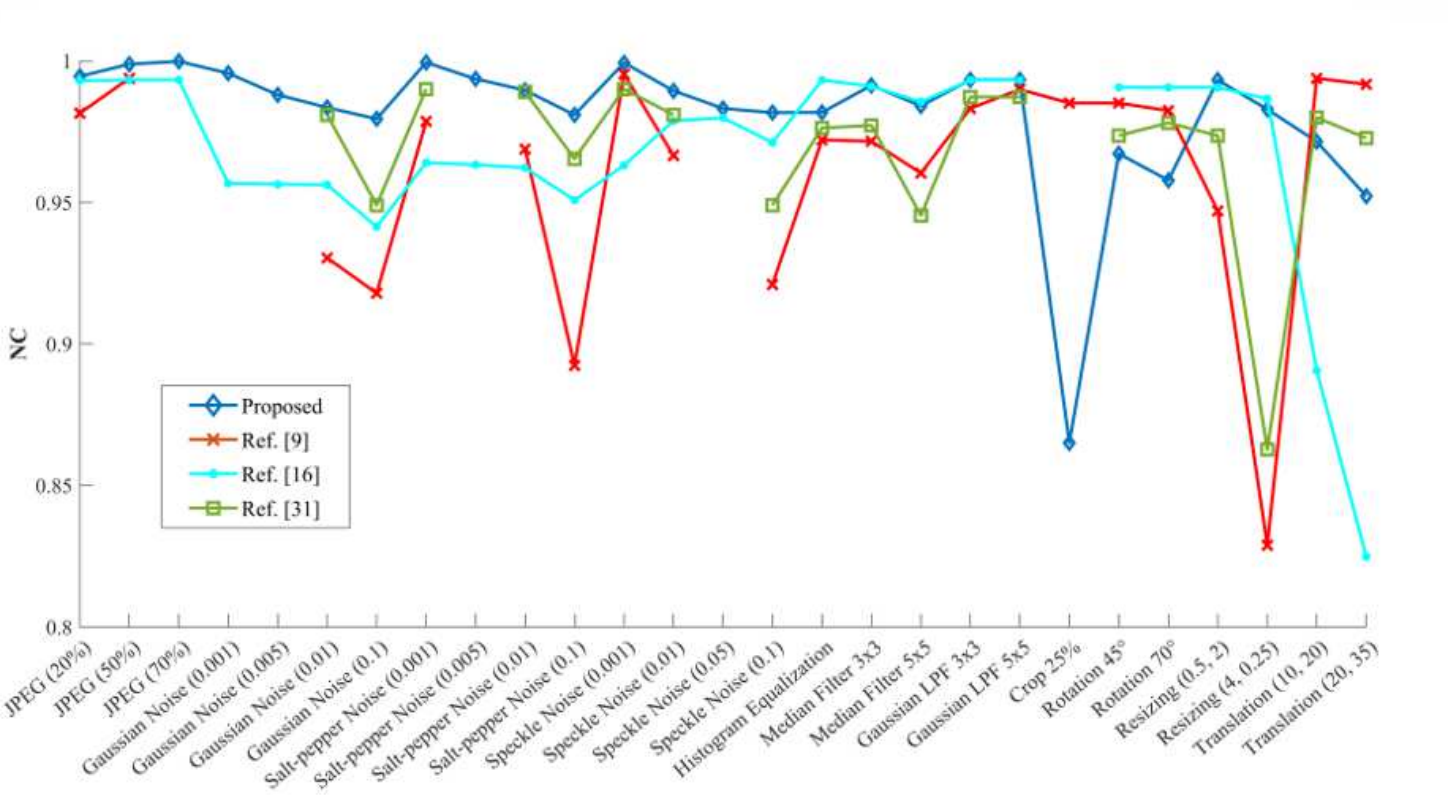
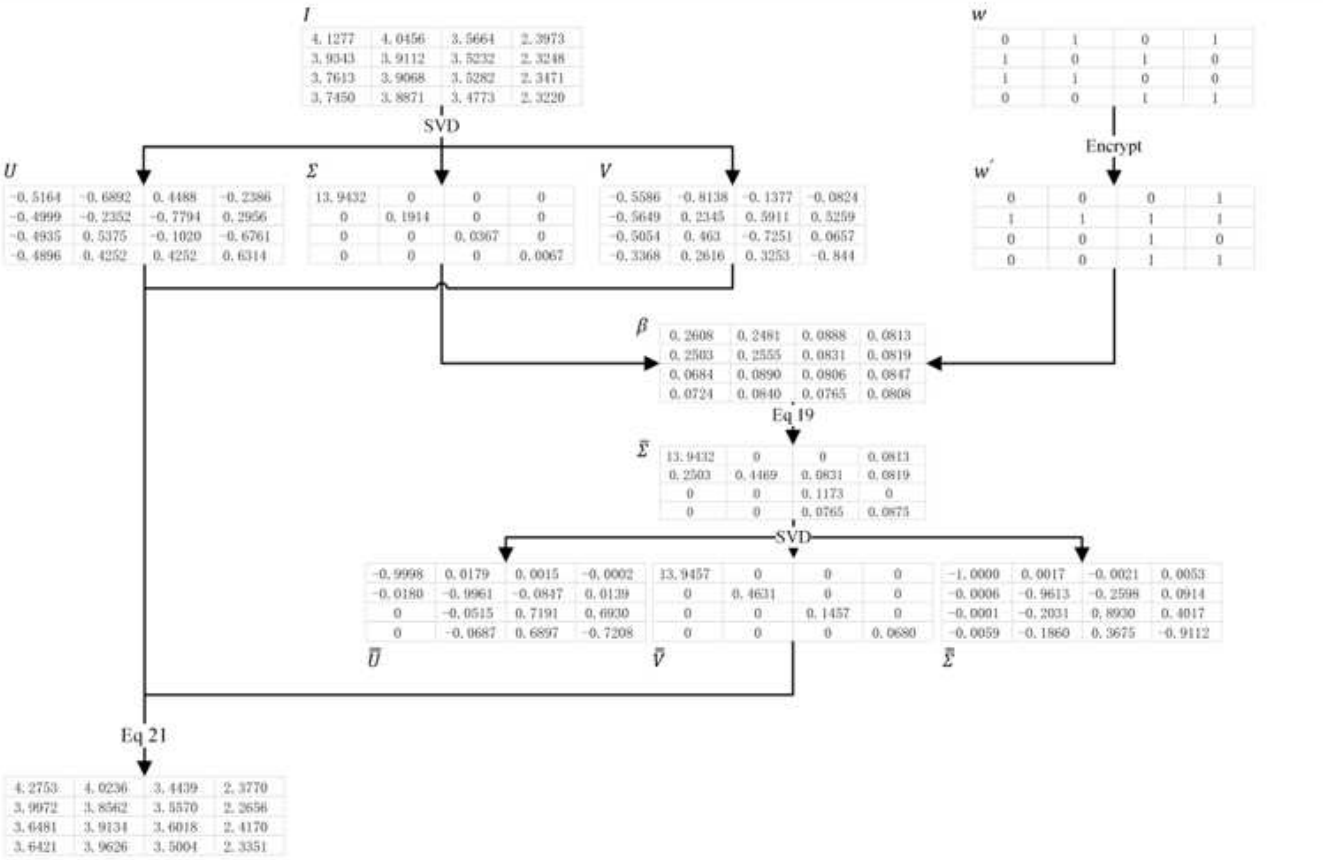
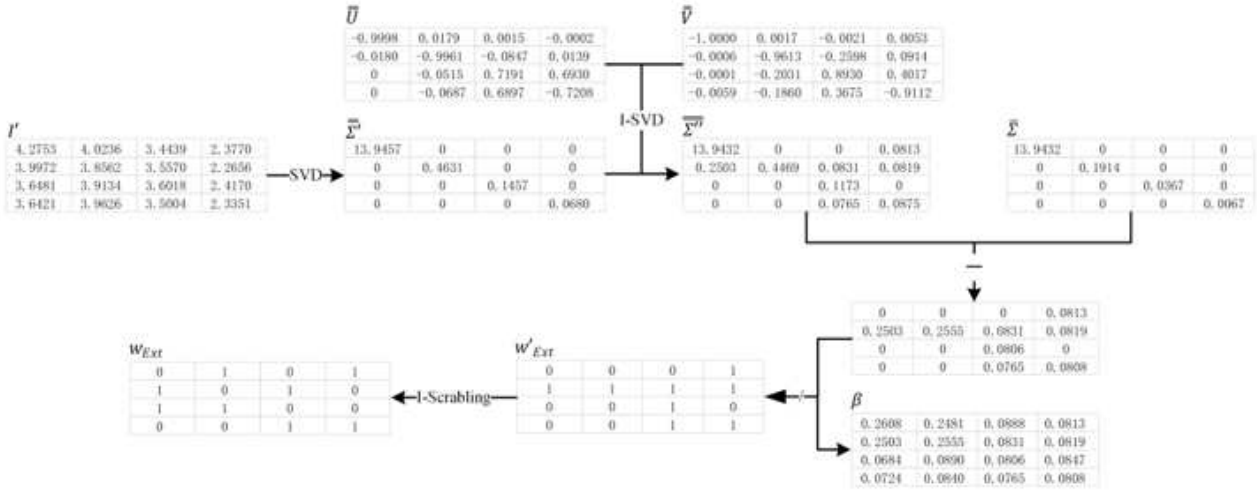


Figure 10

The NC comparison of the proposed scheme with the existing non-blind robust watermarking schemes.



Example 1



Example 2

Figure 11

Examples 1-2