algorithms

MDPI

Article

RST Resilient Watermarking Scheme Based on DWT-SVD and Scale-Invariant Feature Transform

Yunpeng Zhang, Chengyou Wang * and Xiao Zhou

School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai 264209, China; zhyp@mail.sdu.edu.cn (Y.Z.); zhouxiao@sdu.edu.cn (X.Z.)

* Correspondence: wangchengyou@sdu.edu.cn; Tel.: +86-631-568-8338

Academic Editor: Pierre Leone
Received: 17 January 2017; Accepted: 22 March 2017; Published: 30 March 2017

Abstract: Currently, most digital image watermarking schemes are affected by geometric attacks like rotation, scaling, and translation (RST). In the watermark embedding process, a robust watermarking scheme is proposed against RST attacks. In this paper, three-level discrete wavelet transform (DWT) is applied to the original image. The three-level low frequency sub-band is decomposed by the singular value decomposition (SVD), and its singular values matrix is extracted for watermarking embedding. Before the watermarking extraction, the keypoints are selected by scale-invariant feature transform (SIFT) in the original image and attacked image. By matching the keypoints in two images, the RST attacks can be precisely corrected and the better performance can be obtained. The experimental results show that the proposed scheme achieves good performance of imperceptibility and robustness against common image processing and malicious attacks, especially geometric attacks.

Keywords: image watermarking; scale-invariant feature transform (SIFT); discrete wavelet transform (DWT); singular value decomposition (SVD); geometric attacks

1. Introduction

With the tremendous growth in information industry recently, as one of the most essential methods to convey the information from one side to the other, digital images can be easily tampered, which can consequently result in security problems with copyright issues. Thus, the scheme for the authenticity and integrity of image protection becomes essential and meaningful. To solve this problem, digital signatures [1,2] and digital image watermarking [3] are proposed. Because digital signatures can only estimate whether images are tampered but cannot locate the tampered region, the watermarking technique, an effective method to solve the copyright problem of image content, is proposed. According to different characters, watermarking can be classified into three categories: (i) robust watermarking used for copyright protection, which can resist all kinds of attacks; (ii) fragile watermarking, which is sensitive to attacks including malicious tampering and common processing; and (iii) semi-fragile watermarking used to distinguish malicious tampering from non-malicious modification, which is a combination of advantages of robust and fragile watermarking. In addition, both fragile watermarking methods and semi-fragile watermarking methods can be applied in image tamper, location, and recovery.

From the perspective of the working domain where the watermark is embedded, this effective technique can be divided into spatial domain and transform domain [4]. The spatial domain methods modify the pixel value of the digital image directly to embed the watermark information. The advantages of spatial watermarking method are easy implementation and low computational complexity. However, this kind of method is fragile to the common image processing operation and other attacks. In contrast, the watermark information is embedded into the host image by modifying transform coefficients of the original image in the transform domain methods. Compared with spatial methods, methods based on mathematical transform have better imperceptibility and robustness. Discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT), and singular value decomposition (SVD) [5] are the common transforms applied in the transform domain watermarking.

Owing to its stable algebraic character, SVD is applied as a normal method for watermarking scheme, especially for robust watermarking. Liu and Tan [6] firstly introduced the typical watermarking algorithm based on SVD. In this method, singular values obtained by SVD are modified for the purpose of embedding the watermarking into the host image. In the watermark embedding process, the watermark information is embedded in the form of weighted sum with the help of the scale factors. Different from Liu and Tan's scheme, Chang et al. [7] proposed another SVD based watermarking scheme, where the watermark is embedded by substituting the specific singular value with the watermark value. In addition, Su et al. [8] introduced a blind dual color image watermarking scheme based on SVD. By analyzing the orthogonal matrix U generated from the SVD, a similarity correlation, in which elements in the second row first column and the third row first column have the same sign and high normalized cross-correlation, is found between these two elements, which can be used in watermarking embedding and extraction. Liu et al. [9] proposed quantized SVD (QSVD) based blind watermarking method, which realized embedding of the watermark by modifying the quaternion elements in U matrix. Worthy of mention is the quaternion, a type of hyper-complex number, consists of one real component and three imaginary components, and an image can be encoded into the form of quaternion. To obtain better performance of the watermarking algorithm, some hybrid schemes based on SVD and other transforms have been proposed. In [10], Li et al. introduced a novel watermarking algorithm based on SVD and DCT. Two bits of a watermark are being embedded into a 32×32 macro-block in the high frequency band of SVD-DCT blocks. This method does not require any additional information except a key for extraction. Sverdlov et al. [11] embedded the watermark after DCT into four quadrants/blocks performed by SVD, which DCT coefficients are mapped to, and singular values of the watermark after DCT are embedded into each quadrant. Lai et al. [12] proposed a DWT and SVD based watermarking scheme, embedding the watermark information into singular values of the host image's DWT sub-bands. In [13], with the help of directive contrast operation as well as wavelet coefficients, Bhatnagar and Raman obtained the reference image and embedded the watermark into a reference image based on SVD and DWT. Mishra et al. [14] proposed an optimized image watermarking based on DWT-SVD and the Firefly algorithm. The singular value of a binary watermark is embedded into the three-level low frequency sub-band, also known as LL sub-band, by the use of optimized scaling factors. In [15], Narula et al. made an analysis on DWT watermarking scheme and DWT-SVD watermarking scheme used in RGB images, concluding that the hybrid DWT-SVD based scheme has better performance than the conventional DWT based scheme. D. Singh and S. K. Singh [16] proposed a robust watermarking scheme based on DWT, SVD, and DCT with Arnold encryption, solving the false positive problem. In [17], Ansari et al. proposed integer wavelet transform (IWT) and SVD based watermarking, making use of these transforms properties to solve the false positive problem. To optimize the scaling factor, the artificial bee colony (ABC) algorithm is applied to improve the quality of watermarking.

Although SVD is applied in the watermarking scheme because of its stability, robustness of schemes based on SVD and other transforms to geometrical attacks is not satisfying. Rotation, scaling, and translation (RST) [18] are common geometrical attacks in image processing. Because of RST attacks on the host image, the watermark cannot be detected and extracted as normal. It is urgent to research and propose the watermark method with the resistance to the RST attacks [19]. To solve this problem, the scale-invariant feature transform (SIFT) [20] is applied in image watermarking, which is a type of efficient method for interesting points detection and extraction, as well as local feature description. Due to its significant function, SIFT is widely applied in computer vision field, such as image matching and image object recognitions. There are some characters in SIFT, including invariant character to RST and robustness against affine transform. Thus, SIFT can be applied in various kinds of fields such as object recognition, image indexing, segmentation, registration, and data hiding [21]. In recent years, SIFT is applied extensively in watermarking. Lee et al. [22] proposed a novel image watermarking scheme using local invariant features, as well as embedding the watermark into the patches in circle shapes generated by SIFT. To deal with the synchronization errors, Luo et al. [23] proposed an adaptive watermarking scheme based on DFT and SIFT. In this method, DFT is performed on the sub-image selected from the host image for watermark embedding. In [24], Lyu et al. proposed image watermarking scheme based on SIFT and DWT, where they applied the DWT on the selected SIFT areas. Thorat and Jadhav [25] proposed an anti-geometrical attacks watermarking scheme based on IWT and SIFT. This scheme applied SIFT on the red components of the image, extracted the feature points and performed IWT on the blue and green components to extract low-frequency coefficients for watermark embedding. Pham et al. [26] proposed a robust watermarking scheme based on SIFT and DCT, embedding the watermark into the selected feature region after DCT. In [27], Zhang and Tang proposed a watermarking algorithm based on SVD and SIFT to solve the synchronization problem. The SIFT is used for watermarking resynchronization. The embedding of watermark is done using SVD technique, and SIFT algorithm is used to find feature points, which is further used for watermarking detection. Besides that, for geometric invariance of the watermarking schemes, the moments transform domain has attracted the watermarking community as an alternative transform domain to embed the watermark recently. In [28], Yuan and Pun introduced a geometric invariant watermarking based on SIFT and Zernike moments, where SIFT is applied to obtain the circular region as well as the Zernike moment performed on binary regions, and magnitudes of local Zernike moments altered for watermark embedding. In [29], Wang et al. proposed a geometrically invariant watermarking scheme using radial harmonic Fourier moments to embed the watermark into their magnitudes by quantization. Tsougenis et al. [30] made great efforts to analyze advantages and disadvantages of watermarking methods based on moment theory, and achieved comparative study on performance of moment-based watermarking scheme. Due to the efficiency of SIFT for image matching and image features, it is becoming an innovative option for the image watermarking method in recent years. The basic theory of the SIFT will be illustrated later in Section 2.

In this paper, a new robust watermarking scheme based on SVD, DWT, and SIFT is proposed. Firstly, the host image is performed by DWT for three times, and the LL_3 sub-band is selected for SVD operation. Then, the watermark is embedded into the three-level LL_3 sub-band. The SIFT keypoints, also known as feature points, are saved as keys for correcting the RST attacks. In the extraction process, the capability of attack resistance can be attained owing to the SIFT feature matching. Experimental results show that, with the excellent imperceptibility, the proposed scheme is resilient to both common image processing and various attacks, e.g., Gaussian noise, salt and pepper noise, RST, cropping, etc.

The rest of this paper is organized as follows. In Section 2, we present the SIFT algorithm. Section 3 addresses the concrete watermark embedding and extraction procedures. Section 4 gives experimental evaluation of robustness and imperceptibility compared with previous schemes, and demonstrates the advantage of the proposed scheme. Conclusions and the future works are given finally in Section 5.

2. SIFT Algorithm

Lowe [20] proposed to extract the local scale-invariant feature keypoints of descriptors, and use these descriptors for the matching of two related images. Generating steps of SIFT feature descriptor are described, which contains four parts in total.

2.1. Scale-Space Peak Selection

The basic theory of the scale-space approach [31] is to introduce a scale parameter in the visual information processing model and obtain visual processing information on different scales by continuously changing scale parameters. Then, the information is integrated to explore essential characteristics of the image. For achieving the scale transformation, Gaussian convolution kernel [32] is the only linear kernel applied. The scale-space kernel f_{out} can be defined as Equation (1):

$$f_{\text{out}} = K_{\text{n}} * f_{\text{in}}, \tag{1}$$

where K_{n} is the kernel, f_{in} is the input signal, and $*$ represents the convolutional calculation.

The scale-space $S(x, y, \sigma)$ of the image $I(x, y)$ is shown as Equation (2):

$$S(x,y,\sigma) = G(x,y,\sigma) * I(x,y),\ G(x,y,\sigma) = \frac{1}{2\pi\sigma^2} \mathrm{e}^{-(x^2+y^2)/2\sigma^2}, \tag{2}$$

where $G(x, y, \sigma)$ is the scale variable Gaussian function, (x, y) is the spatial coordinates, and σ is the scale-space factor, which decides the smoothness of the image. The large value of σ represents smoother image overview features of large scales, and the small value of σ describes the abundant image detailed features of small scales.

To detect stable points in scale-space effectively, Lowe [20] proposed the difference of Gaussian (DOG) scale-space presented as Equation (3):

$$D(x,y,\sigma) = [G(x,y,k\sigma) - G(x,y,\sigma)] * I(x,y) = S(x,y,k\sigma) - S(x,y,\sigma), \tag{3}$$

where $I(x, y)$ is the input image and k is the multiple between two neighboring scale-spaces.

With the help of DOG scale-space image, all extreme points can be detected as keypoints in the candidate points.

2.2. Keypoints Location

The next step is to locate keypoints, aiming at orientating the location of keypoints precisely. In this way, a large number of extreme points are obtained. However, not all the extreme points are keypoints, and there should be a method to eliminate some points. There are two steps for point elimination: rough picking and fine picking. Rough picking is mainly to pick those candidate keypoints with low contrast and marginalized candidate keypoints. Due to fact that the DOG operator has a strong response for image edges, fine picking is adopted in the way of edge response to further eliminate the keypoints. Thus, the procedure of keypoint location has been completed.

2.3. Direction Matching

The next step is the keypoint orientation assignment, and the purpose is to achieve the SIFT features of rotation invariance. For scaling smoothed image I_{L}, which means that the image I_{L} has been performed by keypoint elimination, we compute the central derivative of I_{L} at every keypoints. Further scale and orientation at every keypoint (x, y) can be calculated by Equation (4):

$$\begin{cases} \theta(x,y) = \text{arctan2}\{[I_{\text{L}}(x,y+1) - I_{\text{L}}(x,y-1)]/[I_{\text{L}}(x+1,y) - I_{\text{L}}(x-1,y)]\} \\ g(x,y) = \sqrt{[I_{\text{L}}(x+1,y) - I_{\text{L}}(x-1,y)]^2 + [I_{\text{L}}(x,y+1) - I_{\text{L}}(x,y-1)]^2} \end{cases}, \tag{4}$$

where $\theta(x, y)$ is the direction of the gradient and $g(x, y)$ is the gradient modulus value.

After obtaining the gradient direction and amplitude, the gradient direction of the keypoints can be determined by a gradient direction histogram. The maximum/peak value of the histogram represents the direction of gradient at the neighbor of this keypoint. The peak value of histogram is set as the main direction of this keypoint, and when there is another peak with the value of the main peak's 80%, this direction is expected to be recorded as the auxiliary direction of this keypoint to improve the robustness. The direction matching has been completed with the location, orientation, and scale.

2.4. Keypoint Description

The keypoint description is to find the local image descriptor of the keypoints. Lowe [20] chose the gradient direction histograms to describe the keypoints. The specific procedures of keypoint description can be concluded with three steps:

Step 1 The scale and orientation are computed in the 16 × 16 neighbor of keypoints.

Step 2 The 16 × 16 neighborhood is divided into 4 × 4 blocks. Thus, there are 16 blocks in the neighbor of every keypoint as well as eight orientations in the central point of every 4 × 4 block.

Step 3 128 orientations can be obtained as the keypoint feature in the vector with size of 1 × 128. To simplify the analysis, suppose the 8 × 8 neighbor of the keypoint is divided into 4 × 4 blocks, and there will be four sub-blocks. The diagram of keypoints directions are shown in Figure 1.

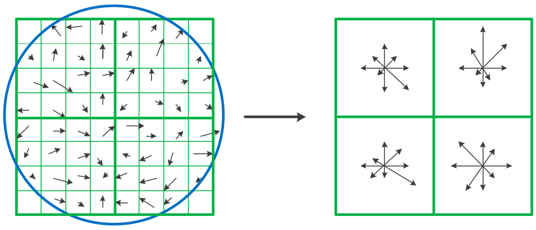


Figure 1. Directions of the keypoints.

So far, all of the steps of the SIFT algorithm are completed. In this paper, SIFT is applied to correct the RST attacks to obtain better robustness of the watermarked image.

3. The Proposed Scheme

3.1. Watermark Embedding Process

The flow diagram of the watermark embedding process is shown in Figure 2.

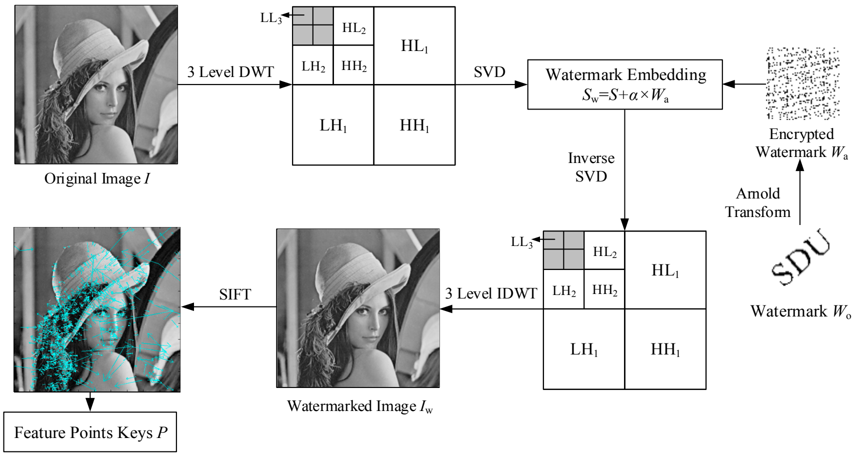


Figure 2. Flow diagram of the watermark embedding process.

The concrete steps are described as follows:

Step 1 The original image I is transformed with DWT three times, and each level of DWT is performed sequentially on the original image, LL_1, and LL_2. Finally, LL_3 is obtained for the SVD transform in Step 3. Due to the fact that the LL sub-band has sufficient information, the capacity of watermark embedding is large in the LL sub-band, which can ensure the good imperceptibility of the proposed method.

Step 2 The watermark information is encrypted with the Arnold transform, and the scrambling time is saved as key T.

Step 3 According to Equations (5) and (6), SVD is performed on the LL_3 sub-band to get three matrices: both U and V are orthogonal matrices, and S is the diagonal matrix of singular values. After that, singular values of the LL_3 sub-band are altered:

$$I_{\mathrm{LL}_3} = USV^{\mathrm{T}}, \tag{5}$$

$$S_{\mathrm{w}} = S + \alpha \times W_{\mathrm{a}}, \tag{6}$$

where α is the scaling factor, determining the performance of the watermarking scheme in robustness and imperceptibility, and W_{a} is the watermark encrypted with Arnold transform.

Step 4 Owing to the fact that the watermark for embedding is an image matrix, S_{w} is not a diagonal matrix after Equation (6), which can result in distortion in inverse SVD transform. Thus, SVD is performed on the S_{w} again to obtain the watermarked diagonal matrix, which is illustrated by:

$$S_{\mathrm{w}} = U_{\mathrm{w}} S_{\mathrm{ww}} {V_{\mathrm{w}}}^{\mathrm{T}}. \tag{7}$$

Step 5 The watermarked sub-band $I_{\mathrm{LL}_{3\mathrm{w}}}$ is generated by S_{ww}, U, and V, as shown in Equation (8):

$$I_{\mathrm{LL}_{3\mathrm{w}}} = US_{\mathrm{ww}}V^{\mathrm{T}}. \tag{8}$$

Step 6 According to the concrete process in Step 1, three-level inverse DWT (IDWT) is performed with other sub-bands to generate the watermarked image I_{w}.

Step 7 After Step 6, SIFT is performed on the watermarked image I_{w}, and feature points are extracted. Meanwhile, descriptors of the watermarked image are recorded as keys P for the feature matching in the extraction process. To be more concrete, the coordinates, scales, and orientations of the feature points in the watermarked image are obtained, which are used for RST attack correction.

In the end, the watermark embedding process is finished.

3.2. Watermark Extraction Process

The extraction process can be implemented without the original image but feature keys, which can be regarded as the semi-blind watermark scheme. The flow diagram of the watermark extraction process is shown in Figure 3.

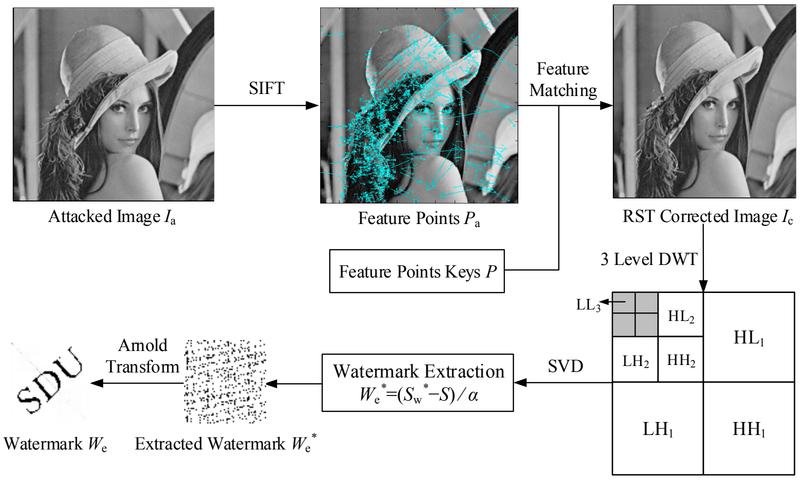


Figure 3. Flow diagram of the watermark extraction process.

The concrete steps are demonstrated as follows:

Step 1 The attacked image I_a is performed with SIFT, and the feature points P_a in the attacked image can be obtained accordingly.

Step 2 In the embedding process, the feature points in watermarked image are recorded as keys P. In this step, keys P should be stored in a matrix and transmitted along with the watermarked image for feature matching with the feature points P_a.

As can be seen in Figure 4, two sets of feature points in two images are selected as matching keypoints, and lines are drawn between two keypoints in two images separately.

Step 3 After the feature matching process finished, RST attacks can be corrected with the angle, coordinates, and scales, which is illustrated concretely in Section 3.3. Then, the RST corrected image I_c is obtained for watermark extraction.

Step 4 Three-level DWT is performed on the corrected image I_c, and then LL_3, LH_3, HL_3, and HH_3 bands are obtained. Similar to the embedding process, the LL_3 sub-band $I^*_{\mathrm{LL}_{3\mathrm{w}}}$ is selected for the SVD transform in the next step.

Step 5 SVD is performed on the corrected sub-band using Equation (9), and $S_{\mathrm{ww}}{}^*$ is recorded for the next step.

$$I^*_{\mathrm{LL}_{3\mathrm{w}}} = U^* S_{\mathrm{ww}}{}^* V^{*\mathrm{T}}. \tag{9}$$

Step 6 S^*_w is retrieved back by Equation (10):

$$S^*_\mathrm{w} = U_\mathrm{w} S^*_{\mathrm{ww}} V_\mathrm{w}{}^\mathrm{T}. \tag{10}$$

Step 7 The extracted watermark is generated for the LL_3 sub-band, which is shown in Equation (11):

$$W^*_\mathrm{e} = (S^*_\mathrm{w} - S)/\alpha. \tag{11}$$

Step 8 The extracted watermark is decrypted by the Arnold transform with key T recorded in the embedding process.

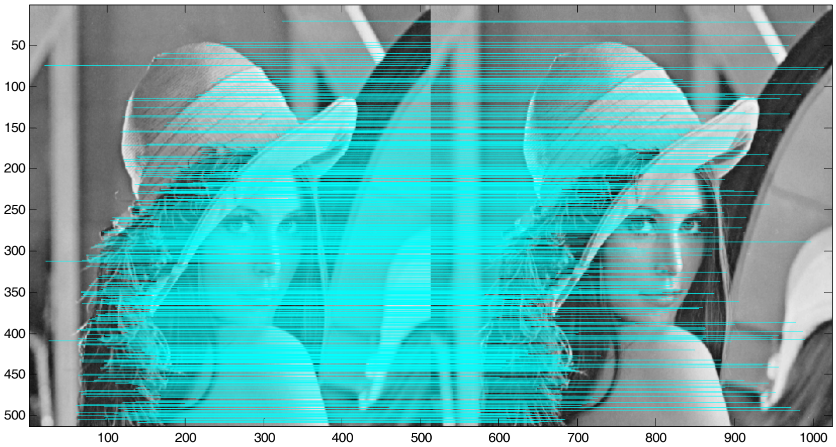


Figure 4. Scale-invariant feature transform (SIFT) feature matching.

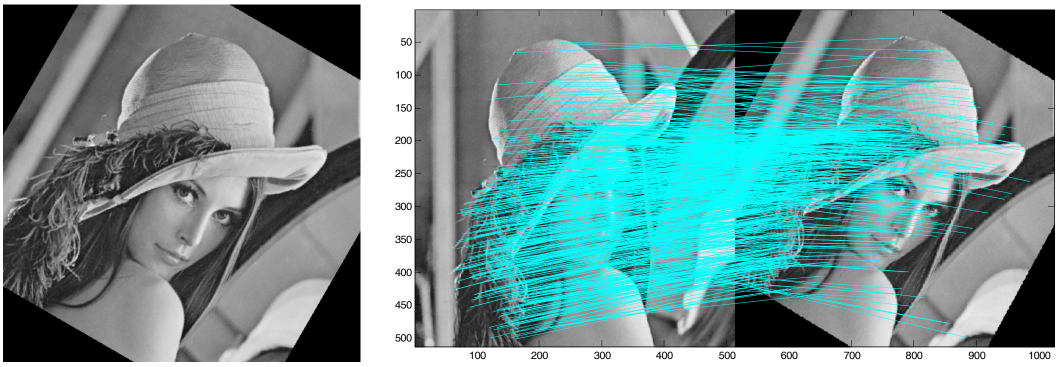
So far, the watermark extraction process is finished.

3.3. RST Attack Correction Based on SIFT

As demonstrated in Sections 3.1 and 3.2, after that, the SIFT feature of the image is extracted, and horizontal coordinates, vertical coordinates, scales, orientation factors, as well as the descriptors of keypoints can be obtained. Descriptors key of feature keypoints P saved in the embedding process and descriptors key of feature points P_{a} are matched, and M pairs of matching points can be obtained for the following correction.

3.3.1. Rotation Attack Correction

The image is rotated by a certain degree, resulting in information destruction and loss. The match between rotated image and watermarked image is shown in Figure 5.



(**a**) (**b**)

Figure 5. Matching between rotated image and watermarked image: (**a**) rotated image (30°); (**b**) feature matching.

The two keypoints of watermarked image are set as i_{w} and j_{w} separately, and two keypoints of rotated image are set as i_{r} and j_{r}. According to the basic mathematics, the vector can be obtained by the calculation on coordinates between two points. Thus, the vector in the watermarked image and rotated image can be set as $\overrightarrow{i_{\mathrm{w}} j_{\mathrm{w}}}$ and $\overrightarrow{i_{\mathrm{r}} j_{\mathrm{r}}}$, respectively. For the correction, the rotation angle of the kth matching point is recorded as ϕ_k. So far, the corrected angle of rotation can be given in Equation (12):

$$\beta_{\mathrm{c}} = \frac{1}{m}\sum_{k=1}^{m} \phi_k,\ \phi_k = \arccos\left(\frac{\overrightarrow{i_{\mathrm{w}} j_{\mathrm{w}}} \cdot \overrightarrow{i_{\mathrm{r}} j_{\mathrm{r}}}}{\left|\overrightarrow{i_{\mathrm{w}} j_{\mathrm{w}}}\right|\left|\overrightarrow{i_{\mathrm{r}} j_{\mathrm{r}}}\right|}\right), \tag{12}$$

where m is the number of valid matching points. Equation (12) means that any two pairs of matching points are picked out to calculate the rotation angle, and then the average value of the angles' sum is calculated. In this context, the corrected angle β_{c} is obtained. Thus, the attacked image at the receiving end should be rotated by the angle of β_{c} for the rotation correction.

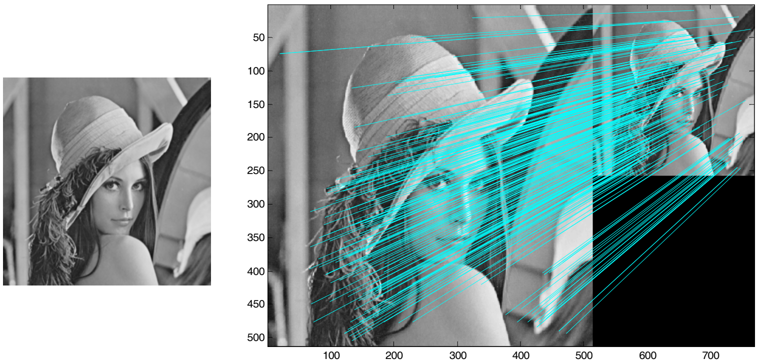
3.3.2. Scaling Attack Correction

Scaling attack is a type of tampering method that can change the size of one image, which can result in the image distortion. The match between scaled image and watermarked image is shown in Figure 6.

Owing to the SIFT characteristics, the scaling coefficient is equal to the size relationship between scaled image and watermarked image. Thus, the scaling coefficient can be extracted from M pairs of matching points. s_{w_k} and s_{s_k} are the kth scale values of the matching points in watermarked image and scaled image, respectively. The corrected scaling coefficient γ is shown as Equation (13):

$$\gamma = \frac{1}{M}\sum_{k=1}^{M} \frac{s_{\mathrm{w}_k}}{s_{\mathrm{s}_k}}. \tag{13}$$

Apparently, γ is the mean of ratios between s_{w_k} and s_{s_k}. After obtaining the corrected scaling coefficient, the received image should be scaled with the parameter γ to achieve the rotation complementary.

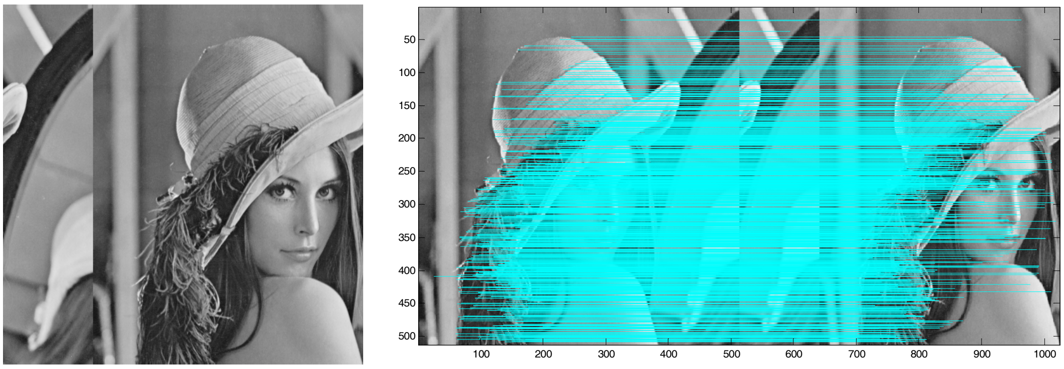


(**a**) (**b**)

Figure 6. Matching between scaled image and watermarked image: (**a**) scaled image (0.5); (**b**) feature matching.

3.3.3. Translation Attack Correction

The definition of the translation attack is that all points of one image are moved towards the same linear direction for the same distance. The translation attack cannot change the shape and size of the attacked image, but result in image information destruction. The match between horizontally translated image (128 pixels) and watermarked image is shown in Figure 7.



(**a**) (**b**)

Figure 7. Matching between translated image and watermarked image: (**a**) horizontally translated image (128 pixels); (**b**) feature matching.

Translation correction is implemented with the help of matching points' coordinates. Similar to scaling attack correction, coordinates of the watermarked image and translated image are set as $(x_{\mathrm{w}}, y_{\mathrm{w}})$ and $(x_{\mathrm{t}}, y_{\mathrm{t}})$, and the size of the image is $N \times N$. The corrected horizontal and vertical coordinates, x_{c} and y_{c}, can be calculated by Equation (14):

$$x_{\mathrm{c}} = \begin{cases} x_{\mathrm{t}} - x_{\mathrm{w}} + N, & x_{\mathrm{t}} < x_{\mathrm{w}} \\ x_{\mathrm{t}} - x_{\mathrm{w}}, & \text{otherwise} \end{cases}, \; y_{\mathrm{c}} = \begin{cases} y_{\mathrm{t}} - y_{\mathrm{w}} + N, & y_{\mathrm{t}} < y_{\mathrm{w}} \\ y_{\mathrm{t}} - y_{\mathrm{w}}, & \text{otherwise} \end{cases}. \tag{14}$$

After that, x_{c} and y_{c} are used to correct the attacked image on the horizontal and vertical location of coordinates in the inverse direction to achieve the translation correction.

The corrections of RST attacks are demonstrated, respectively, as above all.

4. Experimental Results and Analysis

In this section, performances in watermark robustness and imperceptibility of the proposed method are given and analyzed. This scheme is tested on the image with size of 512 × 512, and the watermark applied in this scheme is a binary image with size of 64 × 64. The scheme is tested on MATLAB R2014a with an Intel (R) Core (TM), Santa Clara, TX, USA, i3-2100 3.10 GHz CPU, 6 GB memory computer.

The proposed scheme is performed on a number of standard images, which are shown in Figure 8.

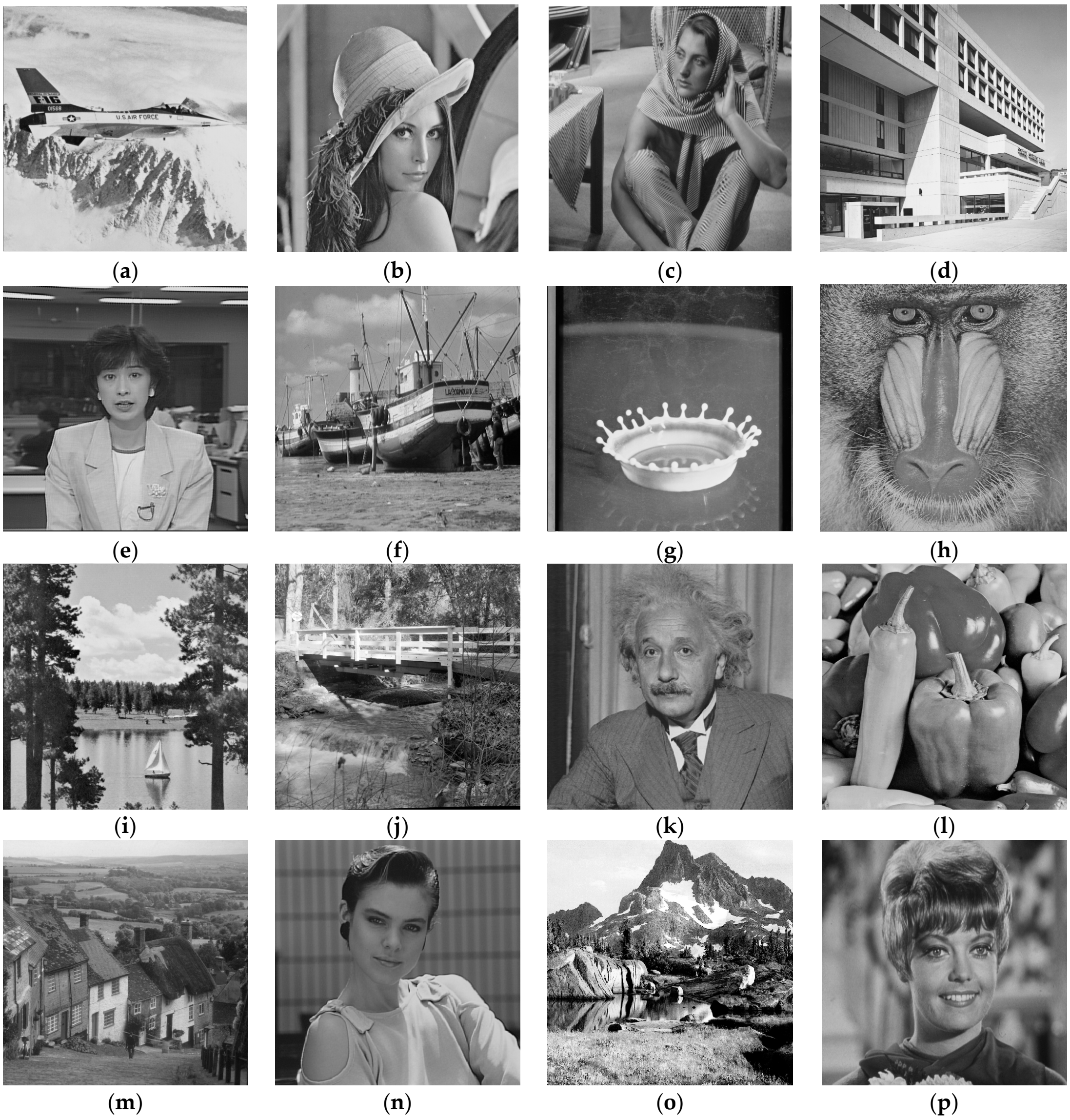


Figure 8. Test images: (**a**) Airplane; (**b**) Lena; (**c**) Barbara; (**d**) Bank; (**e**) Announcer; (**f**) Fishing Boat; (**g**) Milkdrop; (**h**) Baboon; (**i**) Boat; (**j**) Bridge; (**k**) Einstein; (**l**) Peppers; (**m**) Goldhill; (**n**) Model; (**o**) Mountain; (**p**) Zelda.

The Lena and Barbara images are selected for representative in this scheme. Compared with the Lena image, the Barbara image has more texture information. Similarly, considering symmetry and asymmetry of watermarks, the English character and logo images of Shandong University, China, set as w_1 and w_2, are applied in this scheme for representation. In addition, the character watermark is embedded into the host image Lena, and the logo image watermark is embedded into the host image Barbara.

4.1. Evaluation of Imperceptibility

After the watermark embedding, compared with the original image, the quality of the watermarked image will be reduced. Peak signal-to-noise ratio (PSNR) is the quality evaluation index adopted in most watermarking schemes to evaluate the imperceptibility performance of the algorithm. As for an image with size of $N \times N$, the PSNR is defined as Equation (15):

$$\text{PSNR} = 10\lg\frac{255^2}{\text{MSE}} = 10\lg\left[\frac{255^2 N^2}{\sum\limits_{i=0}^{N-1}\sum\limits_{j=0}^{N-1}[I(i,j) - I_{\text{w}}(i,j)]^2}\right](\text{dB}), \tag{15}$$

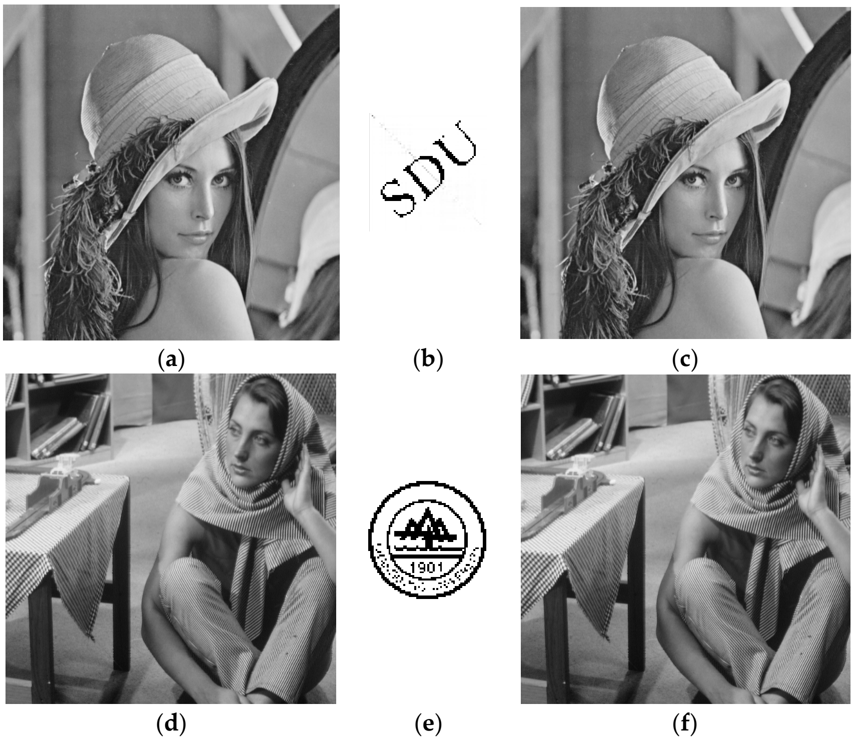
where $I(i,j)$ and $I_{\text{w}}(i,j)$ are the pixel values on the coordinates of row i and column j in the host image and the watermarked image separately.

Structural similarity index (SSIM) overcomes the disadvantage of PSNR, becoming a useful index of the similarity detection, which is defined as Equation (16):

$$\text{SSIM} = \frac{2\mu_I\mu_{I_\text{w}} + C_1}{\mu_I{}^2 + \mu_{I_\text{w}}{}^2 + C_1}\,\frac{2\sigma_I\sigma_{I_\text{w}} + C_2}{\sigma_I{}^2 + \sigma_{I_\text{w}}{}^2 + C_2}\,\frac{\sigma_{II_\text{w}} + C_3}{\sigma_I\sigma_{I_\text{w}} + C_3}, \tag{16}$$

where μ_I and μ_{I_w} denote the mean of original image I and watermarked or restored image I_w, respectively. Furthermore, σ_I and σ_{I_w} are the variance of image I and I_w separately, while σ_{II_w} is the covariance between I and I_w. C_1, C_2, and C_3 are positive parameters. The value of SSIM ranges from 0 to 1. When SSIM is equal to 1, I and I_w are exactly the same.

Figure 9 shows the good perceptual transparency of the watermarked image compared with the original image. After SIFT is performed on Lena and Barbara images, 1233 keypoints and 1590 keypoints are extracted in these two watermarked images, respectively.



(**a**) (**b**) (**c**)

(**d**) (**e**) (**f**)

Figure 9. Imperceptibility of the watermark: (**a**) original Lena image; (**b**) original character watermark w_1; (**c**) watermarked Lena; (**d**) original Barbara image; (**e**) original logo watermark w_2; (**f**) watermarked Barbara.

4.2. Evaluation of Robustness

The normalized correlation (NC) is applied to calculate the similarity of two images and further evaluate the robustness of the watermarking scheme, which is defined as Equation (17):

$$NC = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} W_o(i,j) \times W_e(i,j)}{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} W_o(i,j) \times W_o(i,j)}, \tag{17}$$

where W_o is the original watermark and W_e is the extracted watermark. The size of the watermark is $n \times n$.

The watermark is embedded into host images with different scaling factors, as shown in Figure 10. To resolve the trade-off between the robustness and invisibility of watermarking, the scaling factor is set as 0.5.

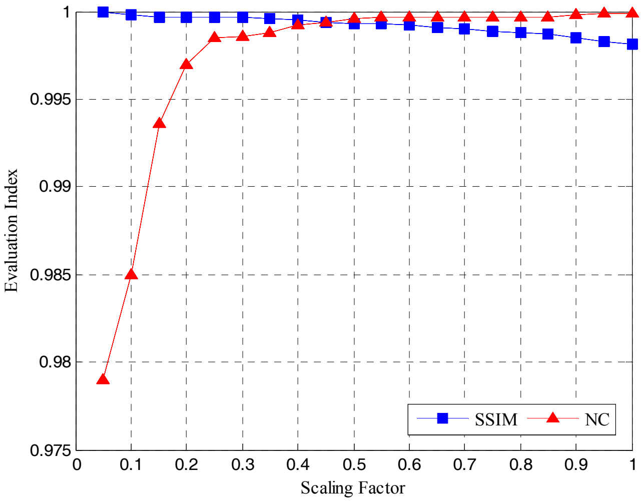


Figure 10. Structural similarity index (SSIM) and normalized correlation (NC) values of the proposed method with different quantization steps.

Table 1 gives the results of test images in number of keypoints and NC value (host images are tested with watermark 1).

Table 1. Experimental results on test images.

Images	Number of Keypoints	NC
Airplane	2037	0.9970
Lena	1233	0.9964
Barbara	1590	0.9969
Bank	948	0.9973
Announcer	973	0.9975
Fishing Boat	1943	0.9978
Milkdrop	272	0.9972
Baboon	3264	0.9976
Boat	2881	0.9971
Bridge	3813	0.9974
Einstein	812	0.9977
Peppers	780	0.9967
Goldhill	1947	0.9973
Model	593	0.9965
Mountain	2442	0.9964
Zelda	880	0.9969

4.2.1. Common Attacks

In Figures 11–15, the extracting results under different image attacks are given, such as JPEG 100, salt and pepper noise with densities of 0.01 and 0.05, Gaussian noise with mean 0, and variances of 0.01 and 0.05, center cropping on the 256 × 256 region, and median filter (3 × 3).

(1) JPEG (100).

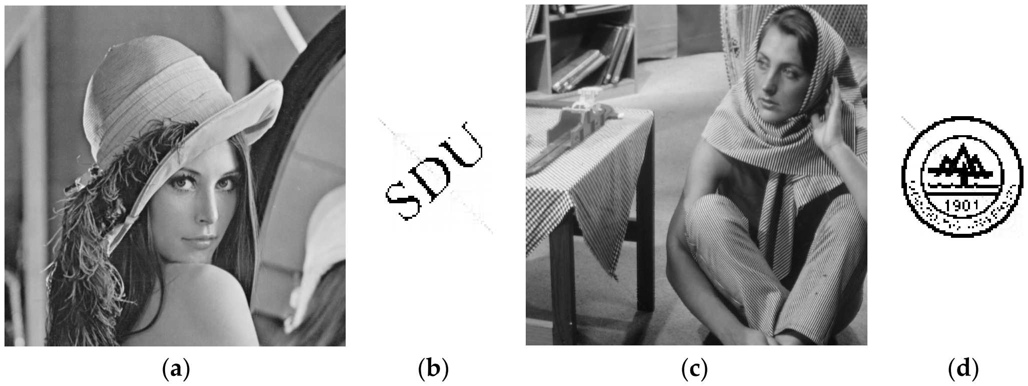


Figure 11. Watermarked images and extracted watermarks under JPEG (100): (**a**) watermarked Lena; (**b**) extracted watermark w_1; (**c**) watermarked Barbara; (**d**) extracted watermark w_2.

(2) Salt and pepper noise (0.01 and 0.05).

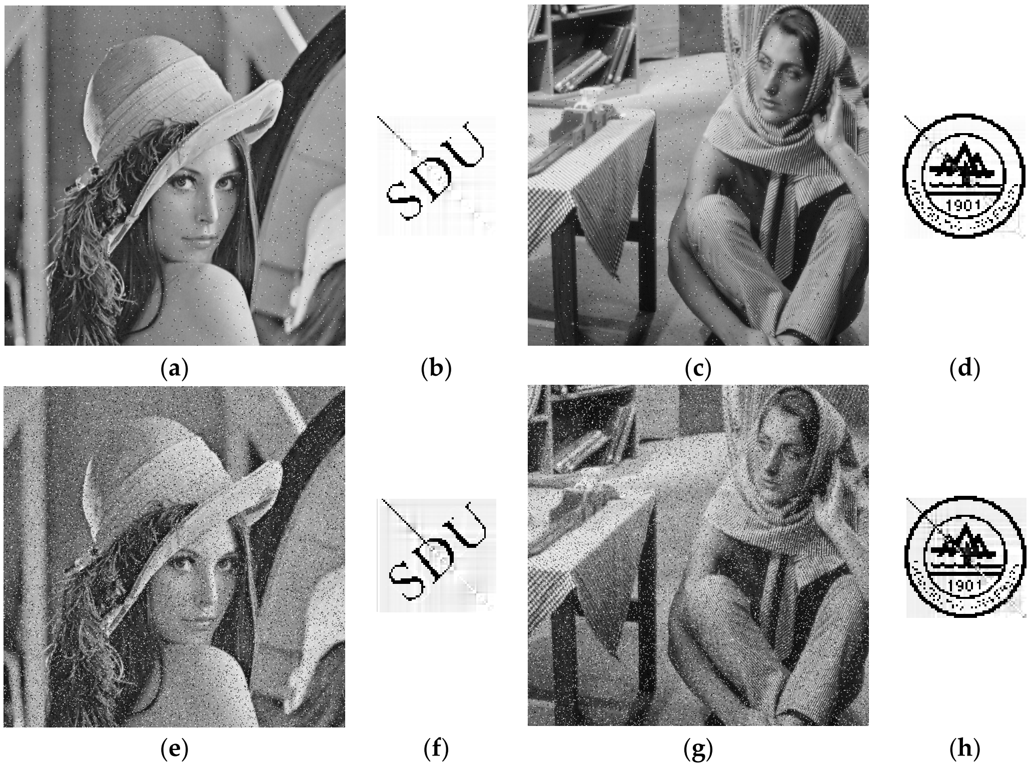


Figure 12. Watermarked images and extracted watermarks under salt and pepper noise: (**a**) watermarked Lena under salt and pepper noise (0.01); (**b**) extracted watermark w_1; (**c**) watermarked Barbara under salt and pepper noise (0.01); (**d**) extracted watermark w_2; (**e**) watermarked Lena under salt and pepper noise (0.05); (**f**) extracted watermark w_1; (**g**) watermarked Barbara under salt and pepper noise (0.05); (**h**) extracted watermark w_2.

(3) Gaussian noise ((0, 0.01) and (0, 0.05)).

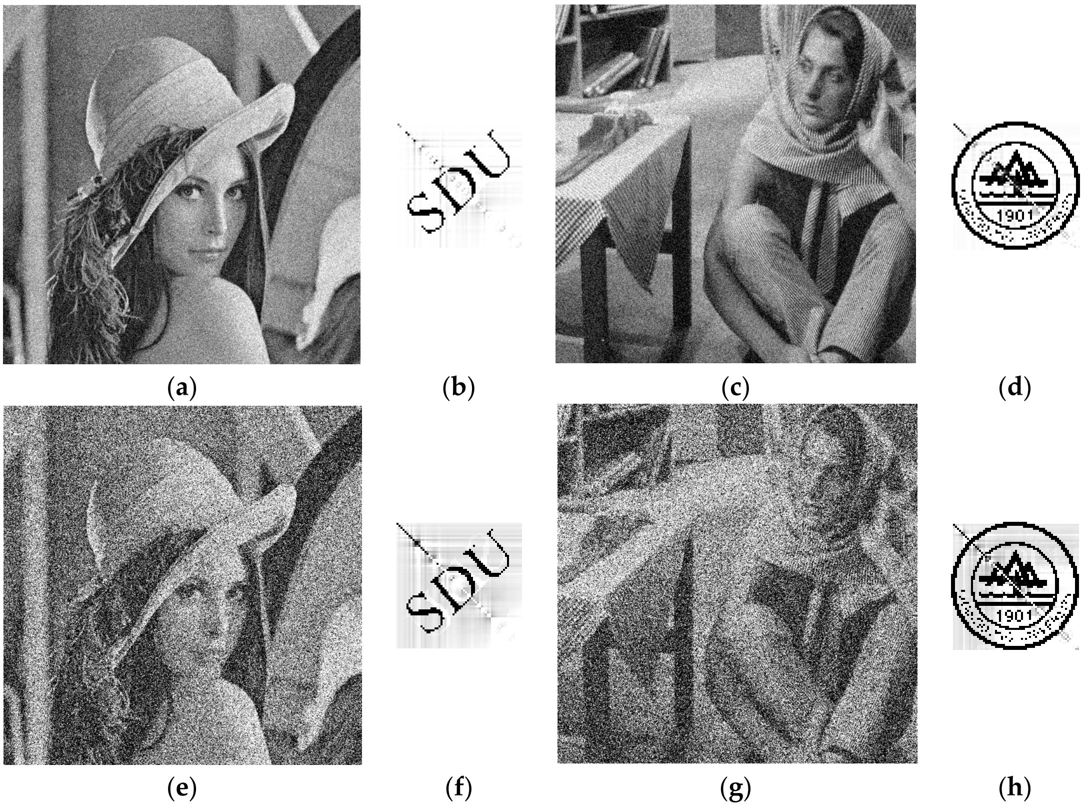


Figure 13. Watermarked images and extracted watermarks under Gaussian noise: (**a**) watermarked Lena under Gaussian noise (0, 0.01); (**b**) extracted watermark w_1; (**c**) watermarked Barbara under Gaussian noise (0, 0.01); (**d**) extracted watermark w_2; (**e**) watermarked Lena under Gaussian noise (0, 0.05); (**f**) extracted watermark w_1; (**g**) watermarked Barbara under Gaussian noise (0, 0.05); (**h**) extracted watermark w_2.

(4) Center cropping (25%).

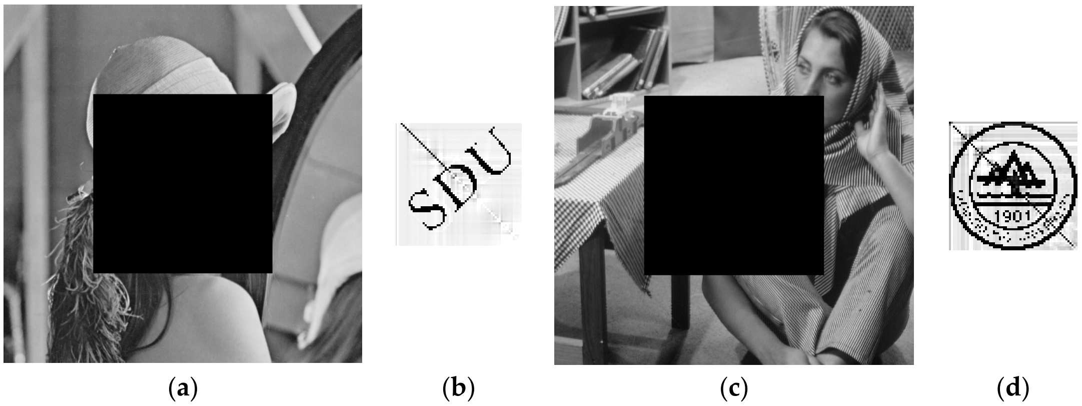
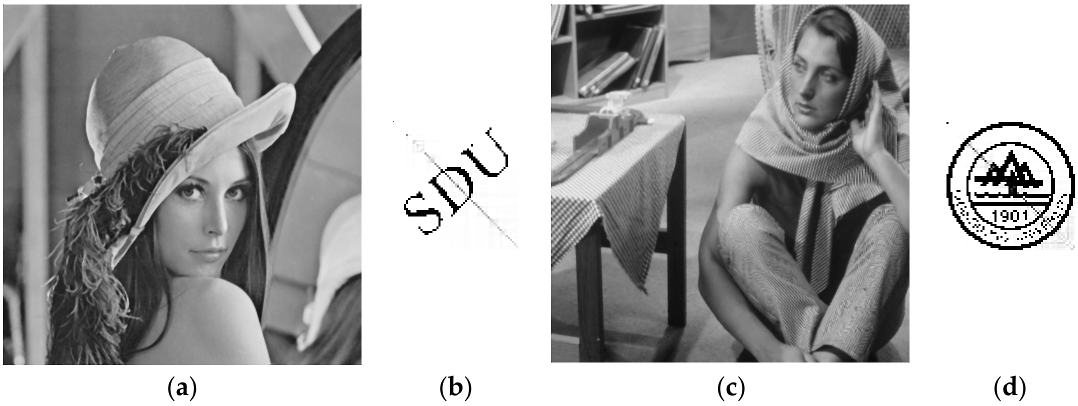


Figure 14. Watermarked images and extracted watermarks under center cropping (25%): (**a**) watermarked Lena; (**b**) extracted watermark w_1; (**c**) watermarked Barbara; (**d**) extracted watermark w_2.

(5) Median filter (3 × 3).



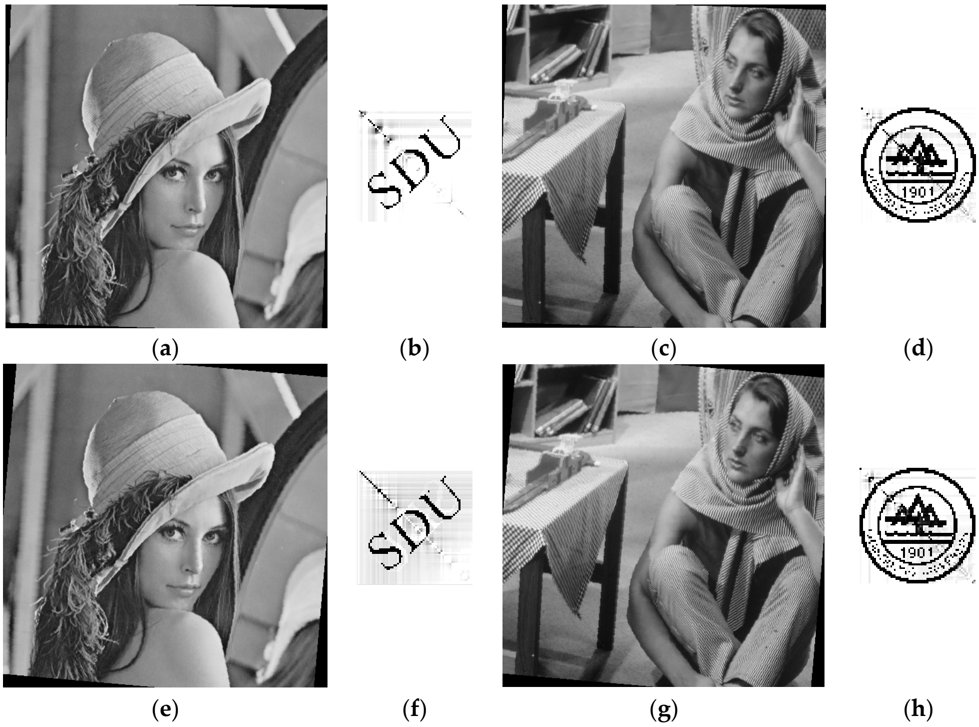
(**a**) (**b**) (**c**) (**d**)

Figure 15. Watermarked images and extracted watermarks under median filter (3 × 3): (**a**) watermarked Lena; (**b**) extracted watermark w_1; (**c**) watermarked Barbara; (**d**) extracted watermark w_2.

4.2.2. RST Attacks

In Figures 16–18, watermarked images and extracted watermarks of the proposed scheme are shown under RST attacks with different parameters. For rotation, there are five cases of parameters simulated in the scheme, which contain 2°, 5°, 10°, 30°, and 45°. In the scaling attacks, four different scales are performed to change the size of watermarked images, i.e., 0.25, 0.5, 0.9, and 1.2. In the perspective of translation attacks, the translation of watermarked image is performed in horizontal and vertical directions for 128 pixels, respectively.

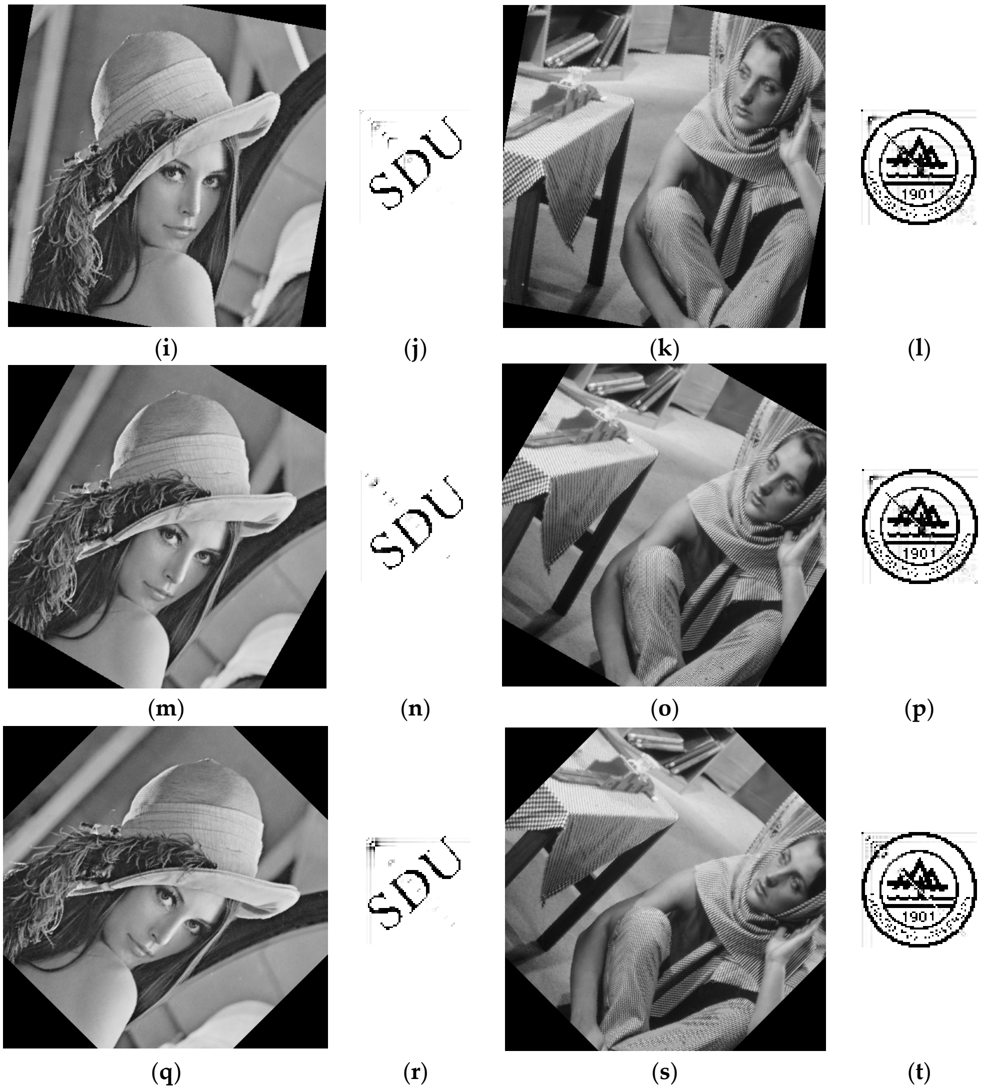
(1) Rotation.



(**a**) (**b**) (**c**) (**d**)

(**e**) (**f**) (**g**) (**h**)

Figure 16. *Cont.*



(**i**) (**j**) (**k**) (**l**)

(**m**) (**n**) (**o**) (**p**)

(**q**) (**r**) (**s**) (**t**)

Figure 16. Watermarked images and extracted watermarks under rotation: (**a**) rotated Lena (2°); (**b**) extracted watermark w_1; (**c**) rotated Barbara (2°); (**d**) extracted watermark w_2; (**e**) rotated Lena (5°); (**f**) extracted watermark w_1; (**g**) rotated Barbara (5°); (**h**) extracted watermark w_2; (**i**) rotated Lena (10°); (**j**) extracted watermark w_1; (**k**) rotated Barbara (10°); (**l**) extracted watermark w_2; (**m**) rotated Lena (30°); (**n**) extracted watermark w_1; (**o**) rotated Barbara (30°); (**p**) extracted watermark w_2; (**q**) rotated Lena (45°); (**r**) extracted watermark w_1; (**s**) rotated Barbara (45°); (**t**) extracted watermark w_2.

(2) Scaling.

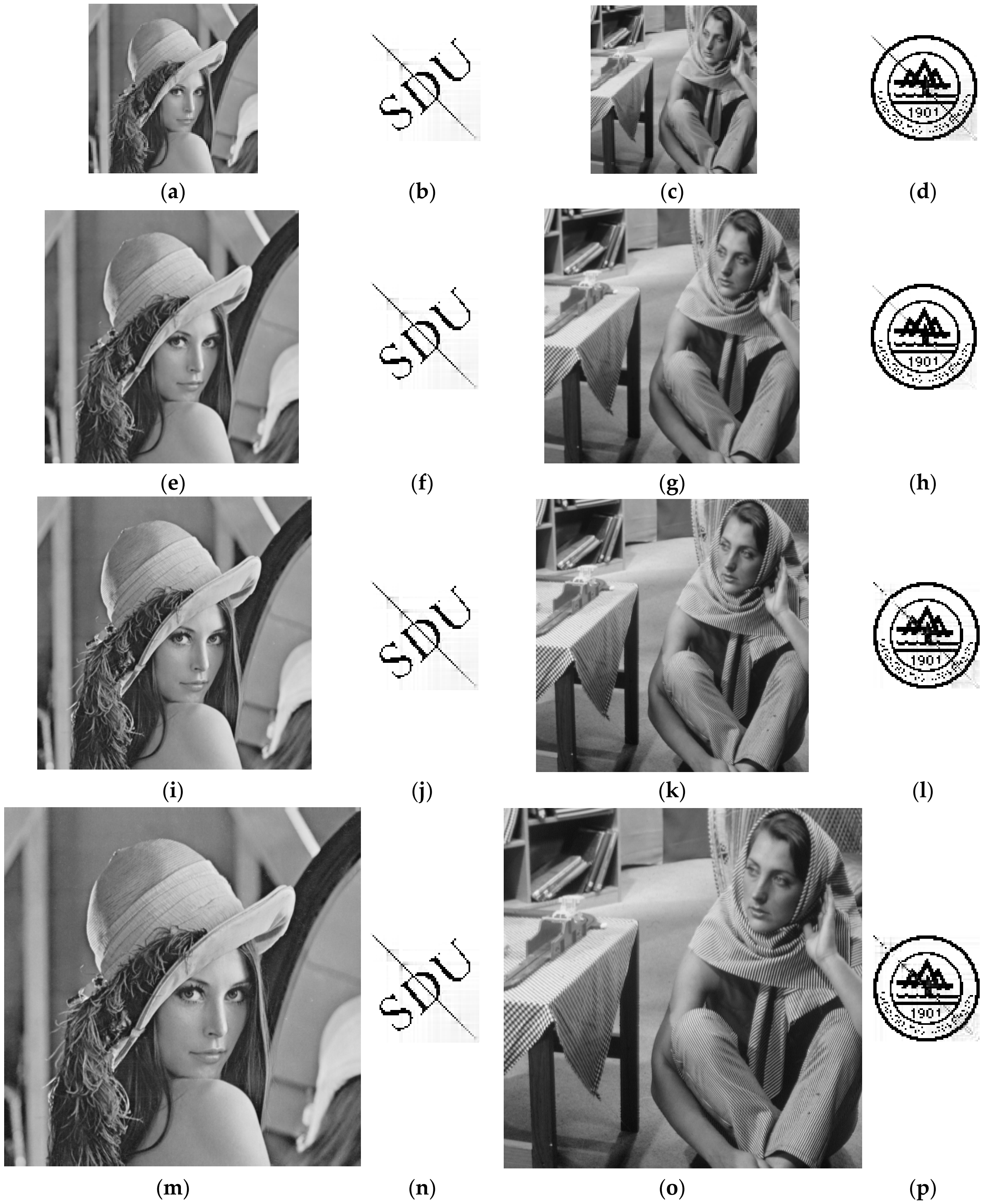


Figure 17. Watermarked images and extracted watermarks under scaling attacks: (**a**) scaled Lena (0.25); (**b**) extracted watermark w_1; (**c**) scaled Barbara (0.25); (**d**) extracted watermark w_2; (**e**) scaled Lena (0.5); (**f**) extracted watermark w_1; (**g**) scaled Barbara (0.5); (**h**) extracted watermark w_2; (**i**) scaled Lena (0.9); (**j**) extracted watermark w_1; (**k**) scaled Barbara (0.9); (**l**) extracted watermark w_2; (**m**) scaled Lena (1.2); (**n**) extracted watermark w_1; (**o**) scaled Barbara (1.2); (**p**) extracted watermark w_2.

(3) Translation.

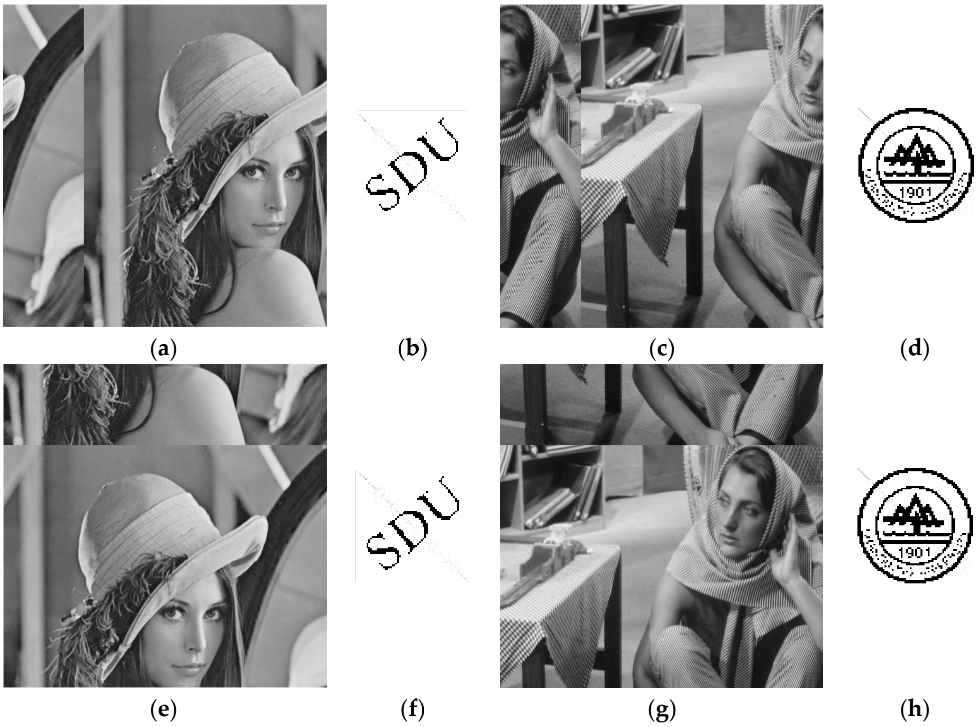


Figure 18. Watermarked images and extracted watermarks under translation attacks: (**a**) horizontally translated Lena (128 pixels); (**b**) extracted watermark w_1; (**c**) horizontally translated Barbara (128 pixels); (**d**) extracted watermark w_2; (**e**) vertically translated Lena (128 pixels); (**f**) extracted watermark w_1; (**g**) vertically translated Barbara (128 pixels); (**h**) extracted watermark w_2.

Table 2 gives the robustness performance of the proposed scheme on two sets of host images and watermarks. Lena image and character watermark are given in the first column, and Barbara image and logo watermark are given in the second column. The PSNR value of the proposed method is 54.6 dB, which expresses good imperceptibility of the watermarked image.

Table 2. Robustness performance of the proposed scheme.

Different Attacks	Lena and w_1	Barbara and w_2
Scaling (0.25)	0.9744	0.9713
Scaling (0.5)	0.9919	0.9910
Scaling (0.9)	0.9931	0.9731
Scaling (1.2)	0.9906	0.9726
Rotation (2°)	0.9741	0.9703
Rotation (5°)	0.9813	0.9659
Rotation (10°)	0.9861	0.9738
Rotation (30°)	0.9861	0.9822
Rotation (45°)	0.9828	0.9839
Horizontal cycling translation (128 pixels)	0.9964	0.9962
Vertical cycling translation (128 pixels)	0.9964	0.9962
JPEG (100)	0.9966	0.9964
Median filter (3 × 3)	0.9913	0.9848
Center cropping (25%)	0.9179	0.8859
Gaussian noise (0, 0.01)	0.9788	0.9799
Gaussian noise (0, 0.05)	0.9509	0.9206
Salt and pepper noise (0.01)	0.9758	0.9759
Salt and pepper noise (0.05)	0.9644	0.9476

To illustrate the robustness of the proposed algorithm against multiple attacks, Table 3 is given for robustness performance, which suggests that the proposed scheme has a good ability for multiple attacks' resistance.

Table 3. Robustness performance on different combination of attacks.

Different Combination of Attacks	Lena and w_1	Barbara and w_2
Rotation (10°) and JPEG (100)	0.9964	0.9738
Rotation (10°) and Gaussian noise (0, 0.05)	0.9644	0.9437
Rotation (10°) and Salt and pepper noise (0.05)	0.9779	0.9592
Rotation (10°) and Center cropping (25%)	0.9098	0.9165
Rotation (10°) and Median filter (3 × 3)	0.9862	0.9729
Scaling (0.5) and JPEG (100)	0.9920	0.9616
Scaling (0.5) and Gaussian noise (0, 0.05)	0.9239	0.9165
Scaling (0.5) and Salt and pepper noise (0.05)	0.9331	0.9348
Scaling (0.5) and Center cropping (25%)	0.8170	0.8807
Scaling (0.5) and Median filter (3 × 3)	0.9861	0.9578
Horizontal translation and JPEG (100)	0.9966	0.9964
Horizontal translation and Gaussian noise (0, 0.05)	0.9068	0.9190
Horizontal translation and Salt and pepper noise (0.05)	0.9400	0.9455
Horizontal translation and Center cropping (25%)	0.8981	0.8724
Horizontal translation and Median filter (3 × 3)	0.9917	0.9846
Rotation (10°) and Scaling (0.5)	0.9857	0.9669
Scaling (0.5) and Horizontal translation	0.9912	0.9646
Horizontal translation and Rotation (10°)	0.9851	0.9677

4.3. Performance Comparison with Previous Schemes

To further evaluate the proposed scheme, our scheme is compared with two previous schemes [6,24]. Because there is similarity between precious schemes and proposed scheme in application of feature points and SVD separately. Table 4 compares the robustness against different attacks among Liu et al.'s scheme [6], Lyu et al.'s scheme [24], and the proposed scheme. In Liu et al.'s scheme with PSNR = 42.5 dB, the typical SVD based watermarking method was introduced, and the watermark information was embedded into the singular value of the host image in a certain pixel size, which explored a novel idea and method for copyright protection. However, if the host image is cropped at the area of watermark embedding, this scheme cannot achieve the robustness performance. Lyu et al. extracted the feature points by SIFT, and embedded the watermark information into the circle DWT domain of SIFT feature area, where the PSNR value is up to 84.6 dB. Although this scheme has great features of rotation and scaling, the robustness performance degrades with the angle increase of the rotation attacks.

Table 4. Comparisons in watermark robustness aganist different attacks among Liu et al.'s scheme [6], Lyu et al.'s scheme [24], and the proposed scheme.

Different Attacks	Liu et al.'s Scheme [6]	Lyu et al.'s Scheme [24]	Proposed Scheme
Median filter (3 × 3)	0.5170	0.6450	0.9913
Center cropping (25%)	0.9822	0.9800	0.9179
JPEG (100)	0.9941	0.9820	0.9966
Rotation (2°)	0.9687	0.9400	0.9741
Rotation (5°)	0.9197	0.9310	0.9813
Rotation (10°)	0.7825	0.8860	0.9861
Scaling (0.9)	0.9710	0.9560	0.9931
Scaling (1.2)	0.8709	0.9820	0.9906

5. Conclusions

In this paper, an RST resilient watermark scheme is proposed to obtain better imperceptibility and robustness against RST attacks on the basis of DWT and SVD. In the proposed scheme, the binary watermark image is embedded into the singular values in the three-level DWT domain. With the help of the SIFT, RST attacks on the host image can be corrected to promote the robustness. Experimental results show that the proposed scheme is able to resist different attacks, including common image processing and malicious attacks. Notably, compared with the previous scheme, the proposed scheme achieves better imperceptibility and robustness against RST attacks. For future work, the novel watermarking scheme applied to color images should be researched.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (No. 61201371), the Research Award Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province, China (No. BS2013DX022), and the Natural Science Foundation of Shandong Province, China (No. ZR2015PF004).

Author Contributions: Yunpeng Zhang and Chengyou Wang conceived the algorithm and designed the experiments; Yunpeng Zhang performed the experiments; Chengyou Wang and Xiao Zhou analyzed the results; Yunpeng Zhang drafted the manuscript; and Xiao Zhou revised the manuscript. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dittmann, J.; Steinmetz, A.; Steinmetz, R. Content-based digital signature for motion pictures authentication and content-fragile watermarking. In Proceedings of the 6th IEEE International Conference on Multimedia Computing and Systems, Florence, Italy, 7–11 June 1999; pp. 209–213.
2. Lou, D.C.; Liu, J.L. Fault resilient and compression tolerant digital signature for image authentication. *IEEE Trans. Consum. Electron.* **2000**, *46*, 31–39.
3. Langelaar, G.C.; Setywan, I.; Lagendijk, R.L. Watermarking digital image and video data. *IEEE Signal Process. Mag.* **2000**, *17*, 20–46. [CrossRef]
4. Barni, M.; Bartolini, F.; Cappellini, V. A DCT-domain system for robust image watermarking. *Signal Process.* **1998**, *66*, 357–372. [CrossRef]
5. Qi, X.J.; Xin, X. A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. *J. Vis. Commun. Image Represent.* **2015**, *30*, 312–327. [CrossRef]
6. Liu, R.Z.; Tan, T.N. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans. Multimedia* **2002**, *4*, 121–128.
7. Chang, C.C.; Tsai, P.; Lin, C.C. SVD-based digital image watermarking scheme. *Pattern Recognit. Lett.* **2005**, *26*, 1577–1586. [CrossRef]
8. Su, Q.T.; Niu, Y.G.; Zou, H.L.; Liu, X.X. A blind dual color images watermarking based on singular value decomposition. *Appl. Math. Comput.* **2013**, *219*, 8455–8466. [CrossRef]
9. Liu, F.; Feng, H.; Lu, C. Blind watermarking scheme based on U matrix through QSVD transformation. *Int. J. Secur. Appl.* **2015**, *9*, 203–216. [CrossRef]
10. Li, Z.; Yap, K.H.; Lei, B.Y. A new blind robust image watermarking scheme in SVD-DCT composite domain. In Proceedings of the 18th IEEE International Conference on Image Processing, Brussels, Belgium, 11–14 September 2011; pp. 2757–2760.
11. Sverdlov, A.; Dexter, S.; Eskicioglu, A.M. Robust DCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies. In Proceedings of the 13th European Signal Processing Conference, Antalya, Turkey, 4–8 September 2005; pp. 29–32.
12. Lai, C.C.; Tsai, C.C. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans. Instrum. Meas.* **2010**, *59*, 3060–3063. [CrossRef]
13. Bhatnagar, G.; Raman, B. A new robust reference watermarking scheme based on DWT-SVD. *Comput. Stand. Interfaces* **2009**, *31*, 1002–1013. [CrossRef]
14. Mishra, A.; Agarwal, C.; Sharma, A.; Bedi, P. Optimized gray-scale image watermarking using DWT-SVD and Firefly algorithm. *Expert Syst. Appl.* **2014**, *41*, 7858–7867. [CrossRef]
15. Narula, N.; Sethi, D.; Bhattacharya, P.P. Comparative analysis of DWT and DWT-SVD watermarking techniques in RGB images. *Int. J. Signal Process. Image Process. Pattern Recognit.* **2015**, *8*, 339–348. [CrossRef]
16. Singh, D.; Singh, S.K. DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimed. Tools Appl.* **2016**. [CrossRef]

17. Ansari, I.A.; Pant, M.; Ahn, C.W. Robust and false positive free watermarking in IWT domain using SVD and ABC. *Eng. Appl. Artif. Intell.* **2016**, *49*, 114–125. [CrossRef]
18. Zheng, D.; Zhao, J.Y.; Saddik, A.E. RST-invariant digital image watermarking based on log-polar mapping and phase correlation. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 753–765. [CrossRef]
19. Ye, X.Y.; Chen, X.T.; Deng, M.; Wang, Y.L. A SIFT-based DWT-SVD blind watermark method against geometrical attacks. In Proceedings of the 7th International Congress on Image and Signal Processing, Dalian, China, 14–16 October 2014; pp. 323–329.
20. Lowe, D.G. Object recognition from local scale-invariant features. In Proceedings of the 7th IEEE International Conference on Computer Vision, Kerkyra, Greece, 20–27 September 1999; pp. 1150–1157.
21. Mikolajczyk, K.; Schmid, C. A performance evaluation of local descriptors. *IEEE Trans. Pattern Anal. Mach. Intell.* **2005**, *27*, 1615–1630. [CrossRef] [PubMed]
22. Lee, H.K.; Kim, H.; Lee, H.Y. Robust image watermarking using local invariant features. *Opt. Eng.* **2006**, *45*, 535–545.
23. Luo, H.J.; Sun, X.M.; Yang, H.F.; Xia, Z.H. A robust image watermarking based on image restoration using SIFT. *Radio Eng.* **2011**, *20*, 525–532.
24. Lyu, W.L.; Chang, C.C.; Nguyen, T.S.; Lin, C.C. Image watermarking scheme based on scale-invariant feature transform. *KSII Trans. Internet Inf. Syst.* **2014**, *8*, 3591–3606.
25. Thorat, C.G.; Jadhav, B.D. A blind digital watermark technique for color image based on integer wavelet transform and SIFT. *Procedia Comput. Sci.* **2010**, *2*, 236–241. [CrossRef]
26. Pham, V.Q.; Miyaki, T.; Yamasaki, T.; Aizawa, K. Geometrically invariant object-based watermarking using SIFT feature. In Proceedings of the 14th IEEE International Conference on Image Processing, San Antonio, TX, USA, 16–19 September 2007; pp. 473–476.
27. Zhang, L.; Tang, B. A combination of feature-points-based and SVD-based image watermarking algorithm. In Proceedings of the International Conference on Industrial Control and Electronics Engineering, Xi'an, China, 23–25 August 2012; pp. 1092–1095.
28. Yuan, X.C.; Pun, C.M. Feature extraction and local Zernike moments based geometric invariant watermarking. *Multimed. Tools Appl.* **2014**, *72*, 777–799. [CrossRef]
29. Wang, C.P.; Wang, X.Y.; Xia, Z.Q. Geometrically invariant image watermarking based on fast radial harmonic Fourier moments. *Signal Process. Image Commun.* **2016**, *45*, 10–23.
30. Tsougenis, E.D.; Papakostas, G.A.; Koulouriotis, D.E.; Tourassis, V.D. Performance evaluation of moment-based watermarking methods: A review. *J. Syst. Softw.* **2012**, *85*, 1864–1884. [CrossRef]
31. Koenderink, J.J. The structure of image. *Biol. Cybern.* **1984**, *50*, 363–370. [CrossRef] [PubMed]
32. Babaud, J.; Witkin, A.P.; Baudin, M.; Duda, R.O. Uniqueness of the Gaussian kernel for scale-space filtering. *IEEE Trans. Pattern Anal. Mach. Intell.* **1986**, *8*, 26–33. [CrossRef] [PubMed]