International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.191-206
http://dx.doi.org/10.14257/ijsia.2016.10.10.18

Image Watermarking Scheme Based on DWT-DCT and SSVD

Zhi Zhang, Chengyou Wang* and Xiao Zhou

School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai 264209, China
sduzhi@163.com, wangchengyou@sdu.edu.cn, zhouxiao@sdu.edu.cn

Abstract

With the fast development of network, it becomes urgent to protect copyright and rightful ownership of an image, and digital watermark technology is a comprising solution to do that. However, the false positive problem exists in a number of watermarking schemes based on singular value decomposition (SVD). This paper offers a novel image watermark scheme to avoid the false positive problem, which combines with discrete cosine transform (DCT), discrete wavelet transform (DWT), and shuffled singular value decomposition (SSVD). In order to address the problem, the principal components obtained by SSVD are embedded into a constructed matrix composed of the direct current (DC) component which is extracted from the non-overlapping image block acquired by dividing the low frequency. The low frequency is obtained by applying DWT to the host image. Otherwise, the experiments concerning the imperceptibility and robustness are conducted in this paper. Compared with other reliable watermark methods, the obtained experimental results demonstrate that the proposed method has excellent imperceptibility and behaves satisfactory robustness in resisting the attacks such as Salt and Pepper noise, Gaussian noise, and image cropping, etc.

Keywords*: Digital Watermarking; Discrete Wavelet Transform (DWT); Discrete Cosine Transform (DCT); Shuffled Singular Value Decomposition (SSVD)*

1. Introduction

Due to the rapid evolution of network technology, it becomes much easier for folks to get digital information and kinds of resources. The Internet is greatly convenient to exchange information between individuals, but meanwhile, it leads to a multitude of security problems at the aspect of copyright disputes. Facing these issues, the digital watermarking technique is a promising solution for copyright protection, which is a technology of embedding watermark with intellectual property rights into carriers [1] such as image, audio, and video. The two importance properties of robust watermarking methods are imperceptibility and robustness. The imperceptibility refers that the watermark embedded in the cover image is hard to be perceived by naked eyes. The robustness is defined as the ability against a host of innocent and malicious attacks such as signal processing operations and geometric attacks.

Over the past several decades, a number of watermarking schemes have been proposed and implemented by many researchers since its release. An ocean of watermarking schemes is mainly divided into two types: (i) Spatial domain and (ii) Transform domain. It is worth mentioning that the least significant bit (LSB) [2] is one of the most representative methods in spatial domain, which embeds the watermark into the cover image by modifying the least significant bit. The transform domain includes discrete cosine transform (DCT) [3], discrete Fourier transform (DFT), and discrete wavelet transform (DWT), etc. In 2002, Liu and Tan [4] first proposed the singular value decomposition (SVD) based watermark scheme, which took full advantage of the stability of SVD. Owing to its stability, a sea of hybrid watermarking methods with regard to SVD

ISSN: 1738-9976 IJSIA

sprang up for a while, for example, a watermarking scheme based DCT-SVD [5], a watermarking algorithm based SVD-DWT [6], and a watermarking method based DWT-DCT-SVD [7, 8]. However, Zhang and Li [9] stated the critical defect of Liu and Tan's scheme, which is also called as false positive problem. Besides that, an attack aiming at the watermarking scheme based on SVD was presented in [10]. If there is a question, there will be an answer. Jain *et. al.*, [11] presented a reliable watermarking scheme based on SVD in which the major components were inserted into the cover image. It is based on the fact that the left and right singular matrices obtained by SVD can store most information of a watermark. The problem has also been solved in [12].

In this paper, we propose a novel watermarking scheme based DCT-DWT and shuffled singular value decomposition (SSVD) after summarizing the common point from the watermarking schemes solved the false positive problem. First of all, the host image is performed by one-level DWT using 'Haar' wavelet and the low frequency approximation sub-band LL_1 is acquired. Meanwhile, the SSVD is performed on the watermark and the principal components are chosen as the embedding information, while the rest components are viewed as a part of keys. LL_1 is divided into non-overlapping image blocks, and then a constructed matrix is composed of the direct current (DC) components derived from the image block DCT coefficients obtained by DCT on each image block. The principal components of watermark are embedded into the constructed matrix. The watermarked image is obtained after a series of inverse transformations.

The remaining part of the paper is organized as follows. Section 2 gives the preliminaries, which includes the SVD transform, the basic SVD-based watermarking scheme, the weakness of the SVD-based watermark scheme, the SSVD and evaluation criterion of watermark scheme. The proposed watermark method is designed in Section 3, including the procedure of watermark embedding and watermark extraction. Experimental results on the proposed scheme are shown in Section 4. Conclusions and remarks on possible further work are given finally in Section 5.

2. Preliminaries

In this section, we review the SVD transform, the basic watermarking scheme based SVD [4] and point out the weakness of the method. Besides that, the SSVD is introduced briefly in this section. The evaluation criterion is given here, which includes normalized correlation (NC) and peak-signal-to-noise ratio (PSNR).

2.1. Singular Value Decomposition

SVD is an effective numerical analysis tool used in matrices analysis. In the SVD transform, a matrix $\boldsymbol{A}_1$ with size of $N_1 \times N_1$ can be resolved into three parts

$$\boldsymbol{A}_1 = \boldsymbol{U}_1\boldsymbol{S}_1\boldsymbol{V}_1^{\mathrm{T}} = \left[u_1, u_2, \cdots, u_N\right]\begin{bmatrix}\Sigma & 0\\ 0 & 0\end{bmatrix}\left[v_1, v_2, \cdots, v_N\right], \tag{1}$$

where the $\boldsymbol{U}_1$ and $\boldsymbol{V}_1$ are the $N_1 \times N_1$ unitary matrices. $[u_1, u_2, \cdots, u_N]$ and $[v_1, v_2, \cdots, v_N]$ are the column vectors. $\boldsymbol{S}_1$ is an $n \times n$ diagonal matrix, where $\Sigma = diag(\lambda_1, \lambda_2, \cdots, \lambda_r)$. The diagonal element λ_i denotes the *i*th singular value of $\boldsymbol{A}_1$. The SVD transformation can be performed on an image of any size. It should be noted that the two unitary matrices of an image, $\boldsymbol{U}_1$ and $\boldsymbol{V}_1$, specify the geometric information of an image, while the singular values $\boldsymbol{S}_1$ represent the luminance information of an image [11].

2.2. SVD-based Watermarking Method

In the section, we review briefly the SVD-based watermarking method in [4]. The process of watermark embedding is as follows. Firstly, the SVD is applied on the host image $\boldsymbol{A}_2$,

$$\boldsymbol{A}_2 = \boldsymbol{U}_2 \boldsymbol{S}_2 \boldsymbol{V}_2^{\mathrm{T}} . \tag{2}$$

Then, a watermark matrix $\boldsymbol{W}_1$ is added into the singular value matrix $\boldsymbol{S}_2$, and the new matrix $\boldsymbol{S}_2 + \alpha \boldsymbol{W}_1$ is decomposed into $\boldsymbol{U}_{\mathrm{w1}}$, $\boldsymbol{S}_{\mathrm{w1}}$, and $\boldsymbol{V}_{\mathrm{w1}}$ by SVD transform, where α is the scaling factor that determines the embedding intensity of $\boldsymbol{W}_1$,

$$\boldsymbol{S}_2 + \alpha \boldsymbol{W}_1 = \boldsymbol{U}_{\mathrm{w1}} \boldsymbol{S}_{\mathrm{w1}} \boldsymbol{V}_{\mathrm{w1}}^{\mathrm{T}} . \tag{3}$$

The watermarked image $\boldsymbol{A}_{\mathrm{w1}}$ is obtained by

$$\boldsymbol{A}_{\mathrm{w1}} = \boldsymbol{U}_2 \boldsymbol{S}_{\mathrm{w1}} \boldsymbol{V}_2^{\mathrm{T}} . \tag{4}$$

In the procedure of watermark extraction, the watermark $\boldsymbol{W}_1^*$ is extracted from the watermarked image $\boldsymbol{A}_{\mathrm{w1}}$. The watermark extraction can be described as follows,

$$\boldsymbol{A}_1^* = \boldsymbol{U}_1^* \boldsymbol{S}_{\mathrm{w1}}^* \boldsymbol{V}_1^{*\mathrm{T}} , \tag{5}$$

$$\boldsymbol{D}_1^* = \boldsymbol{U}_{\mathrm{w1}} \boldsymbol{S}_{\mathrm{w1}}^* \boldsymbol{V}_{\mathrm{w1}}^{\mathrm{T}} , \tag{6}$$

$$\boldsymbol{W}_1^* = (\boldsymbol{D}_1^* - \boldsymbol{S}_2) / \alpha . \tag{7}$$

Note that the matrices $\boldsymbol{U}_{\mathrm{w1}}$, $\boldsymbol{S}_2$, and $\boldsymbol{V}_{\mathrm{w1}}$ are the keys in the watermark extraction. The above is the whole SVD-based watermarking scheme.

2.3. Weakness of SVD-based Watermarking Method

An attack was proposed in [9], aiming at the SVD-based watermarking scheme [4] mentioned in Section 2.2, which was also called as the false positive problem. After performing SVD on an image, the matrices $\boldsymbol{U}_2$ and $\boldsymbol{V}_2$ represent the details and structure of the image, while the matrix $\boldsymbol{S}_2$ specifies the luminance of the image stated previously in Section 2.1. In [9], the authors have pointed out that in Eq. (7), the extracted watermark $\boldsymbol{W}_1^*$ and $\boldsymbol{D}_1^*$ were different just in the diagonal values, which was up to the scaling factor α. Accordingly, the malicious image attackers can use the fake $\boldsymbol{U}_{\mathrm{f}}$, $\boldsymbol{V}_{\mathrm{f}}$ matrices, which are from $\boldsymbol{S}_2 + \alpha \boldsymbol{W}_{\mathrm{f}} = \boldsymbol{U}_{\mathrm{f}} \boldsymbol{S}_{\mathrm{f}} \boldsymbol{V}_{\mathrm{f}}^{\mathrm{T}}$, to create a fake matrix as $\boldsymbol{D}_{\mathrm{f}}^* = \boldsymbol{U}_{\mathrm{f}} \boldsymbol{S}_{\mathrm{w1}}^* \boldsymbol{V}_{\mathrm{f}}^{\mathrm{T}}$ in Eq. (6). As a result, the extracted watermark in Eq. (7) will be similar to the fake watermark rather than the original watermark. It is obvious to be seen that a line across the diagonals of the fake extracted watermark.

Suppose the original cover image is available in [9], the attackers could use the same steps to embed the fake watermark in the original image and obtain the fake singular matrices $\boldsymbol{U}_{\mathrm{f}}$ and $\boldsymbol{V}_{\mathrm{f}}$. Then $\boldsymbol{U}_{\mathrm{f}}$ and $\boldsymbol{V}_{\mathrm{f}}$ are used to make a false positive watermark in the process of watermark detection.

Figure 1 shows the results of false positive test, in which the fake extracted watermarks are extracted from the watermarked image Lena by using different fake watermarks (Cameraman and Baboon, *etc*.). By modifying the singular value of the original watermark, one can easily create their own watermark as shown in Figure 1 (e) ~ (h).

From Figure 1, we can see that a serious false positive problem exists in the watermarking scheme [4] based on SVD. Furthermore, the problem exists in [5-8]. By comparing these schemes, it is not difficult to find such a fact that the key step of embedding watermark is $\boldsymbol{S}_2 + \alpha \boldsymbol{W}_1 = \boldsymbol{U}_{\mathrm{w1}} \boldsymbol{S}_{\mathrm{w1}} \boldsymbol{V}_{\mathrm{w1}}^{\mathrm{T}}$, and the matrices, $\boldsymbol{U}_{\mathrm{w1}}$ and $\boldsymbol{V}_{\mathrm{w1}}$, are deemed as a part of keys in the procedure of watermark extraction. $\boldsymbol{U}_{\mathrm{w1}}$ and $\boldsymbol{V}_{\mathrm{w1}}$ represent the details and construction of the watermark stated previously. So it should be avoided embedding the watermark into the cover image by Equation (3).

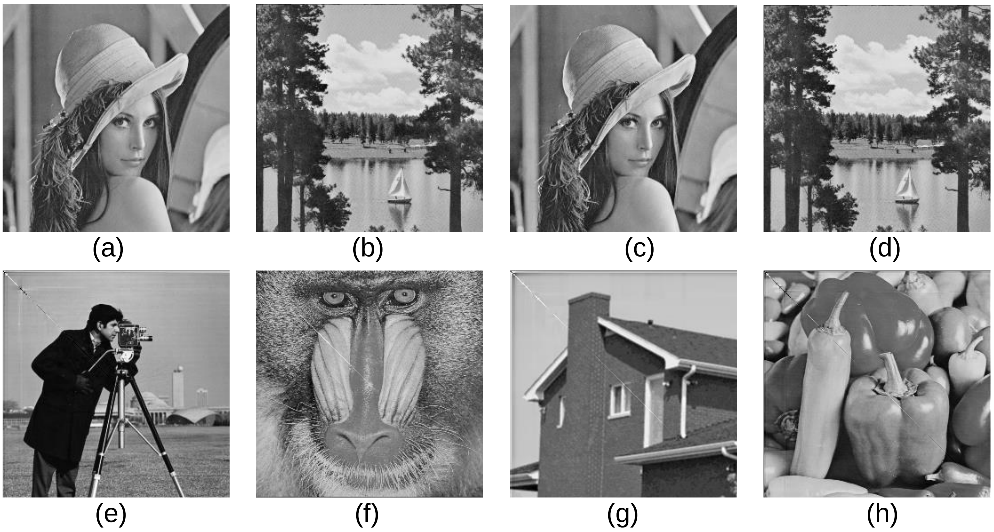

Figure 1. False Positive Test: (a) Original Image Lena; (b) Original Watermark Image Boat; (c) Watermarked Image; (d) Extracted Watermark Using Its Own Keys; (e) Extracted Fake Watermark Cameraman; (f) Extracted Fake Watermark Baboon; (g) Extracted Fake Watermark House; and (h) Extracted Fake Watermark Peppers

2.4. Shuffled Singular Value Decomposition

SSVD was proposed in [13], which is a variation on SVD-based image compression, actually. The change can be regarded as a pretreatment step in which the input image is scrambled, after which it is performed to the standard SVD transformation. The modification comprise a pretreatment step, which is expressed as $\boldsymbol{X} = \hat{S}(\boldsymbol{A}_3)$, where $\hat{S}$ denotes the shuffled operator and $\boldsymbol{X}$ is the permuted image. The size of the image $\boldsymbol{A}_3$ is $N_2 \times N_2$ and $N_2 = n_1^{\ 2}$, where n_1 is integer. $\boldsymbol{X} = \hat{S}(\boldsymbol{A}_3)$ is formed by two steps. In the first place $\boldsymbol{A}_3$ is divided into $n_1 \times n_1$ blocks. And then taking the ith block in row major order and placing its image pixel values in row priority to constitute the ith row of $\boldsymbol{X}$.

Figure 2 demonstrates that the reconstructed image generated by SSVD is better than the image reconstructed by SVD in visual quality under the same image rank condition. In Figure 2, there are a couple of concepts to explain. The SVD transform is applied on image matrix $\boldsymbol{A}_3$, namely, $\boldsymbol{A}_3 = \boldsymbol{U}'\boldsymbol{S}'\boldsymbol{V}'^{\mathrm{T}}$. A rank-$r$ approximation to $\boldsymbol{A}_3$ is the matrix $\boldsymbol{A}_r = \boldsymbol{U}_r \boldsymbol{S}_r \boldsymbol{V}_r^{\mathrm{T}}$, where $\boldsymbol{S}_r$ is the top-left $r \times r$ sub-matrix of $\boldsymbol{S}'$; $\boldsymbol{U}_r$ is made up of the first r columns of $\boldsymbol{U}'$; and $\boldsymbol{V}_r$ consists of the first r rows of $\boldsymbol{V}'^{\mathrm{T}}$. $\boldsymbol{X}_r = \boldsymbol{U}_r' \boldsymbol{S}_r' \boldsymbol{V}_r'^{\mathrm{T}}$ denotes the approximation image , which is similar to $\boldsymbol{X}$.

The PSNR value comparison between SSVD and SVD is shown in Figure 3. It can be seen that PSNR value increases as the growth of rank *r*, which signifies that the approximation image is more and more similar to the original image Barbara. In addition, it is obvious that the PSNR values of SSVD are better than that of SVD under the same rank r, which means that the image $\hat{S}^{-1}(\boldsymbol{X}_r)$ is a much better approximation for $\boldsymbol{A}_3$.

From Figure 2 and Figure 3, we can observe intuitively that the performance of reconstructed image by SSVD is better than that of reconstructed image by SVD. The advantages of SSVD in reconstructed image are the vision effect of approximation and PSNR values in Figure 2 and Figure 3, respectively.

Figure 2. SVD and SSVD Applied on Image Barbara with Size of 256×256: (a) Original Image Barbara; (b) Approximation Image with SVD Rank-2; (c) Approximation Image with SSVD Rank-2; (d) Approximation Image with SVD Rank-5; (e) Approximation Image with SSVD Rank-5; (f) Approximation Image with SVD Rank-10; (g) Approximation Image with SSVD Rank-10; (h) Approximation Image with SVD Rank-20; (i) Approximation Image with SSVD Rank-20; (j) Approximation Image with SVD Rank-50; and (k) Approximation Image with SSVD Rank-50

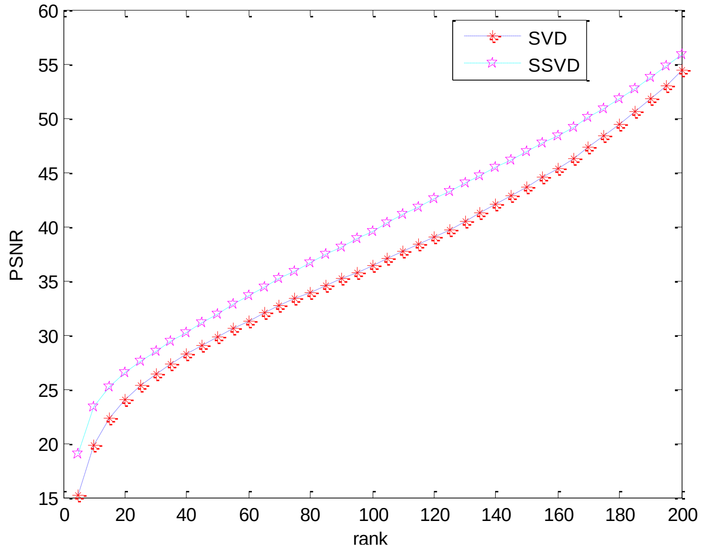

Figure 3. PSNR Comparison between SVD and SSVD

2.5. Evaluation Criterion

The PSNR value between the original image $\boldsymbol{I}$ with size of $M \times N$ and the watermarked image $\boldsymbol{I}^*$ is defined as

$$\text{PSNR} = 10 \times \log_{10} \frac{(I_{\max})^2}{E_{\text{MSE}}} (\text{dB}), \tag{8}$$

$$E_{\text{MSE}} = \frac{1}{MN} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (\boldsymbol{I}(i,j) - \boldsymbol{I}^*(i,j))^2, \tag{9}$$

where $I_{\max}$ is the maximum possible pixel value of original image $\boldsymbol{I}$, and for two images having 8 bits per pixel, $I_{\max}$ is often chosen as 255, so it is in this paper. E_{MSE}, which is the abbreviation of mean squared error between the original image $\boldsymbol{I}$ and the watermarked image $\boldsymbol{I}^*$, is defined by Eq. (9). Typical PSNR value ranges from 30 dB to 50 dB. The higher PSNR value is, the harder to distinguish the difference between the original image and watermarked image by human naked eyes [14].

The NC between the original watermark and extracted watermark is obtained as

$$NC(\boldsymbol{W}, \boldsymbol{W}^*) = \frac{\sum_i \sum_j \boldsymbol{W}(i,j)\boldsymbol{W}^*(i,j)}{\sqrt{\sum_i \sum_j \boldsymbol{W}(i,j)^2} \sqrt{\sum_i \sum_j \boldsymbol{W}^*(i,j)^2}}, \tag{10}$$

where $\boldsymbol{W}$ represents the original watermark and $\boldsymbol{W}^*$ represents the extracted watermark. The NC is a positive value which is less than or equal to 1. A larger NC value means that the extracted watermark is more similar to the original watermark.

3. Proposed Watermarking Scheme

In the section, a novel watermarking method based on DWT-DCT and SSVD is proposed, which contains watermark embedding and watermark extraction. The details of the two processes are described in later sub-sections.

3.1. Watermark Embedding

In the procedure of watermark embedding, there are several basic points concerning DWT and DCT. We will introduce them briefly. DWT is performed on an image, which is divided into four sub-bands, a low resolution approximation sub-band (LL), horizontal (HL), vertical (LH), and diagonal (HH) detail sub-bands. In [3], Huang *et. al.*, presented that the better robustness can be realized if watermark is added in direct current (DC) components because DC components have much greater perceptual capacity than alternating current (AC) components. Accordingly, the DC components are chosen as the location of embedding watermark. Figure 4 shows a block diagram of watermark embedding. The detailed steps of embedding the watermark $\boldsymbol{W}$ with size of $N_2 \times N_2$ into a $M \times M$ gray scale host image $\boldsymbol{I}$ are shown below:

Step 1: The SSVD is performed on $\boldsymbol{W}$ by

$$\boldsymbol{W} = \boldsymbol{U}_{\mathrm{w}} \boldsymbol{S}_{\mathrm{w}} \boldsymbol{V}_{\mathrm{w}}^{\mathrm{T}} . \tag{11}$$

Step 2: The principal components $\boldsymbol{W}_{\boldsymbol{US}}$, which will be embedded into the cover image, are obtained by Eq. (12). The rest components $\boldsymbol{V}_{\mathrm{w}}^{\mathrm{T}}$ are viewed as a part of keys in watermark extraction,

$$\boldsymbol{W}_{\boldsymbol{US}} = \boldsymbol{U}_{\mathrm{w}} \boldsymbol{S}_{\mathrm{w}} . \tag{12}$$

Step 3: The host image is decomposed by one-level wavelet transformation with 'Haar' wavelet, and the sub-band LL_1 with size of $M/2 \times M/2$ is obtained.

Step 4: The LL_1 is divided into $m \times m$ non-overlapping image blocks and the block size is chosen as $m = M/2N_2$. Let $\boldsymbol{B}(i,j)$ denotes the position of an image block at (i,j), where $i,j = 1,2,\cdots,N_2$.

Step 5: Apply DCT on each image block $\boldsymbol{B}(i,j)$. A new matrix $\boldsymbol{B}_{\mathrm{d}}$ is composed of DC components extracted from each block DCT coefficients, and $\boldsymbol{B}_{\mathrm{d}}$ needs to be stored, which will be used to extract watermark information in watermark extraction.

Step 6: The principal components of $\boldsymbol{W}$ are embedded into $\boldsymbol{B}_{\mathrm{d}}$,

$$\boldsymbol{B}_{\mathrm{d}}'(i,j) = \boldsymbol{B}_{\mathrm{d}}(i,j) + \alpha \boldsymbol{W}_{\boldsymbol{US}}(i,j) , \tag{13}$$

where $\boldsymbol{B}_{\mathrm{d}}'(i,j)$ is the distorted DC component in image block (i,j) and α denotes the embedding strength.

Step 7: Inverse DCT is performed on each image block (i,j) and the DC components are replaced by the corresponding values in $\boldsymbol{B}_{\mathrm{d}}'$. After this step, the distorted LL' is obtained.

Step 8: The watermarked image $\boldsymbol{I}_{\mathrm{w}}$ is reconstructed by applying one-level inverse DWT.

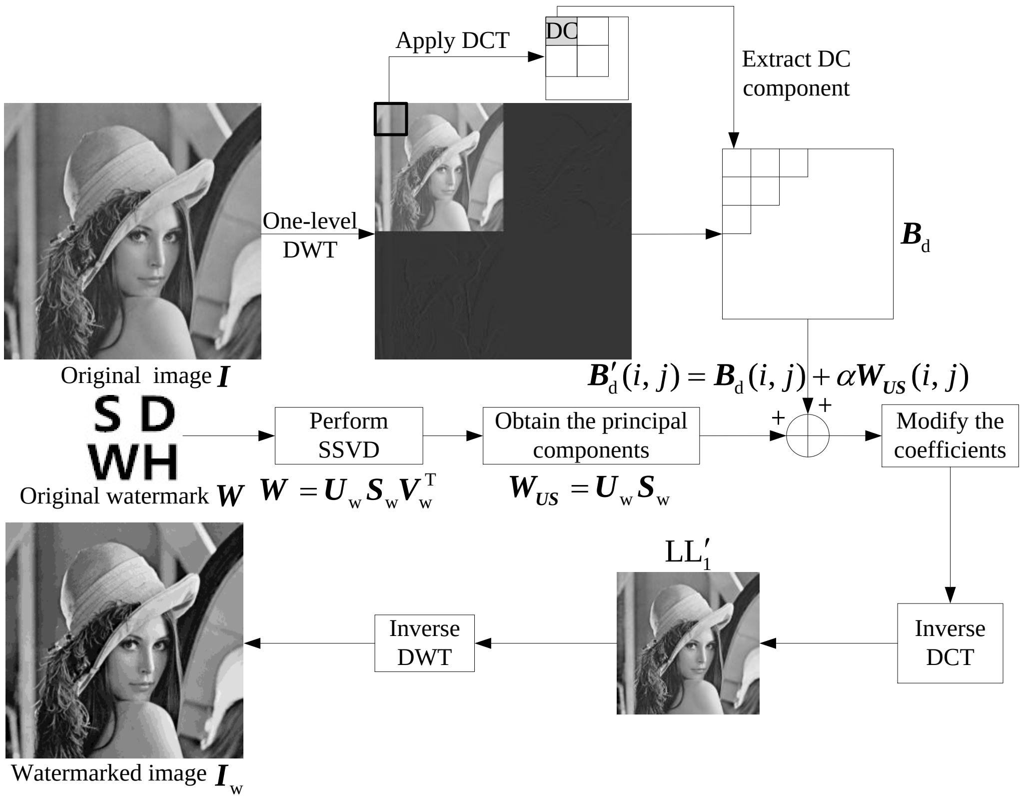

Figure 4. Block Diagram of Watermark Embedding

3.2. Watermark Extraction

In this subsection, the watermark $\boldsymbol{W}^*$ is extracted from the watermarked image $\boldsymbol{I}_{\mathrm{w}}^*$ possibly corrupted by different attacks. Figure 5 shows the schematic diagram of the watermark extraction. Its detailed steps are as follows.

Step 1: One-level 'Haar' DWT is applied on the watermarked image $\boldsymbol{I}_{\mathrm{w}}^*$, and the low frequency sub-band LL_1^* is acquired.

Step 2: LL_1^* is divided into non-overlapping image blocks with size of $m \times m$, which are denoted as $\boldsymbol{B}^*(i,j)$, where $i,j=1,2,\cdots,N_2$.

Step 3: DCT is performed on each block $\boldsymbol{B}^*(i,j)$ and the DC component is extracted from each image block to organize the new matrix $\boldsymbol{B}_{\mathrm{d}}'^*$.

Step 4: The principal components are obtained by

$$\boldsymbol{W}_{\boldsymbol{US}}^*=[\boldsymbol{B}_{\mathrm{d}}'^*(i,j)-\boldsymbol{B}_{\mathrm{d}}(i,j)]/\alpha \,. \tag{14}$$

Step 5: The extracted watermark $\boldsymbol{W}^*$ is obtained as

$$\boldsymbol{W}^*=\boldsymbol{W}_{\boldsymbol{US}}^*\boldsymbol{V}_{\mathrm{w}}^{\mathrm{T}} \,. \tag{15}$$

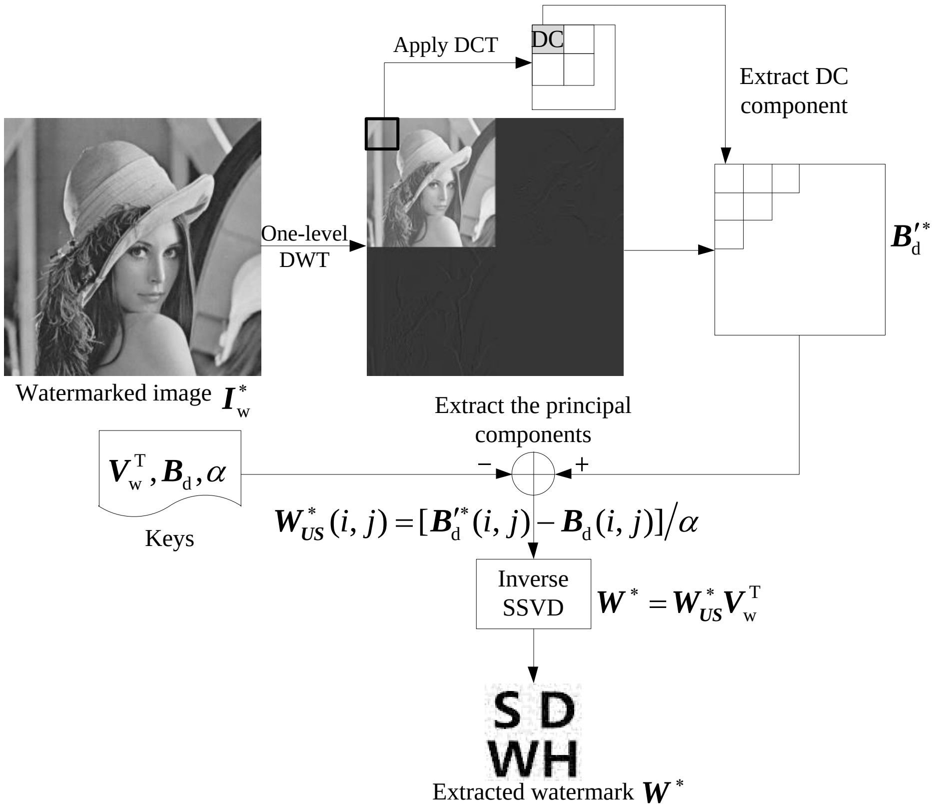

Figure 5. Block Diagram of Watermark Extraction

4. Experimental Results and Performance Analysis

In the section, the experiments with regard to the imperceptibility and robustness of the designed scheme and the false positive test are given. Otherwise, compared with other reliable watermark methods, the proposed scheme shows its advantages and disadvantages. All results are presented in the form of tables and figures, which can convey the effect intuitively. Besides that, the proposed scheme is called as proposed method 1, while the scheme is called as proposed method 2 due to the fact that SSVD is replaced by SVD.

4.1. Imperceptibility and Robustness Test

In the section, some experiments are done to evaluate the proposed scheme's imperceptibility and robustness. The original cover image and the watermark image are gray scale images with size of 512×512 and 64×64, respectively. In the procedure of watermark embedding, the size of the image block is 4×4. The imperceptibility between original image and watermarked image is measured by PSNR, while the quality of extracted watermark is evaluated by NC mentioned previously. The PSNR value is used to measure the similarity between the original image and the watermarked image, while the NC value evaluates the similarity between extracted watermark and original watermark.

In the experiment to test the imperceptivity, the watermark image is embedded into different host images in different scaling factors. The PSNR and NC values are recorded in Table 1 and Table 2. From the two tables, it is obvious that it is appropriate that the embedding intensity α is set as 0.10 to balance the imperceptibility and robustness.

Table 1. PSNR Values of Watermarked Images under Different Embedding Intensities

Embedding intensities	0.01	0.05	0.10	0.50
Lena	59.66	45.67	39.75	26.85
Baboon	59.66	45.67	39.75	26.37
Boat	59.66	45.71	39.85	28.18
Bridge	59.66	45.67	39.75	26.30

Table 2. NC Values of Extracted Watermarks under Different Embedding Intensities

Embedding intensities	0.01	0.05	0.10	0.50
Lena	0.9600	0.9957	0.9984	0.9800
Baboon	0.9600	0.9957	0.9984	0.9918
Boat	0.9600	0.9954	0.9980	0.9660
Bridge	0.9600	0.9956	0.9984	0.9944

Figure 6 shows the results of watermark embedding and watermark extraction without any attacks, where α is chosen as 0.10. In order to test the robustness of the proposed method, various attacks are added to the watermarked image and extracted watermark is taken from the watermarked images under attacks. Figure 7 shows the watermarked images under attacks and Figure 8 shows the extracted watermark corresponding to the attacked watermarked images in Figure 7.

From Table 1, with the increasing embedding strength, PSNR value is on the decline, which means that the imperceptibility of watermark is getting worse. From Figure 7 and Figure 8, we can see that the extracted watermarks are identifiable after the watermarked image corrupted by a number of attacks, such as Salt and Pepper noise, Gaussian noise, JPEG compression, different filtering methods like mean filter and median filter, image sharpening and image cropping, *etc*.

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

Figure 6. Imperceptibility of the Watermark Scheme: (a) Host Image; (b) Original Watermark; (c) Watermarked Image; and (d) Extracted Watermark

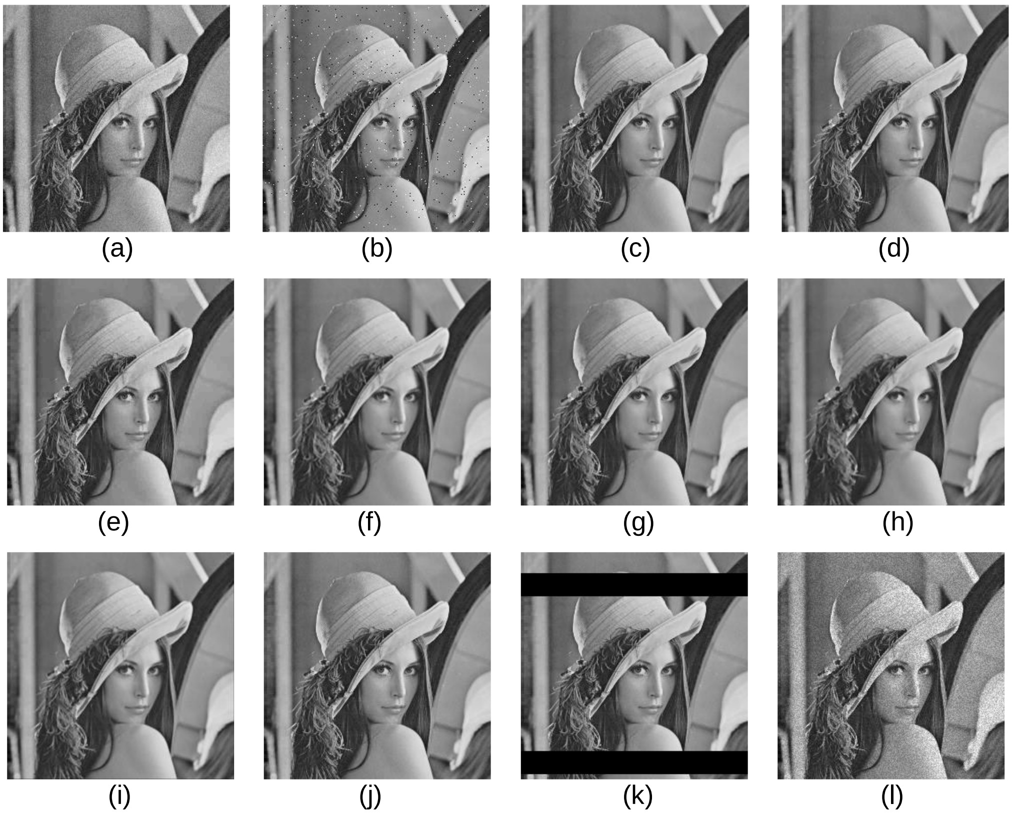

Figure 7. Watermarked Images under Various Attacks: (a) Gaussian Noise (0, 0.001); (b) Salt and Pepper Noise (0.01); (c) JPEG Compression (QF = 70); (d) JPEG Compression (QF = 50); (e) JPEG Compression (QF = 20); (f) Image Rescaling (512×512→200×200→512×512); (g) Median Filter (3×3); (h) Mean Filter (5×5); (i) Mean Filter (3×3); (j) Image Sharpening; (k) Image Cropping; and (l) Speckle Noise (0.01)

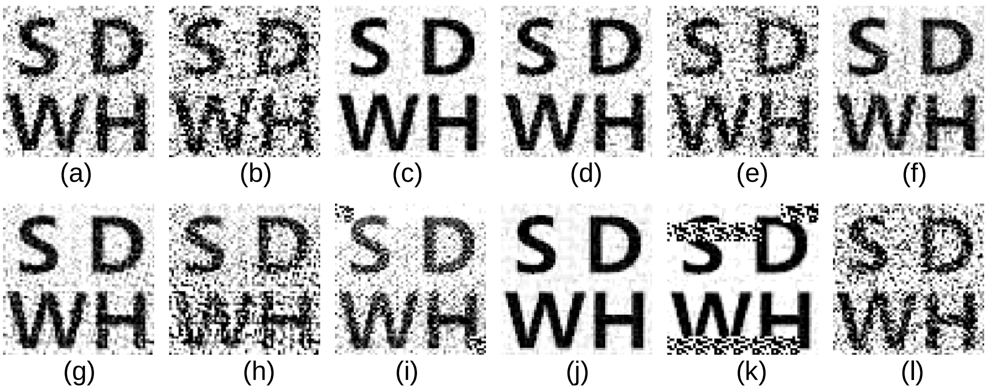

Figure 8. Extracted Watermarks under Corresponding Attacks in Figure 7

In Table 3, the embedding information is different. $\boldsymbol{W}_{\boldsymbol{SV}^{\mathrm{T}}}$ is defined as $\boldsymbol{W}_{\boldsymbol{SV}^{\mathrm{T}}} = \boldsymbol{S}_{\mathrm{w}}\boldsymbol{V}_{\mathrm{w}}^{\mathrm{T}}$ and α is set as 0.10. Then the PSNR values are 39.75 dB and 39.68 dB corresponding to $\boldsymbol{W}_{\boldsymbol{US}}$ and $\boldsymbol{W}_{\boldsymbol{SV}^{\mathrm{T}}}$, respectively. The NC values are included in Table 3, which are used to estimate the similarity between the extracted watermarks and original watermarks (different principal components). Based on the results on Table 3, the proposed scheme has strong ability to resist various attacks added into the watermarked images. Besides, the PSNR values of the watermark scheme are still within the acceptable limit, which indicates that the watermark embedding in the image cannot be found by human vision system.

Table 3. Test of Imperceptibility and Robustness of the Designed Scheme

Embedding information		W_{US}	$W_{SV^{\mathrm{T}}}$
Embedding strength		0.10	0.10
PSNR (dB)		39.75	39.68
NC	**Gaussian noise (0, 0.001)**	0.9592	0.9570
	Salt and Pepper noise (0.01)	0.8905	0.9025
	JPEG compression (QF = 70)	0.9934	0.9935
	JPEG compression (QF = 50)	0.9856	0.9867
	JPEG compression (QF = 20)	0.9193	0.9178
	Image rescaling	0.9769	0.9816
	Median filter (3×3)	0.9779	0.9811
	Median filter (5×5)	0.9052	0.9269
	Mean filter (3×3)	0.9468	0.9668
	Image sharpening	0.9862	0.4498
	Image cropping	0.9196	0.6036
	Speckle noise (0.01)	0.8988	0.9088

4.2. False Positive Test

In this experiment, an experiment concerning the false positive problem is conducted for the designed watermark scheme. α is set as 0.10, while its PSNR value is 39.75 dB and its NC value is 0.9984. We conducted a false positive test by replacing the key $\boldsymbol{V}_{\mathrm{w}}^{\mathrm{T}}$ from the original watermark image with other images such as Cameraman and Peppers. Figure 9 (a) and (b) show the host image and the watermark, respectively, while (c) is the extracted watermark. Figure 9 (d)~(h) are obtained by changing the key $\boldsymbol{V}_{\mathrm{w}}^{\mathrm{T}}$ taken from Cameraman and Peppers, etc. Besides that, the other steps are same exactly. From the results in Figure 9, they indicate that the proposed scheme can avoid the false positive problem mentioned in [8].

4.3. Comparison with Other Reliable Watermark Schemes

In this section, this experiment is conducted to compare the performance of the proposed method with other reliable watermark methods [11, 12]. The scheme mentioned in [11] embedded the principal components $\boldsymbol{W}_{US}$ of the watermark into the singular value matrix of the original image by using an appropriate embedding strength. In the procedure of watermark extraction, the original host image $\boldsymbol{I}$ and the inverse matrices ($\boldsymbol{U}^{-1}$ and $(\boldsymbol{V}^{\mathrm{T}})^{-1}$) are necessary to extract the watermark from the watermarked image possibly corrupted by various attacks, which also increase storage requirement and computational burden. In [12], the original image $\boldsymbol{I}$ is not needed in the watermarking scheme and avoids the operation of matrix inversion. The difference between the proposed scheme and [12] is that the new constructed matrix to embed the principal components is composed of DC component of each image block, while the new constructed matrix inserted the principal components is organized by the largest singular value of each image block. The comparison results are shown in Table 4, in which the PSNR and NC values are listed. It is obvious that the proposed method and the other two methods have their own advantages and disadvantages. The imperceptibility of the proposed scheme is better than the other two schemes under the same embedding strength. The proposed watermark scheme is robust to resist the attacks mentioned in Table 4. The proposed method 1 is that the watermark is applied by SSVD, while SVD is performed on the watermark in the proposed method 2.

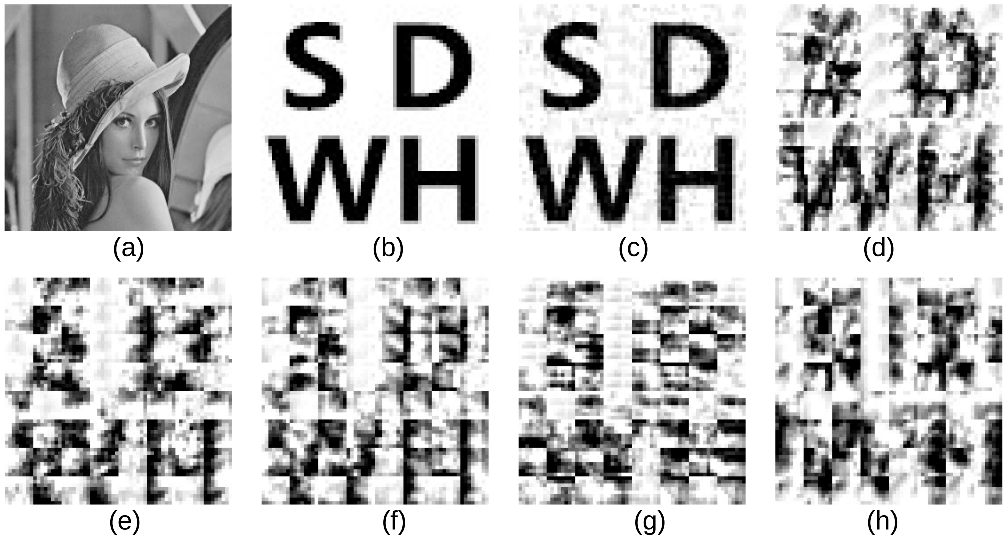

Figure 9. Results of the False Positive Problem: (a) Original Image Lena; (b) Original Watermark; (c) Extracted Watermark Using Its Own Keys; (d) Extracted Watermark Using Cameraman; (e) Extracted Watermark Using Baboon; (f) Extracted Watermark Using Boat; (g) Extracted Watermark Using Bridge; and (h) Extracted Watermark Using Peppers

Table 4. Comparison with Other Reliable Watermark Schemes

Methods		Jain *et. al.*, [11]	Guo and Prasetyo [12]	Proposed method 1	Proposed method 2
Embedding strength		0.10	0.10	0.10	0.10
PSNR (dB)		20.98	39.70	39.75	39.69
NC	**Gaussian noise (0, 0.001)**	0.9695	0.9614	0.9595	0.9595
	Salt and Pepper noise (0.01)	0.9157	0.8882	0.8877	0.8858
	JPEG compression (QF = 70)	0.9960	0.9940	0.9934	0.9941
	JPEG compression (QF = 50)	0.9877	0.9862	0.9856	0.9866
	JPEG compression (QF = 20)	0.9550	0.9229	0.9193	0.9235
	Image rescaling	0.6589	0.9676	0.9769	0.9805
	Median filter (3×3)	0.7083	0.9729	0.9779	0.9821
	Median filter (5×5)	0.5799	0.8897	0.9052	0.9224
	Mean filter (3×3)	0.7086	0.9439	0.9468	0.9555
	Image sharpening	0.9781	0.9741	0.9786	0.9763
	Image cropping	0.8236	0.9205	0.9196	0.9255
	Speckle noise (0.01)	0.9196	0.9027	0.9012	0.9038

5. Conclusions

A novel watermark scheme based DWT-DCT and SSVD is proposed in this paper. A novelty of the proposed scheme is that the principal components are chosen to embed into the constructed matrix composed of DC component of DCT coefficients in each image block, instead of the whole watermark, while the rest components of the watermark are viewed as a part of keys needed in the process of watermark extraction. The watermark scheme avoids the false positive problem occurred in other watermark schemes based on SVD. Otherwise, it shows excellent robustness in resisting attacks such Gaussian noise, Salt and Pepper noise, image cropping, and median filter, *etc*. The proposed scheme can be extended to the video, audio, color image or other works. However, there are a few disadvantages in this proposed scheme, which is the poor performance in resisting some attacks like rotation, affine transformation, translation, and image-enhancement, etc. One of the orientations of the improved watermark scheme is to be robust to the attacks stated above.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61201371), the Natural Science Foundation of Shandong Province, China (No. ZR2015PF004), and the promotive research fund for excellent young and middle-aged scientists of Shandong Province, China (No. BS2013DX022). The authors thank Heng Zhang and Yunpeng Zhang for their kind help and valuable suggestions in revising this paper. The authors also thank the anonymous reviewers and the editors for their valuable comments to improve the presentation of the paper.

References

[1] T. Hai, C. M. Li, J. M. Zain and A. N. Abdalla, “Robust image watermarking theories and techniques: A review”, Journal of Applied Research and Technology, vol. 12, no. 1, **(2014)** Feb., pp. 122-138.

[2] Z. Y. An and H. Y. Liu, “Research on digital watermark technology based on LSB algorithm”, Proceedings of the 4th International Conference on Computational and Information Sciences, Chongqing, China, **(2012)** Aug. 17-19, pp. 207-210.

[3] J. W. Huang, Y. Q. Shi and Y. Shi, “Embedding image watermarks in DC components”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 10, no. 6, **(2000)** Sept., pp. 974-979.

[4] R. Z. Liu and T. N. Tan, “An SVD-based watermarking scheme for protecting rightful ownership”, IEEE Transactions on Multimedia, vol. 4, no. 1, **(2002)** Mar., pp. 121-128.

[5] J. Varghese, S. Subash, O. B. Hussain, M. R. Saadi, B. Babu, M. S. Khan and J. M. Basheer, “An efficient DCT-SVD based algorithm for digital image watermarking”, Proceedings of the International Carnahan Conference on Security Technology, Rome, Italy, **(2014)** Oct. 13-16, Article number: 6987043, 6 pages.

[6] R. Islam and J. M. Kim, “Reliable RGB color image watermarking using DWT and SVD”, Proceedings of the 3rd International Conference on Informatics, Electronics and Vision, Dhaka, Bangladesh, **(2014)** May 23-24, Article number: 6850815, 4 pages.

[7] X. Y. Ye, X. T. Chen, M. Deng, S. Y. Hui and Y. L. Wang, “A multiple-level DCT based robust DWT-SVD watermark method”, Proceedings of the 10th International Conference on Computational Intelligence and Security, Kunming, China, **(2014)** Nov. 15-16, pp. 479-483.

[8] S. Fazli and M. Moeini, “A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks”, Optik - International Journal for Light and Electron Optics, vol. 127, no. 2, **(2016)** Jan., pp. 964-972.

[9] X. P. Zhang and K. Li, “Comments on ‘An SVD-based watermarking scheme for protecting rightful ownership’”, IEEE Transactions on Multimedia, vol. 7, no. 2, **(2005)** Apr., pp. 593-594.

[10] Y. Naderahmadian and S. Beheshyi, “A realistic attack on SVD based watermarking scheme”, Proceedings of the 28th IEEE Canadian Conference on Electrical and Computer Engineering, Halifax, Canada, **(2015)** May 3-6, pp. 1238-1242.

[11] C. Jain, S. Arora, and P. K. Panigrahi, “A reliable SVD based watermarking scheme”, Computer Science, **(2008)**, http://arxiv.org/pdf/0808.0309v1.pdf, 8 pages.

[12] J. M. Guo and H. Prasetyo, “False-positive-free SVD-based image watermarking”, Journal of Visual Communication and Image Representation, vol. 25, no. 5, **(2014)** Jul., pp. 1149-1163.

[13] A. Ranade, S. S. Mahabalarao, and S. Kale, “A variation on SVD based image compression”, Image and Vision Computing, vol. 25, no. 6, **(2007)** Jun., pp. 771-777.

[14] O. O. Khalifa, Y. B. Yusof, and R. F. Olanrewaju, “Performance evaluations of digital watermarking system”, Proceedings of the 8th International Conference on Information Science and Digital Content Technology, Jeju Island, South Korea, **(2012)** Jun. 26-28, pp. 533-536.

Authors

Zhi Zhang, he was born in Shandong province, China, in 1992. He received his B.E. degree in electronic information engineering from Shandong University of Science and Technology, China, in 2016. He is currently pursuing his M.E. degree in information and communication engineering at Shandong University, China. His current research interests include digital image processing and computer vision.

Chengyou Wang, he was born in Shandong province, China, in 1979. He received his B.E. degree in electronic information science and technology from Yantai University, China, in 2004, and his M.E. and Ph.D. degrees in signal and information processing from Tianjin University, China, in 2007 and 2010, respectively. He is currently an associate professor and supervisor of postgraduate students with the School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai, China. His current research interests include digital image/video processing and analysis (transform coding, deblocking, demosaicking, digital watermarking, image dehazing, image quality assessment, *etc*.), computer vision (image retrieval, tamper detection, *etc*.), pattern recognition and machine learning, and multidimensional signal and information processing.

Xiao Zhou, she was born in Shandong province, China, in 1982. She received her B.E. degree in automation from Nanjing University of Posts and Telecommunications, China, in 2003; her M.E. degree in information and communication engineering from Inha University, Korea, in 2005; and her Ph.D. degree in information and communication engineering from Tsinghua University, China, in 2013. She is currently a lecturer and supervisor of postgraduate students with the School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai, China. Her current research interests include wireless communication technology, and digital image processing and computer vision.

