J. Vis. Commun. Image R. 25 (2014) 1149–1163

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

False-positive-free SVD-based image watermarking

Jing-Ming Guo *, Heri Prasetyo

Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan

ARTICLE INFO

Article history:
Received 12 December 2013
Accepted 25 March 2014
Available online 3 April 2014

Keywords:
False positive problem
Image watermarking
Singular Value Decomposition (SVD)
Shuffled SVD (SSVD)
Data hiding
Authentication
Image security
Spread spectrum

ABSTRACT

The need of copyright protection and rightful ownership become very urgent in the fast growing Internet environment. The watermarking offers a convenient way to hide specific information via an imaging system for the consumer electronic devices such as digital camera, scanner, and printer. Numerous efforts have been devoted in the Singular Value Decomposition (SVD)-based image watermarking schemes which embed the visual watermark image into the host image before publishing for public usage. However, the main drawback of the SVD-based image watermarking is its false positive problem of which an attacker can easily claim and obtain the correct watermark from an unauthorized image. In this paper, we proposed a new SVD-based image watermarking by embedding the principal component of a watermark into the host image of block based manner using spread spectrum concept. The experimental results demonstrate that the proposed method overcomes the false positive problem, achieves a high payload, and outperforms the former reliable SVD-based watermarking.

1. Introduction

The main goal of image watermarking is to hide some important information into a host image [1] such that the presence of the watermark cannot be perceived by human vision. A good watermarking algorithm should be able to meet three criteria, i.e. the rightful ownership protection, robustness to image manipulations, and watermark imperceptibility. In the ideal situation, only the real owner can extract the watermark correctly from a watermarked image. Several methods have been addressed for developing or improving the image watermarking scheme as reported in [1,3,10–31,36–39]. The watermarking method in [1,3,10–31] hides the visual watermark information into the host image in the transformed domain using Secure Spread Spectrum concept [1] by employing some specific scaling factor. The SVD transformation is commonly employed in the image watermarking scheme because of stability property in its singular value matrix [3,10–31]. Some extensions have been developed in order to embed the watermark image into host image (or performing the data hiding) in the halftoning domain [36–39]. As reported in literature, the SVD-based [3,10–31] and halftoning-based [36–38] image watermarking are robust against several common image processing attacks and at the same time it hides the watermark information effectively. Before watermark embedding, some preprocessing methods can be applied for improving the host image quality such as contrast enhancement [35]. Since the image watermarking method offers a good tool for ownership protection and privacy, an image watermarking can also be utilized in the video surveillance system [34] in which only the video owner can extract or view the specific information from this video sequence. The watermarking proposed in [3] is the pioneer of the SVD-based image watermarking. Numerous researches have devoted to improve the SVD watermarking performances [11–31].

In the SVD watermarking approach, the watermark information is normally embedded into the singular value matrix of the host image. In general, two common approaches are used to embed the watermark information into a host image: (1) directly insert the watermark image into the singular value matrix of the host image [11–20], or (2) inject the watermark singular value into the singular value matrix of the host image [21–31]. Both methods yield good image quality in terms of the PSNR, and robust against several attacks in terms of the correlation coefficients reported in [11–31].

In the SVD watermarking approaches, the scaling factor plays an important role to control the robustness and imperceptibility of a watermark. By setting a higher value of the scaling factor, the watermarked image is more robust against several attacks. Yet, the image quality is dramatically degraded. In contrast, the transparency of the watermark is achieved by setting a lower scaling factor with a trade-off that the watermarked image is rather less robust against geometric and image processing attacks. However,

* Corresponding author.
E-mail addresses: jmguo@seed.net.tw (J.-M. Guo), heri_inf_its_02@yahoo.co.id (H. Prasetyo).

http://dx.doi.org/10.1016/j.jvcir.2014.03.012
1047-3203/

there is a major flaw with the SVD watermarking scheme as reported in [4–9].

Most literature [21–31] only embeds the watermark singular value into the host image. The SVD-based image watermarking schemes [21–31] have a good stability and robust against the common image manipulation (such as histogram equalization, filtering, adding noise, etc.) and also geometric distortion (such as image cutting, rotation, etc.). However, this embedding strategy leads to an ambiguous situation of the false positive problem. An attacker can easily obtain the correct watermark from an unauthorized image downloaded from the Internet or public available source. A false positive problem occurs when the correct counterfeit extracted watermark is obtained from an arbitrary image in which the embedded watermark is totally different from the extracted watermark. Strictly speaking, an attacker can easily find any reference image from an arbitrary image.

The reliable SVD-based image watermarking has been proposed in [10] in which the principal component is embedded into the host image. It is based on the fact that SVD subspace (left and right singular vectors, matrices U and V^T) can preserve significant amount of information of an image. The false positive problem in [21–31] can be solved using this strategy. However, the reliable SVD-based watermarking [10] is not robust against various attacks and distortions. In this paper, we propose a new SVD-based watermarking scheme which can avoid the false positive problem by embedding the principal component of watermark image into host image. We give a formal definition of the principal component which can be obtained from an ordinary SVD operation or its variation from the watermark image. The proposed method embeds the left principal component ($W_{\Sigma U}$), or right principal component ($W_{\Sigma V^T}$) or eigenvector/key (U or V) into the host image.

The rest of this paper is organized as follows. The SVD-based image watermarking is briefly reviewed in Section 2. Section 3 presents the weakness of the SVD-based image watermarking scheme. The proposed SVD image watermarking is presented in Section 4. Experimental results are documented in Section 5. Finally, the conclusions are drawn at the end of this paper.

2. SVD-based image watermarking

This section gives a brief review of the Singular Value Decomposition (SVD) and its variation. The connection between Karhunen–Loeve Transform (KLT) and SVD as well as its variations are also discussed in this section. Subsequently, the relevant works of the SVD-based image watermarking are reviewed including the core operation in watermark embedding and extraction stage. The robustness and imperceptibility of the SVD-based image watermarking are reported to investigate the effectiveness in terms of the copyright protection and ownership rightful application.

2.1. Singular value decomposition and its variations

The Singular Value Decomposition (SVD) is a linear algebraic tool to diagonalize and decompose a matrix into its eigenvectors and eigenvalues [2–3]. The SVD has been widely used in the image compression since of its ability to find low rank approximation by transforming a given image into a new compact representation. Formally, the SVD of an image $A \in \mathbb{R}^{N\times M}$ is defined as

$$A \Rightarrow U\Sigma V^T \tag{1}$$

where $U \in \mathbb{R}^{N\times r}$ and $V \in \mathbb{R}^{M\times r}$ denote the left and right singular vectors, and $\Sigma \in \mathbb{R}^{r\times r}$ denotes the diagonal matrix consisting singular value in decreasing order, i.e. $\Sigma_r = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_r)$ and $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0$. The $U = [u_1, u_2, \ldots, u_N]$ and $V = [v_1, v_2, \ldots, v_M]$ are unitary matrices which meet $UU^T = U^TU = I_N$ and $VV^T = V^TV = I_M$.

Let r denotes the rank of the matrix A or the number of non-zero singular value in Σ. The compact representation of A in lower rank and each element of A can be defined as (2) and (3), respectively:

$$A = \sum_{i=1}^{r} u_i \lambda_i v_i^T = \sum_{i=1}^{r} \lambda_i u_i v_i^T, \tag{2}$$

$$A_{ij} = \sum_{k=1}^{r} \lambda_k u_{ik} v_{jk}^T. \tag{3}$$

Eq. (3) can be rewritten into another form as

$$A_{ij} = \sum_{k=1}^{r} c_{ik} v_{jk}^T. \tag{4}$$

The element of A can be compared with the Discrete Fourier Transform (DFT) which decomposes the original data into orthogonal basis as

$$A_{ij} = \sum_{k} b_{ik} e^{\mathbf{i}2\pi jk/t}. \tag{5}$$

The form (4) and (5) has similarity in which the DFT cyclical term $e^{\mathbf{i}2\pi jk/t}$ is replaced with the normalized vector term v_{jk}^T in the SVD computation. Basis image in SVD is determined in very specific way from image data rather than from the independent orthogonal transform coefficient [33]. The first few singular vectors in SVD represent low frequency components in the DFT, where the subsequent singular vectors gives the higher frequency. The SVD offers a better image structure result compared with the DFT.

Shuffled Singular Value Decomposition (SSVD) [2] improves the reconstructed image quality by breaking an image A into set of ensemble images $A = \{A_1, A_2, \ldots, A_{n^2}\}$. The SSVD can be viewed as a preprocessing from SVD by permuting the original image A with the data-independent permutation. The permuted image is then fed into the standard SVD algorithm. Formally, the SSVD is defined as

$$A \xrightarrow{\text{SSVD}} S\{A\} \xrightarrow{\text{SVD}} U\Sigma V^T, \tag{6}$$

where $S\{\cdot\}$ denotes the suffled or scrambled operator. It can be an identity operator, bit interleaving operation, or breaking an image into several image blocks to produce a set column wise image. The shuffled operator produces an ensemble image as low resolution sample of image A. Fig. 1 shows the reconstructed image obtained from the SVD and SSVD operation under the same image rank, r. The SSVD produces the reconstructed image with a better visual quality compared with SVD operation using the same image rank. The PSNR comparison between SVD and SSVD is reported in Fig. 2. The SSVD yields a better PSNR compared to that of the SVD under the same image rank.

Kurhunen–Louve Transform (KLT) for an ensemble of images $A \Rightarrow A_1, A_2, \ldots, A_{n^2}$ can be computed as performing shuffled operator to break an image into a set of column vectors. Let x_i be the linearized version of A_i. Suppose that X is a matrix formed from x_i as its column vectors, i.e. $X = [x_1, x_2, \ldots, x_{n^2}]$. The autocorrelation matrix of X is defined as

$$C_X = \frac{1}{n^2}\sum_{i=1}^{n^2} x_i x_i^T = \frac{1}{n^2} XX^T. \tag{7}$$

With means of eigen-decomposition, the matrix C_X can be diagonalized as:

$$C_X \Rightarrow \Phi\Lambda\Phi^T, \tag{8}$$

where Φ and Λ represent the singular vector and singular value, respectively. Then, the KLT of X can be obtained after

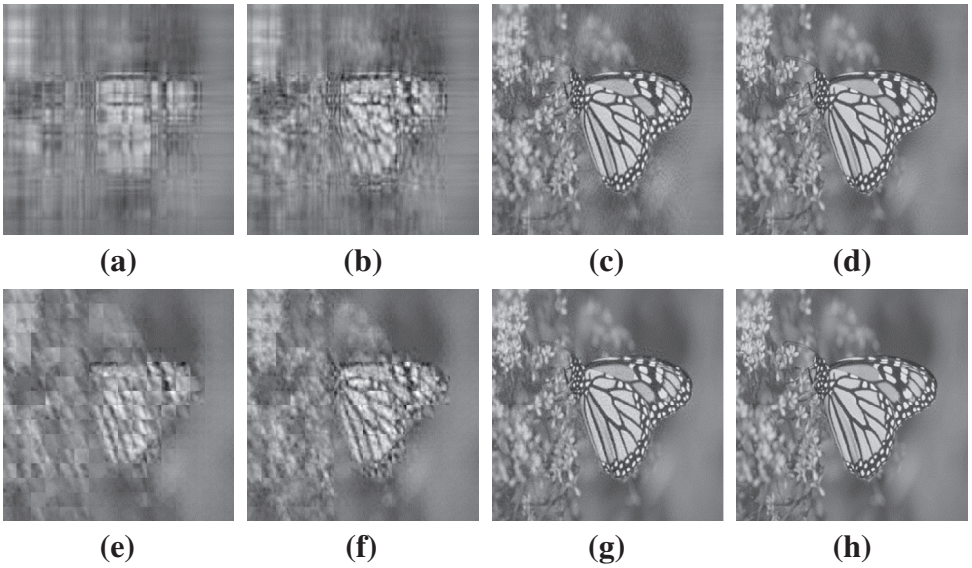

Fig. 1. Image representation using SVD: (a) $r = 5$, (b) $r = 10$, (c) $r = 50$, and (d) $r = 80$. Results from SSVD: (e) $r = 5$, (f) $r = 10$, (g) $r = 50$, and (h) $r = 80$.

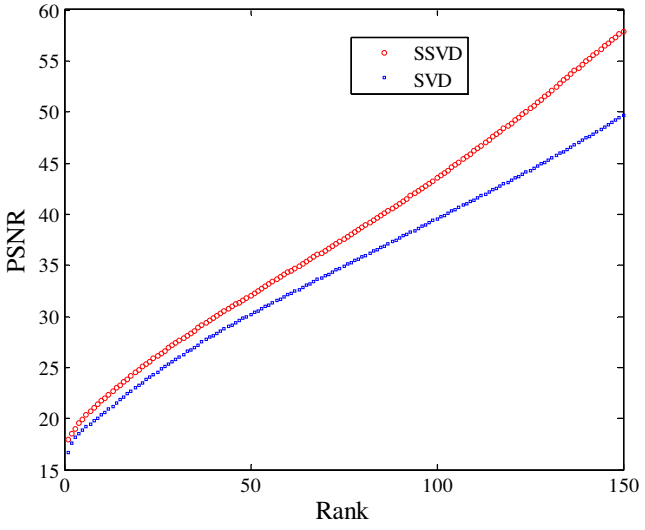

Fig. 2. PSNR comparison between SVD and SSVD.

eigen-decomposition as $Y = \Phi^T X$. Since Φ is data dependent, the matrices Φ and Y are needed to recover matrix X.

By performing the SVD operation on matrix X, we can obtain $X \Rightarrow U\ \Sigma V^T$. Subsequently, the autocorrelation matrix in (7) can be rewritten as:

$$C_X = \frac{1}{n^2} XX^T,$$

$$\Phi\Lambda\Phi^T = \frac{1}{n^2} U\Sigma V^T V\Sigma U^T,$$

$$\Phi\Lambda\Phi^T = U\frac{1}{n^2}\Sigma^2 U^T. \tag{9}$$

From (9), we obtain $\Phi = U$ and $\lambda = \frac{1}{n^2}\Sigma^2$. Further, $Y = \Phi^T X = U^T U\Sigma V^T = \Sigma V^T$. We call the matrix Y as principal component of image/matrix A. To reconstruct matrix X, we simply perform the computation $X = \Phi\, Y = UY$. To obtain the matrix X, one should know the principal component matrix Y and eigenvector U.

Using a similar computation, we may obtain the other principal component of matrix X. Let $Z = X^T$ be the transpose version of matrix X. Applying SVD, one obtains $Z \Rightarrow V\Sigma U^T$ and $Z^T \Rightarrow U\Sigma V^T$. The autocorrelation matrix can be computed using the simple algebra as

$$C_Z = \frac{1}{n^2} ZZ^T,$$

$$\Psi\Xi\Psi^T = \frac{1}{n^2} V\Sigma U^T U\Sigma V^T,$$

$$\Psi\Xi\Psi^T = V\frac{1}{n^2}\Sigma^2 V^T. \tag{10}$$

Then, $\Psi = V$ and $\Xi = \frac{1}{n^2}\Sigma^2$. The new representation of matrix Z can be formulated as $\Upsilon = \Psi^T Z = V^T V\Sigma U^T = \Sigma U^T$ with the transpose version given as $\Upsilon^T = \Sigma U$. The matrix X can be obtained using $X = Z^T = \Upsilon^T\Psi^T = \Upsilon^T V^T$. In our proposed method, the new image representation (principal component) Y or Υ^T is embedded into

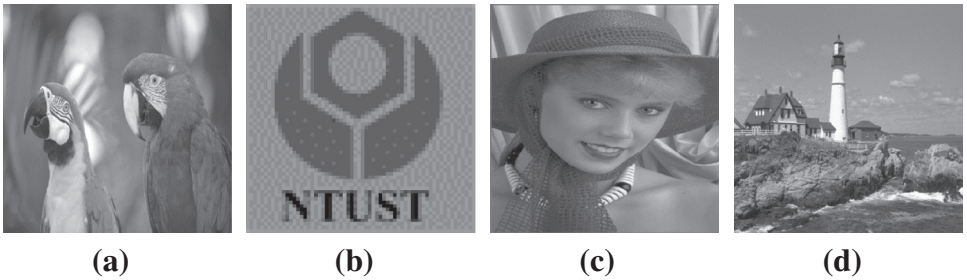

Fig. 3. Image set: (a) Parrots, (b) Logo, (c) Woman Hat, and (d) Light House.

the host image coefficient with their eigenvector U or V as a key in the watermark extraction for recovering the watermark image.

2.2. SVD-based image watermarking

In this subsection, the general strategy of watermark embedding as proposed in [21–31] is reviewed. Let A be a grayscale host image of size $M \times M$, and W is the visual grayscale watermark of size $N \times N$. First, the SVD decomposes the watermark image as

$$W \Rightarrow U_w \Sigma_w V_w^T. \tag{11}$$

Meanwhile, the host image is also decomposed using the Discrete Wavelet Transform (DWT) into four sub-bands, i.e. LL, LH, HL, and HH sub-bands. The sub-band LL is divided into several non-overlapping image blocks, and subsequently the SVD is applied for each image block. The singular value of the visual watermark is directly embedded into the largest singular value matrix of each host image block by employing a suited scaling factor as

$$\lambda_{\max}^d = \lambda_{\max} + \alpha \lambda_w, \tag{12}$$

where $\lambda_{\max}^d$ and $\lambda_{\max}$ denotes the distorted and original largest singular value of the host image, respectively. The notations α and λ_w represent the scaling factor and singular value of the watermark image. The SVD-based image watermarking scheme [21–31] enjoys the main advantage of singular value stability property, in which the watermarked image is similar to the original host image when a little distortion or perturbation is added into host image singular value.

In the watermark extraction, the SVD-based watermarking scheme extracts the watermark W^* from the possibly corrupted watermarked image A_w^*. Particularly, some common image processing attacks and geometric distortions may degrade the image quality. The watermark singular value can be extracted using the following method

$$\lambda_w^* = \frac{1}{\alpha}\{\lambda_{\max}^* - \lambda_{\max}\}, \tag{13}$$

where λ_w^* and $\lambda_{\max}^*$ denote the corrupted watermark singular value and the largest singular value of the corrupted watermarked image. By employing the U_w and V_w^T matrices obtained from the embedding step as the key, the extracted watermark can be obtained as

$$W^* \Leftarrow U_w \Sigma_w^* V_w^T. \tag{14}$$

Fig. 4 shows the SVD-based image watermarking result while the watermarked image is given in Fig. 4(c) and (d), respectively. Figs. 5 and 6 report the watermarked image with various malicious attacks and the extracted watermarks, respectively. From these figures, we can see that the SVD-based image watermarking offers a good solution for hiding the visual watermark image as well as the copyright protection.

3. Weakness of SVD-based image watermarking

The robustness of the SVD-based image watermarking is measured using the Normalized Cross Correlation (NCC) as the similarity between the original watermark image W and the extracted watermark W^* of size $N \times N$ as

$$\rho(W, W^*) = \frac{\sum_{i=1}^N \sum_{j=1}^N (w_{ij} - \mu_W)(w_{ij}^* - \mu_w^*)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^N (w_{ij} - \mu_W)^2} \sqrt{\sum_{i=1}^N \sum_{j=1}^N (w_{ij}^* - \mu_w^*)^2}}, \tag{15}$$

where μ_W and μ_w^* indicate the mean values of the original and extracted watermarks, respectively. The symbol w_{ij} and w_{ij}^* denote the original and extracted watermark at pixel position (i,j).

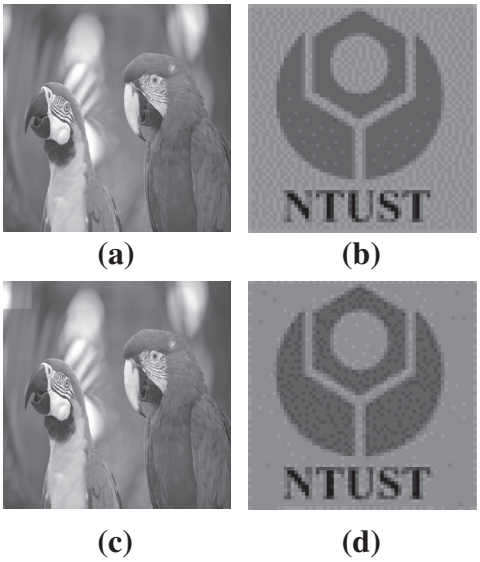

Fig. 4. Visual assessment of imperceptibility in SVD-based image watermarking: (a) host image, (b) watermark image, (c) watermarked image (PSNR = 33.7433), and (d) extracted watermark (NCC = 0.9963).

The other criterion to judge the effectiveness of the RDWT–SVD watermarking is the imperceptibility. The visual quality of a host image should not be degraded too much after the watermark is inserted. The Peak Signal–Noise Ratio (PSNR) can be adopted to objectively measure the similarity between the original and watermarked images. The PSNR between original and watermarked image of size $M \times M$ is defined as:

$$\mathrm{PSNR} = 10 \log_{10} \frac{255^2}{\frac{1}{MN}\sum_{i=1}^M \sum_{j=1}^M \left[A_{ij} - A_{ij}^w\right]^2}. \tag{16}$$

where A_{ij} and A_{ij}^w denote the original and watermarked image at pixel position (i,j).

3.1. False positive problem in SVD-based image watermarking

Suppose that the real owner embeds the watermark W into the host image A to obtain the watermarked image A_w which later published on the Internet or public available means. Suppose an attacker has his own watermark image W_f. By performing the SVD operation on W_f, i.e. $W_f \Rightarrow U_{wf} \Sigma_{wf} V_{wf}^T$, an attacker can easily produce the counterfeit matrix (U_{wf} and V_{wf}^T) as key. At the watermark extraction stage, the false positive problem occurs when an attacker tries to extract the watermark from the watermarked image, A_w.

An attacker will receive the corrupted singular value of watermark Σ_{wf}^* from the watermarked image A_w. Subsequently, an attacker can recover the extracted watermark using Σ_{wf}^* and his counterfeit key (U_{wf} and V_{wf}^T) as

$$W_{wf} \Leftarrow U_{wf} \Sigma_{wf}^* V_{wf}^T. \tag{17}$$

As a result, an attacker can obtain the watermark image W_{wf} which is apparently identical to the watermark image W_f. As we know that the owner's watermarked image A conceives the watermark information W. Fig. 7 reports the false positive test for the extracted watermark using the Parrots watermarked image and Woman Hat and Light House images (as counterfeit reference watermark). By changing the singular value of the extracted watermark as given in (17), one can easily produce their own watermark image as shown in Fig. 7(d)–(e). Table 1 summarizes the false positive

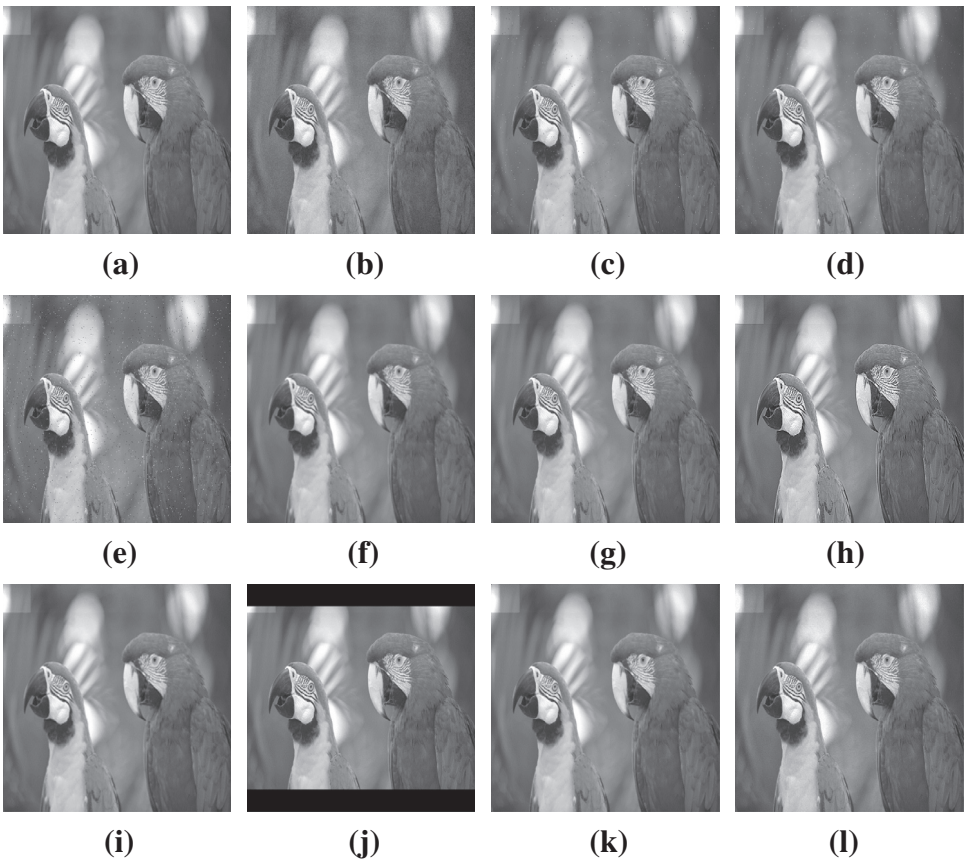

Fig. 5. SVD-based watermarking robustness test under: (a) JPEG compression $Q = 80$, (b) Gaussian noise 0.001, (c) multiplicative uniform noise 0.005, (d) additive uniform noise 0.005, (e) salt and pepper noise 0.01, (f) mean filter, (g) gamma correction, (h) image sharpening, (i) image rescaling $512 \times 512 \rightarrow 256 \times 256 \rightarrow 512 \times 512$, (j) image cropping, (k) median filter 3×3, and (l) speckle noise 0.001.

problem occurred in recent published paper. Apparently, these ambiguity situations in the SVD watermarking cannot be accepted for practical applications which need the ownership validity.

3.2. Analysis of the SVD-based image watermarking

The theoretical analysis of the SVD image watermarking is presented in this section. The SVD-based scheme is an improved image watermarking proposed in [1,3]. Even though SVD-based watermarking seems robust against attacks, it has a major flaw in its false positive problem. Let A and B be full matrices of size $N \times N$. The SVD operation decompose matrix A as $A \Rightarrow U\Sigma_A V^T$. The matrix B is composed by changing the singular value matrix of A with any arbitrary singular value matrix, yielding $B \Leftarrow U\Sigma_B V^T$. The squared error sum between matrix A and B can be trivially derived as:

$$\begin{aligned} ||A,B||_2^2 &= ||A_{ij} - B_{ij}||_2^2, = \sum_{i=1}^{N}\sum_{j=1}^{N}(\Sigma U_A V^T - \Sigma U_B V^T)^2, \\ &= \sum_{i=1}^{N}\sum_{j=1}^{N}\left\{(\Sigma_{ij}^A)^2 + (\Sigma_{ij}^B)^2 - 2\Sigma_{ij}^A\Sigma_{ij}^B\right\}, \\ &= \sum_{i=1}^{N}\sum_{j=1}^{N}(\Sigma_{ij}^A - \Sigma_{ij}^B)^2 = ||\Sigma_A, \Sigma_B||_2^2. \end{aligned} \tag{18}$$

From Eq. (18), the squared error sum for the two matrices A and B is equal to the squared error sum between the two singular value matrices Σ_A and Σ_B. When Σ_A and Σ_B simply have a little difference, the value $||A,B||_2^2$ is close to zero, meaning that the two matrices A and B are nearly identical. In the special case, when A^T is the transposed version of matrix A, then the squared error sum between A and A^T is zero. The matrix A and its transpose have the same non-zero singular values, i.e. $A^T = [\Sigma U_A V^T]^T = V\Sigma_A U^T$. In the SVD-based watermarking scheme, the squared error sum between matrix W_f and W_{wf} is close to zero when the diagonal matrix is slightly different by employing the same key (U_{wf} and V_{wf}) for both matrices.

The element-wise multiplication of matrices A and B can be rewritten in form (3) as

$$\begin{aligned} \sum_{i=1}^{N}\sum_{j=1}^{N}A_{ij}B_{ij} &= \sum_{i=1}^{N}\sum_{j=1}^{N}\sum_{k=1}^{r}\lambda_k^A u_{ik} v_{jk}^T \sum_{k=1}^{r}\lambda_k^B u_{ik} v_{jk}^T, \\ &= \sum_{k=1}^{r}\lambda_k^A\lambda_k^B \sum_{i=1}^{N}u_{ik}u_{ik}\sum_{j=1}^{N}v_{jk}v_{jk}. \end{aligned} \tag{19}$$

The norm of the matrices A and B can be computed as

$$\begin{aligned} ||A|| &= \sum_{i=1}^{N}\sum_{j=1}^{N}A_{ij}A_{ij} = \sum_{i=1}^{N}\sum_{j=1}^{N}\sum_{k=1}^{r}\lambda_k^A u_{ik} v_{jk}^T \sum_{k=1}^{r}\lambda_k^A u_{ik} v_{jk}^T, \\ &= \sum_{k=1}^{r}\lambda_k^A\lambda_k^A \sum_{i=1}^{N}u_{ik}u_{ik}\sum_{j=1}^{N}v_{jk}v_{jk}, \end{aligned} \tag{20}$$

$$\begin{aligned} ||B|| &= \sum_{i=1}^{N}\sum_{j=1}^{N}B_{ij}B_{ij} = \sum_{i=1}^{N}\sum_{j=1}^{N}\sum_{k=1}^{r}\lambda_k^B u_{ik} v_{jk}^T \sum_{k=1}^{r}\lambda_k^B u_{ik} v_{jk}^T, \\ &= \sum_{k=1}^{r}\lambda_k^B\lambda_k^B \sum_{i=1}^{N}u_{ik}u_{ik}\sum_{j=1}^{N}v_{jk}v_{jk}. \end{aligned} \tag{21}$$

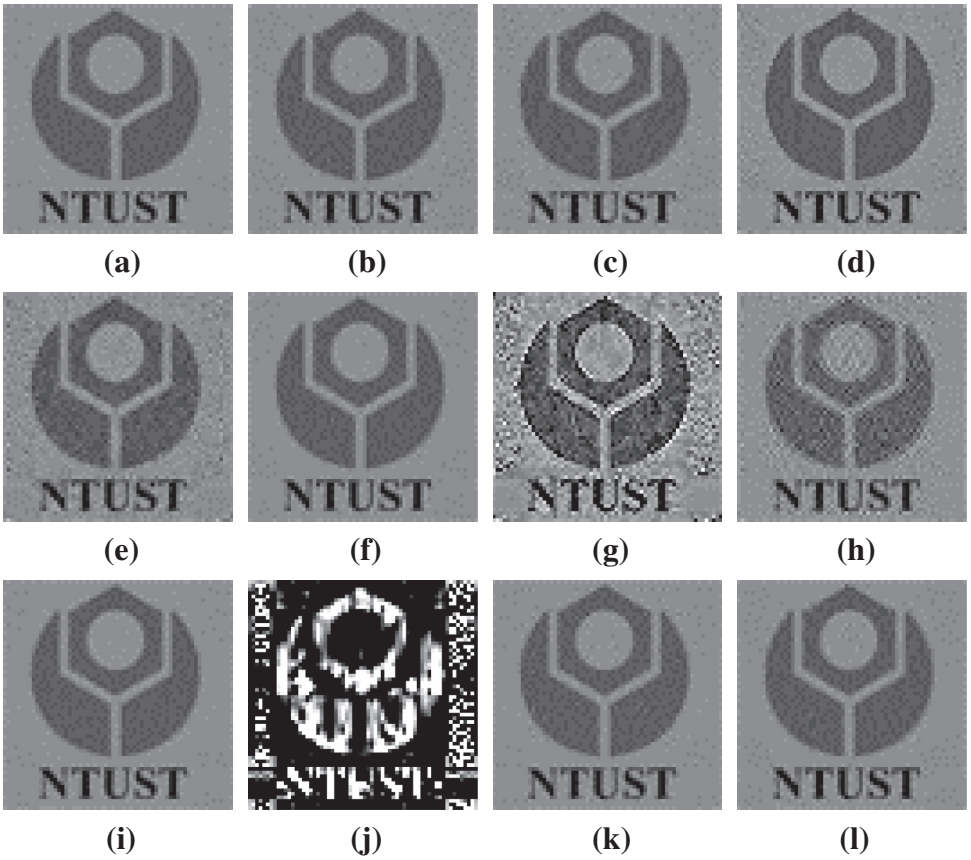

Fig. 6. Extracted watermark under several attacks in Fig. 5: (a) NCC = 0.9954, (b) NCC = 0.9890, (c) NCC = 0.9829, (d) NCC = 0.9857, (e) NCC = 0.9512, (f) NCC = 0.9938, (g) NCC = 0.7836, (h) NCC = 0.9128, (i) NCC = 0.9953, (j) NCC = −0.5185, (k) NCC = 0.9900, and (l) NCC = 0.9906.

Fig. 7. False positive test: (a) watermarked image (PSNR = 33.7433), (b) watermark image, (c) extracted watermark using the original watermark in (b) (NCC = 0.9963), (d) extracted watermark using reference image Woman Hat (NCC = 0.9849), and (e) extracted watermark using reference image Light House (NCC = 0.9857).

Finally, the correlation coefficient is defined as:

$$\begin{aligned}\rho(A,B) &= \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}A_{ij}B_{ij}}{||A||\cdot||B||} \\ &= \frac{\sum_{k=1}^{r}\lambda_k^A\lambda_k^B\sum_{i=1}^{N}u_{ik}u_{ik}\sum_{j=1}^{N}v_{jk}v_{jk}}{\sqrt{\sum_{k=1}^{r}\lambda_k^A\lambda_k^A}\sqrt{\sum_{k=1}^{r}\lambda_k^B\lambda_k^B}\sum_{i=1}^{N}u_{ik}u_{ik}\sum_{j=1}^{N}v_{jk}v_{jk}} \\ &= \frac{\sum_{k=1}^{r}\lambda_k^A\lambda_k^B}{\sqrt{\sum_{k=1}^{r}\lambda_k^A\lambda_k^A}\sqrt{\sum_{k=1}^{r}\lambda_k^B\lambda_k^B}} = \rho(\Sigma_A,\Sigma_B)\end{aligned} \tag{22}$$

The correlation coefficient between A and B is equal to the correlation coefficient between Σ_A and Σ_B. When the diagonal matrices of Σ_A and Σ_B are slightly different, the $\rho(\Sigma_A,\Sigma_B)\approx 1$. The condition $A\approx B$ reveals that the two matrices are highly correlated. Thus, the matrices W_f and W_{wf} are slightly different when the side information (U_w and V_w) is identical and diagonal matrix is slightly different. Fig. 8 shows the effect of changing singular value matrix in Parrots image. From this figure, we can see that the reconstructed image by changing the singular value matrix yields the similar appearance. The difference is only on the image brightness. Fig. 9 shows the NCC values of these images. It can be seen that the NCC value is still very high when the singular value matrix is replaced with the singular value matrix from the other image.

4. Proposed SVD-based image watermarking

In this section, a new SVD-based image watermarking is proposed. The host image is firstly decomposed using the DWT into four sub-bands. The LL sub-band is divided into several non-overlapping image blocks in which SVD is subsequently applied for each image block. The watermark information is embedded into

Table 1
Security attack on the SVD-based image watermarking.

Method	Type of transform	Embedding sub-bands	Perform SVD on Watermark	Size of host image	Size of watermark	Type of watermark	Security attack in [9]	Watermark false positive problem
[11]	Redundant DWT + SVD	All	No	512×512	512×512	Grayscale	Yes	No
[12]	SVD	No	No	256×256	32×32	Grayscale	Yes	No
[13]	DWT + SVD	HH, HL, LH	No	352×288 (video)	198×54 108×33 66×18 144×42 84×24 54×12	Binary	Yes	No
[14]	SVD	No	No	256×256	64×64	Grayscale	Yes	No
[15]	DWT + SVD	LH, HL	No	256×256	128×128	Grayscale	Yes	No
[16]	SVD	No	No	256×256	32×32	Grayscale	Yes	No
[17]	SVD	No	No	–	–	–	Yes	No
[18]	SVD	No	No	-(audio)	256×256	Grayscale	Yes	No
[19]	DCT + SVD	–	No	512×512	64×64	Grayscale	Yes	No
[20]	DWT + SVD	LL, HH	No	512×512	64×64	Grayscale Binary	Yes	No
[21]	Finite radon transform + DWT + SVD	All, LH and HL	Yes	257×257	33×33	Binary	No	Yes
[22]	DWT + SVD	All	Yes	512×512	256×256	Grayscale	No	Yes
[23]	Chaotic map + Hessenberg decomposition + RDWT + SVD	LL	Yes	256×256	256×256 512×512	Binary + Grayscale	No	Yes
[24]	Fractional dual tree complex wavelet transform + SVD	All	Yes	256×256	64×64	Grayscale	No	Yes
[25]	DWT + SVD	LH	Yes	1024×1024	256×256	Grayscale	No	Yes
[26]	Fractional wavelet packet transform + SVD	All	Yes	512×512	128×128	Grayscale	No	Yes
[27]	Redundant fractional wavelet Transform + SVD	LL	Yes	256×256	256×256	Binary + Grayscale	No	Yes
[28]	Redundant DWT + SVD	All	Yes	512×512	512×512	Grayscale	No	Yes
[29]	DWT + nonnegative matrix factorization + SVD	LL, HH	Yes	512×512	64×64	Grayscale	No	Yes
[30]	Fractional wavelet packet transform + SVD	Whole image	Yes	256×256	64×64	Grayscale	No	Yes
[31]	DWT + SVD	LL	Yes	256×256	64×64	Grayscale	No	Yes
Proposed	DWT + SVD (DWT + FFT) (DWT + DCT) (DWT + DWHT) (FFT,DCT,DWHT)	LL	Yes	512×512	64×64 256×256 1024×1024	Grayscale	No	No

the LL image block of the host image by modifying the largest singular value of each image block. Formally, the watermark embedding with the DWT–SVD scheme is as follows.

4.1. Watermark embedding

Let A be a grayscale host image of size $M \times M$, and W be the visual grayscale watermark of size $N \times N$. The watermark size is chosen smaller than the host image size. Before the embedding process, the watermark image is decomposed using the SSVD. The proposed method embeds the watermark principal component into the host image singular value by employing a scaling factor. The scaling factor plays an important role to control the robustness and watermark imperceptibility. The robust watermarking scheme can be achieved by selecting a high scaling factor, causing the watermark is more perceivable by human vision. In contrast, selecting a lower value of scaling factor yields a better image quality, yet it is less robust against some common image manipulations and geometric distortions. Fig. 10 shows the schematic diagram of the proposed watermark embedding scheme introduced as follows.

E1. Perform the SSVD on the watermark image of size $N \times N$ as

$$W \xrightarrow{SSVD} U_w \Sigma_w V_w^T. \tag{23}$$

E2. Obtain the watermark principal component by

$$W_{U\Sigma} \Leftarrow U_w \Sigma_w. \tag{24}$$

Without losing generality, we assume that the watermark image is a full rank matrix, i.e. $r = N$. Let $W_{\Sigma U}(i,j)$ be the principal component in pixel position (i,j), where $i, j = 1,2,\ldots,N$. Each principal component is associated with a single host image block. The matrix V_w^T should be kept as a key for watermark extraction.

E3. Perform 1-level DWT on the host image A of size $M \times M$ to obtain four sub-bands

$$\Im\{A\} \Rightarrow \{A^\theta\}_{\forall\theta}; \theta = (LL, HL, LH, HH), \tag{25}$$

where $\Im\{\cdot\}$ denotes the DWT operation. The size of each sub-band is $\frac{M}{2} \times \frac{M}{2}$. Other transformation can be used to substitute the DWT such as Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), Discrete Walsh–Hadamard Transform (DWHT), etc. We may apply the stationary wavelet transform or redundant wavelet transform to achieve a higher watermark embedding capacity.

E4. Divide the LL sub-band into several non-overlapping blocks of size $m \times m$. Let $ll(i,j)$ denotes an image block at position (i,j), where $i, j = 1,2,\ldots,N$. The block size is chosen as $m = \frac{M}{2N}$.

E5. Apply SVD for each image block $ll(i,j)$:

$$ll(i,j) \Rightarrow U \Sigma V^T, \tag{26}$$

where $\Sigma = diag(\lambda_k)$ and $k = 1, 2,\ldots,m$. The largest singular value of the image block (i,j) is denoted as $\lambda_{max}(i,j)$. The watermark principal component is embedded into the host image by modifying the largest singular value. We need to store $\lambda_{\max}(i,j)$ obtained from this step for extracting watermark information in the watermark extraction procedure.

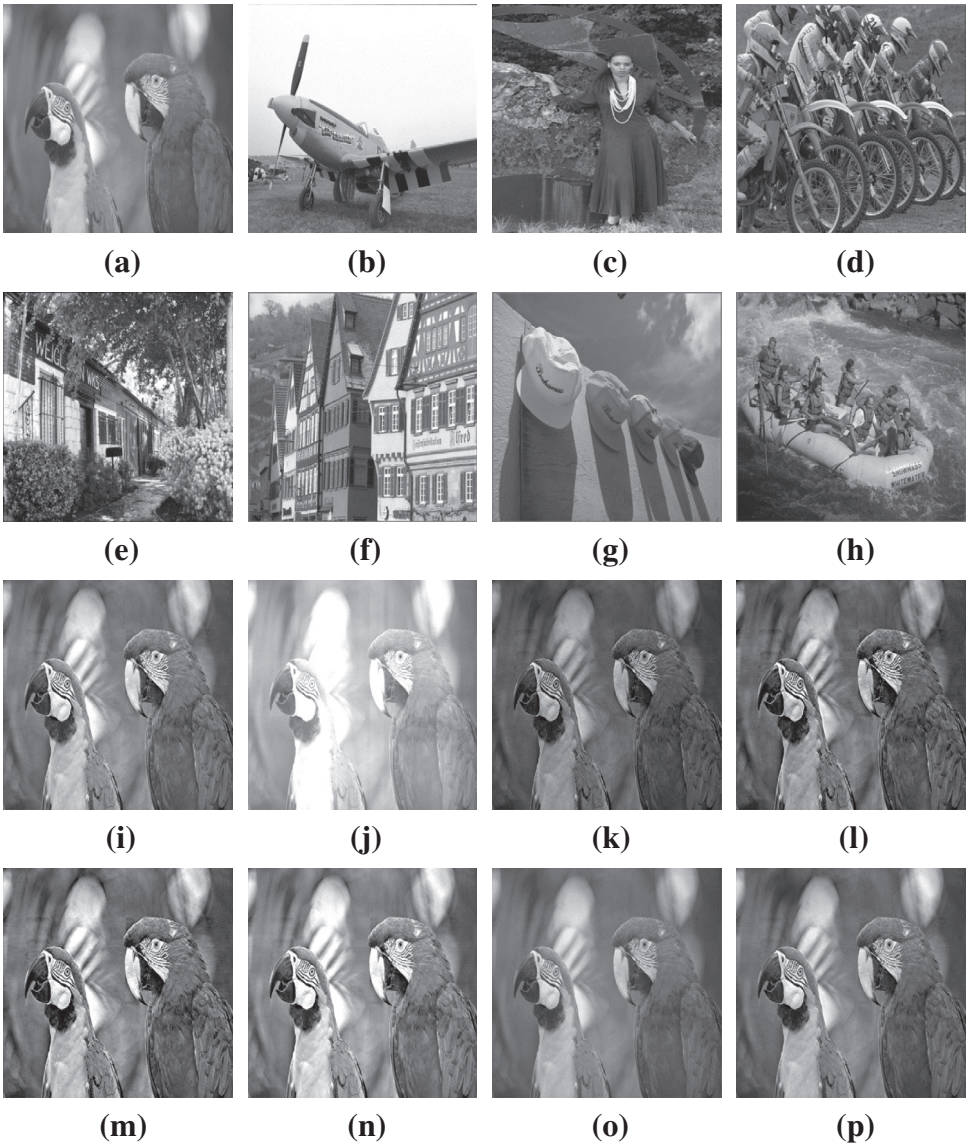

Fig. 8. Effect of changing singular value matrix in Parrots image (a). Figure (i) is reconstructed from U, V of Parrots image and Σ from the average singular value of image (b)–(h). Figures (j)–(p) are obtained from U, V of Parrots image by replacing Σ from the singular value of image (b)–(h). All images are publicly available at [32].

E6. Embed the watermark principal component into the largest singular value of host image for each image block (i,j) using the following formula

$$\lambda^d_{max}(i,j) = \lambda_{max}(i,j) + \alpha W_{\Sigma U}(i,j), \tag{27}$$

where $\lambda^d_{max}(i,j)$ denotes the distorted largest singular value in image block (i,j).

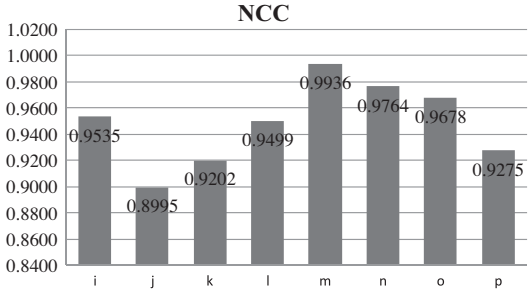

Fig. 9. NCC value from the effect of changing the singular value matrix.

E7. Perform inverse SVD on each image block (i,j) as

$$ll^d(i,j) \Leftarrow U\Sigma^d V^T, \tag{28}$$

where $\Sigma^d = diag(\lambda^d_{max}, \lambda_k)$ for $k = 2,\ldots,m$.

E8. Obtain the distorted LL sub-band image as

$$A^{LL}_d \Leftarrow \{ll^d(i,j)\}. \tag{29}$$

E9. Reconstruct the watermarked image by performing 1-level inverse DWT as

$$A_w \Leftarrow \Im^{-1}\left\{A^{LL}_d, A^{\theta}\right\}, \tag{30}$$

where θ = (HL, LH, HH).

4.2. Watermark extraction

In the watermark extraction, the proposed SVD scheme extracts the watermark W^* from the possibly corrupted watermarked image A^*_w. Some common image processing attacks and geometric

distortions may degrade the watermarked image quality. Fig. 11 shows the schematic diagram of the proposed watermark extraction scheme. By employing the $\lambda_{max}(i,j)$ value obtained from the watermark embedding Step E5 as side information and V_w^T as a key, the watermark extraction step can be formally defined as follow:

X1. Apply 1-level DWT on the possibly corrupted watermarked image as

$$\{A_w^*\} \Rightarrow A_w^{\theta *}, \tag{31}$$

where θ = (LL, HL, LH, HH).

X2. Divide the LL sub-band into several non-overlapping image blocks of size $m \times m$ which are later denoted as $ll^*(i,j)$ where $i, j = 1, 2, \ldots, N$.

X3. Apply the SVD for each image block $ll^*(i,j)$ as

$$ll^*(i,j) \Rightarrow U^* \Sigma^* V^{*T}, \tag{32}$$

where $\Sigma^* = diag(\lambda_k^*)$, and $k = 1, 2, \ldots, m$. The λ_k^* and $\lambda_{max}^*(i,j)$ represent the singular value and the largest singular value for each block, respectively.

X4. Obtain corrupted principal component as

$$W_{\Sigma U}^*(i,j) = \frac{1}{\alpha}(\lambda_{max}^*(i,j) - \lambda_{max}(i,j)). \tag{33}$$

X5. Obtain the extracted watermark as:

$$W^* \Leftarrow W_{\Sigma U}^* V_w^T. \tag{34}$$

The other orthogonal transformations can be used to replace the DWT in step E3 such as FFT, DCT, Discrete Walsh–Hadamard Transform (DWHT), etc. The other watermark

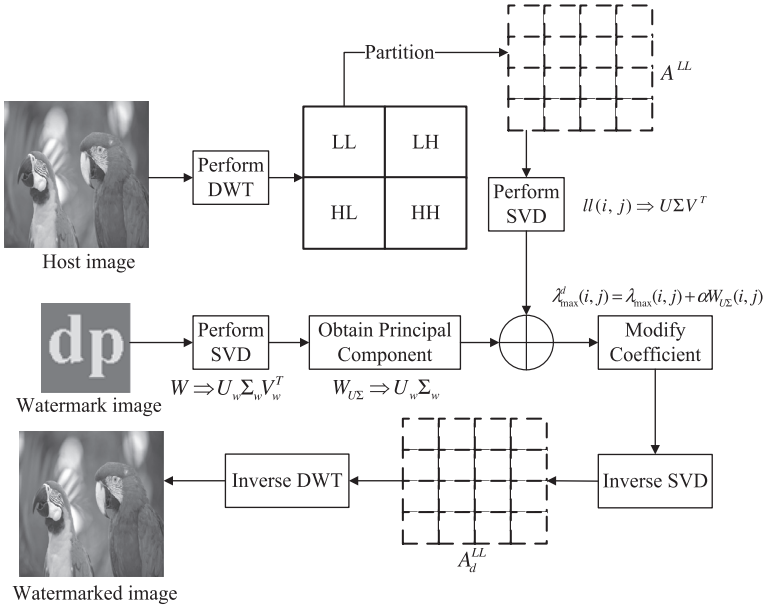

Fig. 10. Flowchart of the proposed watermark embedding.

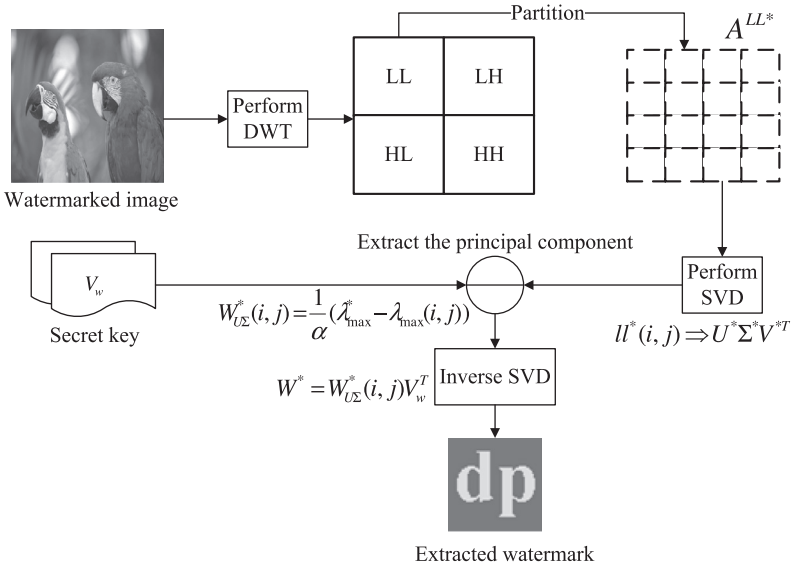

Fig. 11. Flowchart of the proposed watermark extraction.

information such as ΣV^T, U, and V^T can also be inserted into the host image by replacing the watermark principal component $U\Sigma$.

5. Experimental results

In this section, several experiments are conducted to examine the robustness and imperceptibility of the proposed DWT–SVD watermarking. The experiment is carried out using four images, Parrots, Logo, Woman Hat, and Light House, as shown in Fig. 3 [32]. The host and watermark images are grayscale images of size 512×512 and 64×64, respectively. The image block size is set at 4×4 for embedding purpose. The quality of the watermarked image and extracted watermark are objectively measured in terms of the PSNR and NCC, respectively. The PSNR value indicates similarity between the host image and the watermarked version, while NCC verifies the presence of watermark.

5.1. Imperceptibility and robustness test

An experiment is conducted to investigate the imperceptibility and robustness of the proposed SVD-based watermarking scheme. The Parrots and Logo images are adopted as the host and watermark images, respectively, as shown in Fig. 12(a) and (b). In this experiment, the permutation operator for the SSVD is chosen as identity operator, i.e. $W = S(W)$. The scaling factor is set as $\alpha = 0.5$. The watermark principal component $W_{U\Sigma}$ is inserted into the largest singular value of the host image in block based manner. Fig. 12(c) shows the watermarked image with PSNR = 31.3530, indicating that the presence of watermark cannot be easily observed by human vision. Fig. 12(d) shows the extracted watermark image with NCC = 0.9961. The original watermark and extracted watermark are almost identical by considering its high NCC value.

Fig. 13 shows some common image manipulations and geometric distortions for the watermarked image. Fig. 14 shows

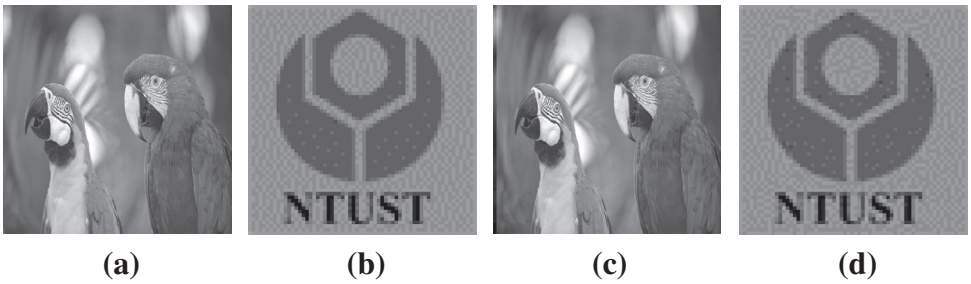

Fig. 12. Imperceptibility of the proposed SVD-based image watermarking. (a) Host image, (b) watermark image, (c) watermarked image (PSNR = 31.3530), and (d) extracted watermark (NCC = 0.9961).

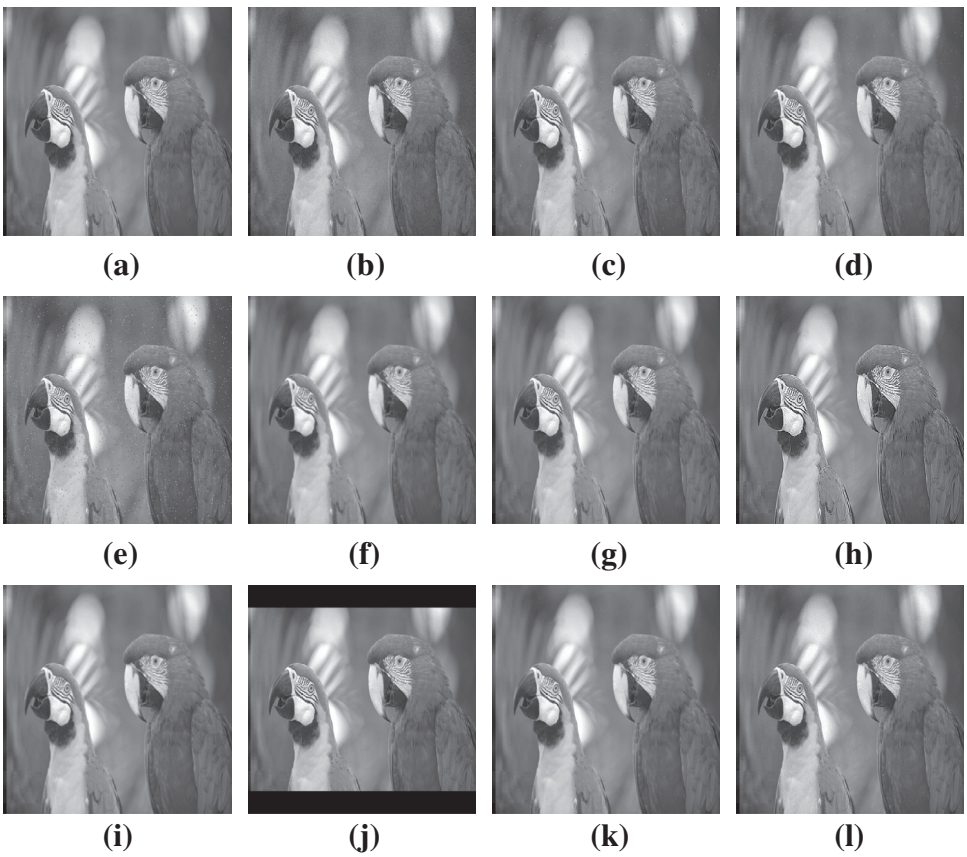

Fig. 13. Robustness of the proposed SVD-based image watermarking under various attacks. The attacks (a)–(l) are the same as in Fig. 5.

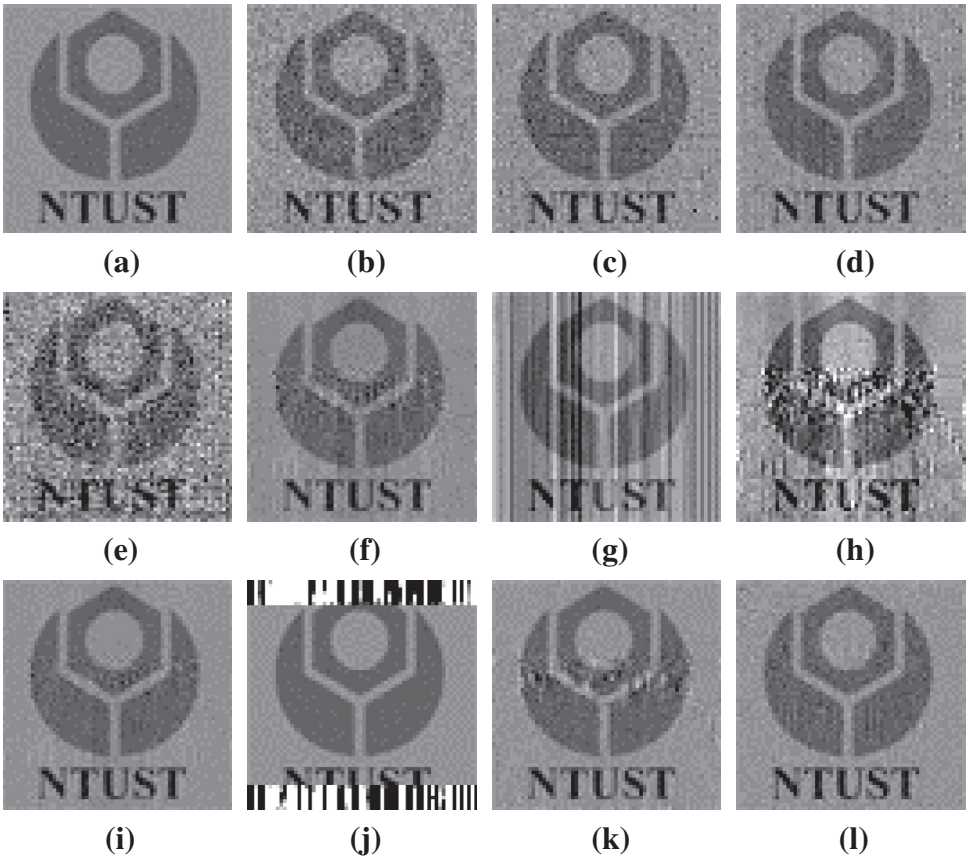

Fig. 14. Extracted watermark from Fig. 13(a)–(l): (a) NCC = 0.9886, (b) NCC = 0.8659, (c) NCC = 0.9020, (d) NCC = 0.9231, (e) NCC = 0.6717, (f) NCC = 0.9278, (g) NCC = 0.7080, (h) NCC = 0.7500, (i) NCC = 0.9710, (j) NCC = 0.4266, (k) NCC = 0.9395, and (l) NCC = 0.9615.

the extracted watermarks and the corresponding NCC values. It can be seen that the extracted watermarks are still recognizable after some attacks are involved in the watermarked image. The imperceptibility and robustness test for the proposed SVD-based image watermarking scheme is reported in Table 2. The proposed method embeds the watermark principal component ($W_{U\Sigma}$, $W_{\Sigma V^T}$) or its key/eigenvector (U, V^T) into the host image by employing specific scaling factor as indicated in Table 2. Based on this result, a conclusion can be made that the proposed SVD-based image watermarking is robust against various attacks and can resist from malicious distortions. The high PSNR of the proposed SVD-based image watermarking implies that the presence of the watermark cannot be perceived by human vision.

Table 2
Imperceptibility and robustness test of the proposed SVD-based image watermarking.

Embedded information	$W_{U\Sigma}$	$W_{\Sigma V^T}$	W_U	W_V
Scaling factor, α	0.5	0.5	450	450
PSNR	31.3530	31.4518	31.2018	31.2277
Attack 1	0.9886	0.9680	0.9903	0.9886
Attack 2	0.8647	0.8452	0.8968	0.8723
Attack 3	0.8912	0.8772	0.9232	0.8916
Attack 4	0.9256	0.9016	0.9563	0.9012
Attack 5	0.6883	0.6607	0.7707	0.7194
Attack 6	0.9278	0.9045	0.9752	0.9793
Attack 7	0.7080	0.6896	0.9476	0.9551
Attack 8	0.7500	0.6692	0.8760	0.9172
Attack 9	0.9710	0.9457	0.9901	0.9882
Attack 10	0.4266	0.4562	0.5574	0.7217
Attack 11	0.9395	0.9181	0.9837	0.9773
Attack 12	0.9603	0.9396	0.9713	0.9698
Average NCC	0.8368	0.8146	0.9032	0.9068

The false positive test is also conducted for the proposed SVD-based image watermarking. Fig. 15(a) and (b) show the watermarked image and the original watermark, respectively. The proposed method can effectively embed the watermark with a high PSNR value, i.e. 31.3530. In the watermark extraction stage, the proposed method can retrieve the watermark with a very high NCC value, i.e. 0.9961. The false positive test is conducted by changing the key V_w^T from Logo image with other images, i.e. Woman Hat and Light House. By changing the key V_w^T, one cannot obtain the correct watermark as shown in Fig. 15(d) and (e) with the NCC value 0.3375 and 0.0487, respectively. From this result, it can be seen that the proposed SVD-based watermarking scheme can avoid the false positive problem which is normally occurred in the SVD-based image watermarking [21–31].

5.2. Embedding watermark in lower rank representation

Another experiment was carried out to embed the watermarks of greater sizes. In this experiment, we choose the watermarks of sizes 256×256 and 1024×1024. Before the embedding process, the SSVD is applied on the watermark and then obtain the new representation with ranks 16 and 4, respectively. The scaling factor for image of 256×256 is set at $\alpha = 0.35$, while $\alpha = 0.1$is used for image of size 1024×1024. Fig. 16 shows the comparative study between the watermarked image using SVD and SSVD. The result of embedding watermark in the lower rank representation using SVD is given in Fig. 16(a) yielding PSNR = 22.6054, while the SSVD yielding PSNR = 22.5948 as shown in Fig. 16(c). The extracted watermark from SVD and SSVD are with NCC = 0.9525 and NCC = 0.9571, respectively. The SSVD offers a better extracted watermark compared to that of the SVD. The result from SSVD is

Fig. 15. False positive test of the proposed SVD-based image watermarking. (a) Watermarked image (PSNR = 31.3530), (b) watermark image, (c) extracted watermark (NCC = 0.9961), (d) extracted watermark using Woman Hat image reference (NCC = 0.3375), and (e) extracted watermark using Light House image reference (NCC = 0.0487).

Fig. 16. Result of the watermark embedding in lower rank representation. Using SVD: (a) watermarked image (PSNR = 22.6054) and (b) extracted watermark (NCC = 0.9525). Using SSVD: (c) watermarked image (PSNR = 22.5948), and (d) extracted watermark (NCC = 0.9571).

Table 3
Imperceptibility and robustness test for lower rank watermark.

Method	Image size = 256 × 256		Image size = 1024 × 1024	
	SVD	SSVD	SVD	SSVD
Scaling factor	0.35	0.35	0.1	0.1
PSNR	22.6054	22.5948	21.3750	21.3118
Attack 1	0.9515	0.9563	0.8428	0.9297
Attack 2	0.9220	0.9299	0.8250	0.9150
Attack 3	0.9262	0.9306	0.8291	0.9164
Attack 4	0.9403	0.9451	0.8343	0.9223
Attack 5	0.8577	0.8685	0.7802	0.8737
Attack 6	0.9307	0.9413	0.8308	0.9222
Attack 7	0.9093	0.9084	0.8037	0.8941
Attack 8	0.8858	0.8866	0.7648	0.8597
Attack 9	0.9418	0.9501	0.8377	0.9269
Attack 10	0.4139	0.4998	0.4221	0.5253
Attack 11	0.9449	0.9496	0.8378	0.9258
Attack 12	0.9474	0.9521	0.8402	0.9276
Average NCC	0.8810	0.8932	0.7874	0.8782

much better and acceptable for human vision as shown in Fig. 16(d). The robustness and imperceptibility of the proposed SVD-based image watermarking using low rank representation are tabulated in Table 3. It can be seen that the SSVD is more robust compared to that of the SVD under the same scaling factor. The proposed method is able to embed the watermark with a higher capacity by transforming the watermark into another image representation with a lower rank.

5.3. Embedding watermark into another orthogonal transformation

In this sub-section, we make some comparative study by embedding the watermark principal component ($U\Sigma$ and ΣV^T) or eigenvector/watermark extraction key (U and V). The watermark information is embedded into the host image by modifying the LL sub-band in the block based manner. The image block is firstly decomposed using the orthogonal transformation such as FFT, DCT, and Discrete Walsh Hadamard Transform (DWHT). The SVD operation in Step (E5) of watermark embedding is replaced with the orthogonal transformation FFT, DCT, and DWHT. Consequently, the SVD computation in Step (X3) of watermark extraction is also substituted with the corresponding orthogonal transformation used in watermark embedding stage. Tables 4–6 show the imperceptibility and robustness test for the proposed SVD-based image watermarking scheme using orthogonal image transformation. From this method, we can see that the proposed method still performs well without worrying about the false positive problem in the SVD part.

Another experiment was also conducted using the spread spectrum concept [1], in which the watermark principal component is embedded into the transformed coefficients of the host image. The watermark information is inserted into a set of coefficients after the orthogonal transformation (FFT, DCT, DWHT). The watermark embedding is simply performed using $F'(i,j) = F(i,j) + \alpha W_{U\Sigma}(i,j)$ in the block based manner. The $F(i,j)$ and $F'(i,j)$ denote the original and modified specific coefficients in the transformed domain, respectively. For the FFT and DCT, the watermark principal component is injected in the DC component. While the DWHT hides the watermark principal component in its first coefficient, i.e. $D_{WH}(0,0)$. Tables 7–9 show the imperceptibility and robustness test for the proposed watermarking scheme with the spread spectrum concept. Using this scheme, one can guarantee the free of false positive problem. Based on the results recorded in these tables, we can conclude that the proposed SVD-based watermarking scheme is very suited for hiding the watermark information in the spread spectrum domain.

5.4. Comparison with former reliable SVD-based watermarking

In this experiment, the performance of the proposed method is compared with the former reliable SVD-based watermarking scheme [10]. The method in [10] embeds the watermark principal component $W_{U\Sigma}$ into the singular value matrix of host image by

Table 4
Imperceptibility and robustness test for FFT block based.

Embedded information	$W_{U\Sigma}$	$W_{\Sigma V^T}$	W_U	W_V
Scaling factor, α	2	2	1800	1800
PSNR	31.3661	31.4553	31.1985	31.2217
Attack 1	0.9861	0.9664	0.9811	0.9835
Attack 2	0.8658	0.8369	0.8715	0.8673
Attack 3	0.8982	0.8801	0.9342	0.9288
Attack 4	0.9341	0.9127	0.9362	0.9625
Attack 5	0.7064	0.7033	0.7117	0.7103
Attack 6	0.9382	0.9215	0.9709	0.9765
Attack 7	0.7038	0.6866	0.9394	0.9496
Attack 8	0.7591	0.6841	0.8872	0.9171
Attack 9	0.9738	0.9536	0.9852	0.9830
Attack 10	0.4229	0.4527	0.5446	0.7189
Attack 11	0.9345	0.9144	0.9779	0.9723
Attack 12	0.9593	0.9404	0.9665	0.9712
Average NCC	0.8402	0.8210	0.8922	0.9118

Table 5
Imperceptibility and robustness test for DCT block based.

Embedded information	$W_{U\Sigma}$	$W_{\Sigma V^T}$	W_U	W_V
Scaling factor, α	0.4	0.4	350	350
PSNR	33.2875	33.2911	33.3727	33.3948
Attack 1	0.9816	0.9780	0.9734	0.9657
Attack 2	0.8135	0.8009	0.7994	0.8047
Attack 3	0.8624	0.8642	0.9019	0.8762
Attack 4	0.9030	0.8917	0.9089	0.8995
Attack 5	0.6186	0.6295	0.6395	0.5803
Attack 6	0.9151	0.9151	0.9582	0.9593
Attack 7	0.6227	0.6193	0.8890	0.9174
Attack 8	0.7101	0.6487	0.8524	0.8984
Attack 9	0.9637	0.9602	0.9685	0.9644
Attack 10	0.4223	0.4515	0.5408	0.7150
Attack 11	0.9065	0.9017	0.9476	0.9430
Attack 12	0.9420	0.9357	0.9478	0.9366
Average NCC	0.8051	0.7997	0.8606	0.8717

Table 6
Imperceptibility and robustness test for DWHT block based.

Embedded information	$W_{U\Sigma}$	$W_{\Sigma V^T}$	W_U	W_V
Scaling factor, α	0.1	0.1	90	90
PSNR	33.2875	33.2911	33.1327	33.1411
Attack 1	0.9816	0.9780	0.9760	0.9736
Attack 2	0.8161	0.8087	0.8250	0.8318
Attack 3	0.8555	0.8738	0.9038	0.9188
Attack 4	0.9002	0.8939	0.9234	0.8733
Attack 5	0.6389	0.6258	0.6786	0.7172
Attack 6	0.9151	0.9151	0.9633	0.9689
Attack 7	0.6227	0.6193	0.9067	0.9134
Attack 8	0.7101	0.6487	0.8668	0.9138
Attack 9	0.9637	0.9602	0.9720	0.9769
Attack 10	0.4223	0.4515	0.5502	0.7240
Attack 11	0.9065	0.9017	0.9605	0.9659
Attack 12	0.9394	0.9334	0.9579	0.9601
Average NCC	0.8060	0.8008	0.8737	0.8948

utilizing a suited scaling factor. The false positive problem of SVD-based image watermarking can be solved using this approach. However, this approach is less robust against malicious attacks and geometrical distortions. The reliable SVD-based watermarking [10] needs the original host image A and the inverse matrix computation (U^{-1} and $(V^T)^{-1}$) to extract the watermark from the possibly corrupted watermarked image. This disadvantage increases the computational burden and storage requirement in the watermark

Table 7
Imperceptibility and robustness test for FFT spread spectrum.

Embedded information	$W_{U\Sigma}$	$W_{\Sigma V^T}$	W_U	W_V
Scaling factor, α	2	2	1800	1800
PSNR	37.3562	37.3331	37.1951	37.2046
Attack 1	0.9568	0.9588	0.9245	0.9463
Attack 2	0.6752	0.6565	0.6233	0.6861
Attack 3	0.7383	0.7286	0.7753	0.7710
Attack 4	0.8024	0.8047	0.7507	0.7368
Attack 5	0.4445	0.4367	0.4644	0.3802
Attack 6	0.8365	0.8419	0.9110	0.9305
Attack 7	0.4436	0.4366	0.7444	0.7973
Attack 8	0.5780	0.5249	0.8294	0.8788
Attack 9	0.9246	0.9251	0.9205	0.9412
Attack 10	0.4200	0.4521	0.5421	0.7124
Attack 11	0.8085	0.8082	0.9038	0.9242
Attack 12	0.8701	0.8666	0.8626	0.8941
Average NCC	0.7082	0.7034	0.7710	0.7999

Table 8
Imperceptibility and robustness test for DCT spread spectrum.

Embedded information	$W_{U\Sigma}$	$W_{\Sigma V^T}$	W_U	W_V
Scaling factor, α	0.4	0.4	350	350
PSNR	33.2875	33.2911	33.3727	33.3948
Attack 1	0.9816	0.9780	0.9734	0.9657
Attack 2	0.8162	0.8034	0.7745	0.8137
Attack 3	0.8582	0.8759	0.8961	0.8921
Attack 4	0.8982	0.8927	0.8831	0.8442
Attack 5	0.6305	0.6215	0.6103	0.6256
Attack 6	0.9151	0.9151	0.9582	0.9593
Attack 7	0.6227	0.6193	0.8890	0.9174
Attack 8	0.7101	0.6487	0.8524	0.8984
Attack 9	0.9637	0.9602	0.9685	0.9644
Attack 10	0.4223	0.4515	0.5408	0.7150
Attack 11	0.9065	0.9017	0.9476	0.9430
Attack 12	0.9408	0.9364	0.9425	0.9225
Average NCC	0.8055	0.8004	0.8530	0.8718

Table 9
Imperceptibility and robustness test for DWHT spread spectrum.

Embedded information	$W_{U\Sigma}$	$W_{\Sigma V^T}$	W_U	W_V
Scaling factor, α	0.1	0.1	90	90
PSNR	27.8225	28.0938	27.1219	27.2723
Attack 1	0.9119	0.7999	0.9942	0.9941
Attack 2	0.8490	0.7272	0.9420	0.9494
Attack 3	0.8798	0.7719	0.9702	0.9817
Attack 4	0.8914	0.7808	0.9656	0.9767
Attack 5	0.7784	0.6698	0.9039	0.8802
Attack 6	0.8818	0.7747	0.9792	0.9770
Attack 7	0.7788	0.6823	0.9778	0.9813
Attack 8	0.7888	0.6542	0.9008	0.9393
Attack 9	0.9000	0.7883	0.9907	0.9869
Attack 10	0.4174	0.4424	0.5573	0.7208
Attack 11	0.8903	0.7774	0.9912	0.9881
Attack 12	0.9005	0.7906	0.9887	0.9882
Average NCC	0.8223	0.7216	0.9301	0.9470

Table 10
Computational time comparison between proposed method and [10].

Method	Proposed method	Reliable SVD-based watermarking [10]
Watermark embedding	0.39 s	1.0764 s
Watermark extraction	0.2496 s	1.3884 s

Table 11
Comparison with the former reliable SVD-based watermarking.

Method	Reliable SVD watermarking [10]	Proposed SVD watermarking
Scaling factor, α	0.5	0.5
PSNR	31.3587	31.3530
Attack 1	0.9811	0.9886
Attack 2	0.8719	0.8647
Attack 3	0.8946	0.8912
Attack 4	0.9382	0.9256
Attack 5	0.6909	0.6883
Attack 6	0.3861	0.9278
Attack 7	0.8453	0.7080
Attack 8	0.3693	0.7500
Attack 9	0.4304	0.9710
Attack 10	0.0950	0.4266
Attack 11	0.5237	0.9395
Attack 12	0.9495	0.9603
Average NCC	0.6647	0.8368

extraction stage. In contrast, the proposed SVD-based image watermarking does not need the original image A matrix and avoids the inverse matrix calculation. The computation time between the reliable SVD-based watermarking and proposed method is compared in Table 10. This experiment was conducted in computer environment with the processor Inter Core 2 Quad CPU @2.40 GHz, and 4 GB RAM. These two watermarking approaches are run in Matlab 7.11.0 (R2010b) with un-optimized program code to make a fair comparison. However, we use the Matlab built-in function for computing the inverse matrix in reliable SVD-based watermarking [10]. From this table, we can see that our proposed method offers faster computation compared to the former method. The reliable SVD-based method [10] consumes more computation time in the watermark extraction stage because of inverse matrix calculation (U^{-1} and $(V^T)^{-1}$).

Table 11 shows the PSNR and NCC value comparison between the proposed method and the former reliable SVD-based watermarking. Both methods employ the same scaling factor to make a fair comparison. The proposed SVD-based watermarking is more robust against various attacks as indicated with the higher average NCC value compared with [10]. The proposed SVD-based watermarking is suitable for protecting the ownership rightful with free of false positive problem and un-ambiguity in extraction procedure.

6. Conclusions

A new SVD-based image watermarking was proposed in this paper. The new method solves the ambiguity situation and false positive problem normally occurred in the SVD-based image watermarking schemes. The proposed method embeds the watermark principal component into the host image in which an attacker cannot obtain the desired watermark image without knowing the correct key (eigenvector) from the original watermark. The proposed method also performs well using the spread spectrum watermarking concept. The proposed watermarking scheme can be extended for the color image, video, or audio for the future works. Other orthogonal transformations can be used to replace the DWT to achieve a higher watermark capacity, and improve the corresponding image quality. The determination of scaling factor can be regarded as an optimization problem which can be iteratively updated according to the image content. Yet, the proposed watermarking method is very useful for protecting the rightful ownership in the consumer electronic devices such as digital camera, image display, image publishing system, electronic document imaging, etc.

References

[1] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process. 6 (12) (1997).
[2] A. Ranade, S.S. Mahabalarao, S. Kale, A variation on SVD based image compression, Image Vision Comput. 25 (6) (2007) 771–777.
[3] R.Z. Liu, T.N. Tan, An SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 4 (1) (2002) 121–128.
[4] X.P. Zhang, K. Li, Comments on an SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 7 (3) (2005) 593–594.
[5] R. Rykaczewski, Comments on SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 9 (2) (2007) 421–423.
[6] X. Changzhen, G. Fenhong, L. Zhengxi, Weakness analysis of singular value based watermarking, in: International Conference on Mechantronics and Automation, 2009, pp. 2596–2601.
[7] X. Changzhen, R.K. Ward, J. Xu, On the security of singular value based watermarking, in: IEEE International Conference on Image Processing, 2008, pp. 437–440.
[8] R.A. Sadek, Blind synthesis attack on SVD based watermarking techniques, in: International Conference on Computational Intelligence for Modeling Control and Automation, 2008, pp. 140–145.
[9] J.M. Guo, H. Prasetyo, Security attack on the wavelet transform and singular value decomposition image watermarking, in: IEEE International Symposium Consumer Electronics, 2013, pp. 217–218.
[10] C. Jain, S. Arora, P.K. Panigrahi, A reliable SVD based watermarking scheme, 2008, <http://adsabs.harvard.edu/abs/2008arXiv0808.0309J>.
[11] N.M. Makbol, B.E. Khoo, Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition, AEU Int. J. Electron. Commun. 67 (2) (2013) 102–112.
[12] V. Aslantas, A singular-value decomposition-based image watermarking using genetic algorithm, AEU Int. J. Electron. Commun. 62 (5) (2008) 386–394.
[13] O.S. Faragallah, Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain, AEU Int. J. Electron. Commun. 67 (3) (2013) 189–196.
[14] C.C. Lai, A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm, Digital Signal Process. 21 (4) (2011) 522–527.
[15] C.C. Lai, C.C. Tsai, Digital image watermarking using discrete wavelet transform and singular value decomposition, IEEE Trans. Inst. Measure. 59 (11) (2010) 3060–3063.
[16] V. Aslantas, An optimal robust digital image watermarking based on SVD using differential evolution algorithm, Opt. Commun. 282 (5) (2009) 769–777.
[17] S. Dogan, T. Tuncer, E. Avci, A. Gulten, A robust color image watermarking with singular value decomposition method, Adv. Eng. Software 42 (6) (2011) 336–346.
[18] W. Al-Nuaimy et al., An SVD audio watermarking approach using chaotic encrypted images, Digital Signal Process. 21 (2011) 764–779.
[19] M. Ali, C.W. Ahn, M. Pant, A robust image watermarking technique using SVD and differential evolution in DCT domain, Opt. Int. J. Light Electron. Opt. (2013), http://dx.doi.org/10.1016/j.ijleo.2013.06.082.
[20] M. Ali, C.W. Ahn, P. Siarry, Differential evolution algorithm for the selection of optimal scaling factors in image watermarking, Eng. Appl. Artif. Intel. (2013), http://dx.doi.org/10.1016/j.engappai.2013.07.009.
[21] S. Rastegar, F. Namazi, K. Yaghmaie, A. Aliabadian, Hybrid watermarking based on singular value decomposition and Radon transform, AEU Int. J. Electron. Commun. 65 (7) (2011) 658–663.
[22] E. Ganic, A.M. Eskicioglu, Robust embedding of visual watermarks using DWT–SVD, J. Electron. Imaging 14 (4) (2005) 043004.
[23] G. Bhatnagar, A new facet in robust digital watermarking framework, AEU Int. J. Electron. Commun. 66 (4) (2012) 275–285.
[24] G. Bhatnagar, Q.M.J. Wu, Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform, Future Gener. Comput. Syst. 29 (1) (2013) 182–195.
[25] C. Song, S. Sudirman, M. Merabti, A robust region-adaptive dual image watermarking technique, J. Visual Commun. Image Representation 23 (3) (2012) 549–568.
[26] G. Bhatnagar, Q.M.J. Wu, B. Raman, A new robust adjustable logo watermarking scheme, Comput. Secur. 31 (1) (2012) 40–58.
[27] G. Bhatnagar, Q.M.J. Wu, A new logo watermarking based on redundant fractional wavelet transform, Math. Comput. Model. 58 (1–2) (2013) 204–218.
[28] S. Lagzian, M. Soryani, M. Fathy, Robust watermarking scheme based in RDWT–SVD: embedding data in all subbands, in: International Symposium on Artificial Intelligent and Signal Processing, 2011, pp. 48–52.
[29] M. Ouhsain, A.B. Hamza, Image watermarking scheme using nonnegative matrix factorization and wavelet transform, Expert Syst. Appl. 36 (2) (2009) 2123–2129.
[30] G. Bhatnagar, B. Raman, Q.M.J. Wu, Robust watermarking using fractional wavelet packet transform, IET Image Process. 6 (4) (2012) 386–397.
[31] E. Yen, L.H. Lin, Rubik's cube watermarking technology for grayscale images, Expert Syst. Appl. 37 (6) (2010) 4033–4039.
[32] H.R. Sheikh, Z. Wang, L. Cormack, A.C. Bovik, LIVE Image Quality Assessment Database Release 2, [Online]. Available: <http://www.live.ece.utexas.edu/research/quality>.

[33] M. Narwaria, W. Lin, SVD-based quality metric for image and video using machine learning, IEEE Trans. Syst. Man Cybern. B Cybern. 42 (2) (2012) 347–364.
[34] S.C. Huang, An advanced motion detection algorithm with video quality analysis for video surveillance systems, IEEE Trans. Circuits Syst. Video Technol. 21 (1) (2011) 1–14.
[35] S.C. Huang, F.C. Cheng, Y.S. Chiu, Efficient contrast enhancement using adaptive gamma correction with weighting distribution, IEEE Trans. Image Process. 9 (1) (2013) 1032–1041.
[36] J.M. Guo, Y.F. Liu, Hiding multitone watermarks in halftone images, IEEE Multimedia 17 (1) (2010) 34–43.
[37] J.M. Guo, Y.F. Liu, Joint compression/watermarking scheme using majority-parity guidance and halftoning-based block truncation coding, IEEE Trans. Image Process. 19 (8) (2010) 2056–2069.
[38] J.M. Guo, M.F. Wu, Y.C. Kang, Watermarking in conjugate ordered dither block truncation coding images, Signal Process. 89 (10) (2009) 1864–1882.
[39] J.M. Guo, A new model-based digital halftoning and data hiding designed with LMS optimization, IEEE Trans. Multimedia 9 (4) (2007) 687–700.