J Inf Process Syst, Vol.13, No.6, pp.1585~1601, December 2017
https://doi.org/10.3745/JIPS.03.0086

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Review on Digital Image Watermarking Based on Singular Value Decomposition

Chengyou Wang*, Yunpeng Zhang*, and Xiao Zhou*

Abstract

With the rapid development of computer technologies, a number of image modification methods have emerged, which have great impacts on the security of image information. Therefore, it is necessary to protect the integrity and authenticity of digital images, and digital watermarking technique consequently becomes a research hotspot. An effort is made to survey and analyze advancements of image watermarking algorithms based on singular value decomposition (SVD) in recent years. In the first part, an overview of watermarking techniques is presented and then mathematical theory of SVD is given. Besides, SVD watermarking model, features, and evaluation indexes are demonstrated. Various SVD-based watermarking algorithms, as well as hybrid watermarking algorithms based on SVD and other transforms for copyright protection, tamper detection, location, and recovery are reviewed in the last part.

Keywords

Copyright Protection, Tamper Detection, Digital Image Watermarking, Evaluation Indexes, Singular Value Decomposition (SVD)

1. Introduction

With the tremendous growth in information industry recently, as one of the most essential methods to convey the information from one side to the other, digital images can be spread worldwide. This extremely promotes the information exchange in human's world, but in the meantime, it can consequently result in the security problem with copyright issues. So how to ensure the authenticity and integrity protection of images becomes urgent and important. To solve this problem, digital signature [1,2] and digital watermarking [3] were proposed. Owing to that digital signature depends on embedding much signature information into the carrier, digital watermarking technique, an effective method to solve copyright problems of image contents, was proposed. According to different robustness, digital watermarking can be classified into three categories: (i) robust watermarking used for copyright protection, which can resist all kinds of attacks, (ii) fragile watermarking, which is sensitive to attacks including malicious tamper and common processing, (iii) semi-fragile watermarking used to distinguish malicious tamper from non-malicious modification, which is a combination of advantages in robust and fragile watermarking.

Manuscript received February 13, 2017; first revision April 26, 2017; second revision May 29, 2017; accepted May 30, 2017.
Corresponding Author: Xiao Zhou (zhouxiao@sdu.edu.cn)
* School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai, China (wangchengyou@sdu.edu.cn, zhyp@mail.sdu.edu.cn, zhouxiao@sdu.edu.cn)

Additionally, both fragile watermarking and semi-fragile watermarking can be applied in image tamper detection, location, and recovery. However, considering the ability of resisting the common image operation, robustness of semi-fragile watermarking is better than that of fragile watermarking.

In terms of work domain where the watermark is embedded into the host image, this effective technique is divided into two categories: spatial domain and transform domain [4]. Spatial domain methods modify pixel values of the host image directly for watermark embedding, which have advantages of easy implementation and low computation complexity. However, spatial methods are fragile to the common image processing and malicious attacks. On the contrary, algorithm with watermark information embedded by modifying transform coefficients of the host image is defined as transform domain watermarking. Compared with spatial methods, methods based on different transforms have the better transparency and robustness. The most common transforms applied in transform-based watermarking algorithms are discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD) [5].

In recent years, more and more watermarking algorithms based on SVD have been proposed as a powerful technique for copyright protection, tamper detection, location, and recovery. In fact, SVD becomes the research hotspot owing to three advantages: (i) matrices obtained by SVD is unfixed; (ii) singular values can still remain intact when the image is perturbed; (iii) singular values can represent intrinsic algebraic properties of an image. In this paper, we make a comparative and reviewing study on watermarking algorithms based on SVD. Besides, introductions of SVD theory and watermarking evaluation indexes are made. To help the further research, future challenges are also given in the paper.

The remainder of this survey paper will be listed as follows. Section 2 and Section 3 introduce SVD and features of image watermarking based on SVD used for copyright protection, tamper detection, and self-recovery. Evaluation indexes of watermarking algorithms are described in Section 4. In Section 5, literature review is presented. Conclusions and future challenges are demonstrated finally in Section 6.

2. Overview of SVD and Watermarking Model

SVD is an orthogonal transform used for matrix diagonalization [6]. As Eq. (1) shows, $\boldsymbol{A}$ is an $m \times n$ matrix with rank r. $\boldsymbol{U}$ and $\boldsymbol{V}$ are two orthogonal matrices.

$$\boldsymbol{U}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{V} = \begin{bmatrix} \Sigma & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} \end{bmatrix}, \tag{1}$$

where $\Sigma = \mathrm{diag}\{\sigma_1, \sigma_2, \cdots, \sigma_r\}$ and $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r > 0$. $\sigma_1^2, \sigma_2^2, \cdots, \sigma_r^2$ are positive feature values in the matrix $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$, and the SVD of matrix $\boldsymbol{A}$ can be represented by Eq. (2):

$$\boldsymbol{A} = \boldsymbol{U}\begin{bmatrix} \Sigma & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} \end{bmatrix}\boldsymbol{V}^{\mathrm{T}}. \tag{2}$$

In the matrix analysis, Frobenius norm of $\boldsymbol{A}$ is defined as Eq. (3):

$$\|\boldsymbol{A}\|_{\mathrm{F}}^2 = \mathrm{tr}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}). \tag{3}$$

Referring to the basic matrix theory in Eq. (4), Eq. (5) can be attained.

$$\mathrm{tr}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}) = \mathrm{tr}(\boldsymbol{V}\begin{bmatrix}\Sigma & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}^{\mathrm{T}}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U}\begin{bmatrix}\Sigma & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}\boldsymbol{V}^{\mathrm{T}}) = \mathrm{tr}(\boldsymbol{V}\begin{bmatrix}\Sigma^2 & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}\boldsymbol{V}^{\mathrm{T}}) = \sum_{l=1}^{r}\sigma_l^2 , \tag{4}$$

$$\|\boldsymbol{A}\|_{\mathrm{F}}^2 = \sum_{l=1}^{r}\sigma_l^2 . \tag{5}$$

As Eq. (5) indicates, squared Frobenius norm of matrix should be equal to quadratic sum of all singular values in the matrix. Hence, as for an image, Frobenius norm of the image matrix can be used to measure the image's energy, and main energy of an image concentrates on singular values of larger numerical values. Reserving larger singular values in images, compressed image that mostly reflects the appearance and characters can be obtained. Moreover, losses of energy and information concentrate on the neglected and smaller singular values. Weyl's theorem [7] demonstrates that when perturbation is imposed to images, changes of images' singular values will not exceed the largest singular value in perturbation matrix, which renders that image watermarking algorithm based on SVD possesses remarkable quality of steadiness.

Letter watermark of Shandong University (Weihai) is embedded into the host image Airplane by SVD, which is shown in Fig. 1.

(a) (b) (c)

Fig. 1. Example of SVD-based image watermarking: (a) host image Airplane, (b) letter watermark, and (c) watermarked image Airplane.

In general, basic SVD-based image watermarking algorithm mainly includes two stages: embedding and extraction, as shown in Fig. 2. In the embedding stage, encrypted watermark information is embedded into the original host image decomposed by SVD. The inverse operation is performed in the extraction stage to extract the watermark. According to different purposes, robustness test, tamper detection, and self-recovery can be realized by using the extracted watermark after extraction stage.

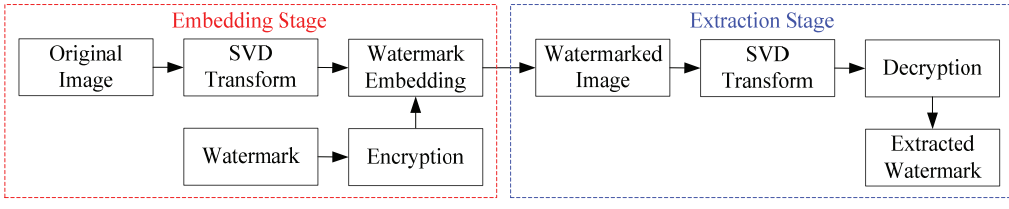


Fig. 2. Diagram of SVD-based image watermarking algorithm.

3. Features of Image Watermarking Based on SVD

According to different watermarking applications, there are different specific features and requirements. Actually, there is no one kind of watermarking that can meet all requirements [8]. To help us make a complete and profound study, features of SVD-based image watermarking are given as follows.

3.1 Perceptual Transparency

In application, the embedded watermark should be transparent, which means that it cannot be recognized and distinguished from the original image by the naked eye. Furthermore, better perceptual transparency leads to better security of watermarked image. However, in the meantime, watermark should not affect or degrade the quality greatly of the original data in most application. Under above premises, watermarks are embedded into host images in watermarking algorithms.

3.2 Security

Watermark information should be secure and difficult for tampering and forging. For this purpose, watermark information is usually encrypted before being embedded into original image to promote the watermark security. The frequently used encryption methods include logistic map [9], cat map, also known as Arnold transform [10], block mapping function [11], etc. Besides, false detection rate in fragile and semi-fragile watermarking algorithms should be low. That is to say, when original image is modified, the digital watermark should be altered consistently, and detection on the modification of the original data can be implemented accordingly.

3.3 Watermark Payload

The application of watermarking algorithm decides the amount of information stored in the watermark [3]. Watermark payload is the maximum amount of information hidden in the host image. It depends on statistical character, distortion limit of the host image, and is related to the robustness and transparency of watermarking algorithms. The purpose of discussing payload is to analyze the upper bound of embedded watermark information content with satisfying requirements of perceptual transparency and robustness.

3.4 Blind Detection

Contrary to the non-blind watermarking algorithm which needs original image to extract the watermark from the host image, blind watermarking algorithm was proposed to extract the watermark without the assistance of original image. It only needs the watermarked image in the watermark extraction, which makes blind watermarking algorithms more practical in application.

3.5 Robustness

Robustness means that even though watermarked data is destroyed, the watermark can be extracted. According to different watermarking types illustrated previously, different watermarking algorithms should have different degrees of robustness.

3.5.1 Robust watermarking

As illustrated in Section 1, robust watermarking can resist all kinds of attacks containing general attacks and geometric attacks. As for general attacks, factors can be JPEG compression, filtering (median filtering, average filtering, etc.), noise addition (Gaussian noise, salt and pepper noise, speckle noise, etc.), cropping, resampling, digital-to-analogue conversion, analogue-to-digital conversion, etc. However, geometric attacks contain rotation, scaling, and translation (RST) [12] modification on images.

Attacks demonstrated above will degrade the image in some degrees, and robust watermarking algorithms should be robust enough to resist these attacks.

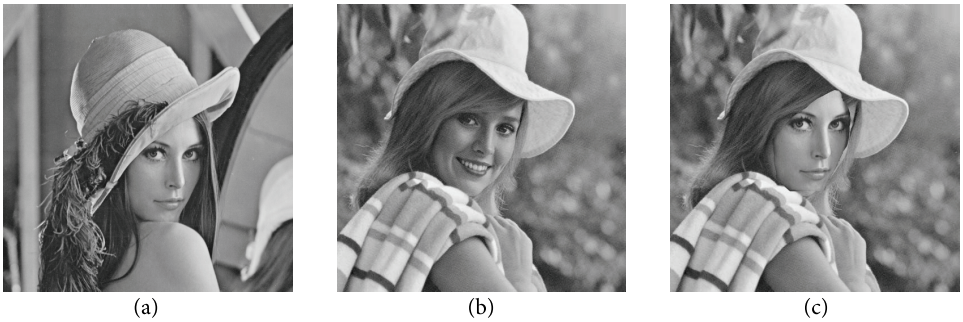
3.5.2 Fragile and semi-fragile watermarking

Different from robust watermarking, fragile and semi-fragile watermarking should be sensitive to some attacks according to their different functions, and factors resulting in destruction can be classified into two types: unintentional modification and intentional modification. The unintentional modification is mainly common image processing. Especially in the semi-fragile watermarking, the embedded watermark should be robust to unintentional modification and sensitive to intentional modification which contains general attacks and special attacks [13].

In general, deletion attack, copy-move, and drawing are considered as general attacks [13]. To be more detailed, deletion attack is to delete the part of an image arbitrarily. Copy-move tamper is to copy a part of one image and paste it to another region of this image, which is intended to create a false impression or hide information. The drawing attack means that the image is painted by using the drawing tool, leaving the image covered partially by the drawing, which causes the loss of the watermarked image information.

Different from general attacks, special attacks are more difficult to be detected by the watermarking algorithms. The main special attacks are given as follows.

(1) Collage attack (CA): Holliman and Memon [14] firstly proposed collage attack, which is a special circumstance that part of image is substituted for counterfeiting purpose. It mostly appears in the watermarking techniques based on blocks. The basic idea of collage attack is that combining regions in different images while preserving their relative spatial location within the image to counterfeit a new image from multiple authenticated images [15]. As is shown in Fig. 3, two standard grayscale images Lena and Elaine with size of 512×512 are utilized, and collage attack is shown by replacing the watermarked Elaine with a specific region of the watermarked Lena at the same coordinate location in Fig. 3(c).

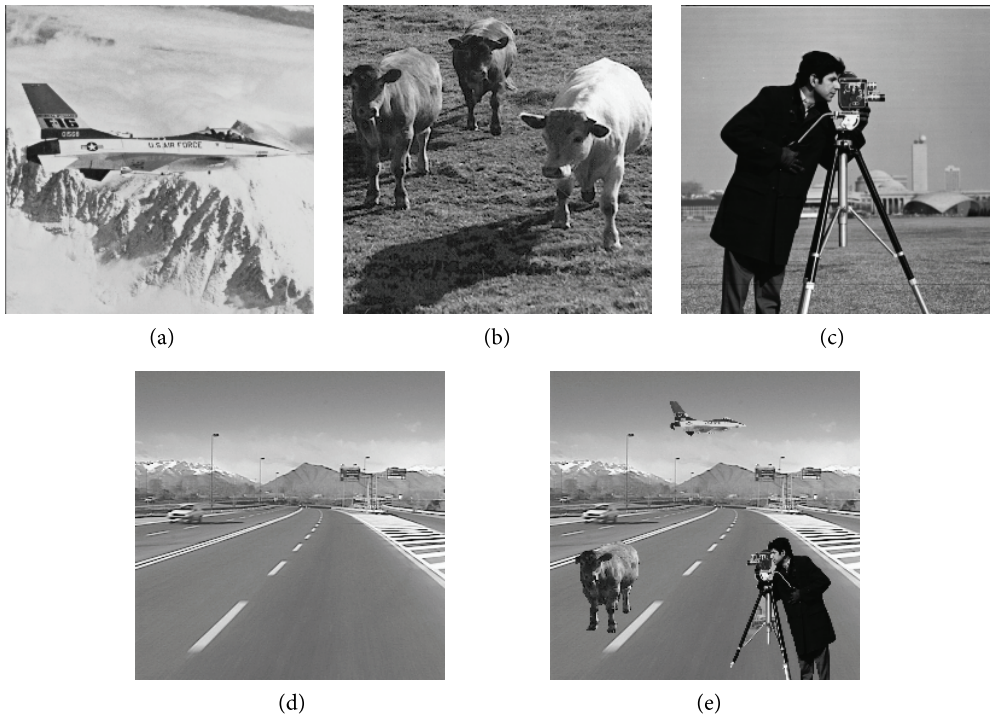


(a) (b) (c)

Fig. 3. CA tamper: (a) watermarked Lena image, (b) watermarked Elaine image, and (c) collage tampered image.

(2) Vector quantization (VQ) counterfeiting attack: a counterfeiting tamper on block-wise watermarking algorithm was proposed by Holliman and Memon [14], which was defined as the vector quantization counterfeiting attack. Attacker uses a collage of authentic image blocks in watermarked images to compound an image he wants to forge. To be more exact, aiming at Wong and Memon's scheme [16], counterfeiting a watermark can be accomplished by modifying the vector quantization of an image, where the codebook is determined by the watermark block to be embedded at that location [13]. Fig. 4 represents the result of multiple VQ attacks in watermarked images.

In fact, both CA and VQ counterfeiting attack have the similar structure of manipulating watermarked images, using watermarked images to tamper another watermarked image. Actually, in the collage attack, the spatial tamper location plays a vital role, while the location is not as important as the former in the VQ attack. Providing a specific example, the collage attack intends to copy the part region at the spatial location (x, y) in watermarked image $\boldsymbol{A}$, and paste it to image $\boldsymbol{B}$ at the same location (x, y), which has the same embedding methods with $\boldsymbol{A}$.



(a) (b) (c)

(d) (e)

Fig. 4. VQ counterfeiting tamper: (a) watermarked Airplane image, (b) watermarked Vacas image, (c) watermarked Cameraman image, (d) watermarked Car image, and (e) multiple VQ tampered image.

(3) Constant average attack (CAA): In the authentication scheme, CAA as a tamper attack that does not alter the features was proposed in [17]. It is an attack that average pixel values of the image blocks are used as the recovery information, which is difficult to be detected. To illustrate more concretely, a specific example is given: there are two image blocks $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ with size of 2×2: $\boldsymbol{B}_1 = (30,30;30,30)$ and $\boldsymbol{B}_2 = (1,1;59,59)$. As it can be seen in Fig. 5, the average calculation results of the two blocks value are equal to 30 similarly. Consequently, by using the average value of 2×2 image block to generate the

watermarking algorithm with recovery ability, the same watermark can be obtained. That is to say, if the attacker substitutes block $\boldsymbol{B}_2$ for block $\boldsymbol{B}_1$, the tamper on the image will be accomplished.

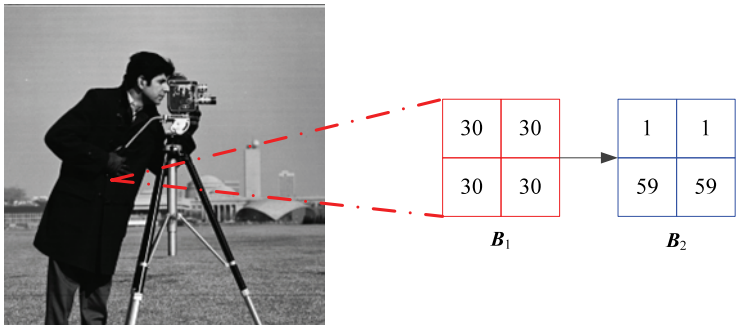


Fig. 5. Constant average attack.

(4) Four-scanning attack: Chang et al. [17] firstly proposed four-scanning attack, which is similar to the conventional dictionary attack. The watermarked image should be divided into 4×4 non-overlapping blocks, and then each block should be segmented into four 2×2 blocks further. Before that, two basic factors should be prepared. The first is the search condition denoted as v_1 to v_4, which are four average values of sub-blocks whose two least significant bits (LSBs) of each pixel are set to zero. The second is the search dictionary composed by the embedded values of watermarked image's all sub-blocks. The process of four-scanning attack includes three steps.

Step 1. Compare v_1 with each v_{s_1} in the first scanning, where v_{s_1} denotes the average value of the first sub-block in the block $\boldsymbol{B}_n$, and n means the block number. The block $\boldsymbol{B}_n$ is marked as suspicious block on the condition that v_{s_1} is equal to v_1.

Step 2. After the first scan finished, the second scan is performed on the suspicious blocks by comparing v_2 with each v_{s_2}. Similarly, v_{s_2} denotes the average value of second sub-block in the block $\boldsymbol{B}_n$. Consequently, the number of suspicious blocks will be reduced if those v_{s_2} is different from v_2.

Step 3. The rest operation will be done in the same manner mentioned above four times.

It is conspicuous that, with the scanning times increasing, the number of suspicious blocks is decreasing, and after scanning four times, the correct block mapped by the conditioned block can be found with high probability. Ultimately, after finding the blocks correlation out, these blocks are tampered certainly.

4. Evaluation Indexes

Due to that SVD is commonly applied in every type of watermarking algorithms, evaluation indexes can be classified into three categories: image quality evaluation indexes for all watermarking algorithms, robustness evaluation indexes for robust watermarking, and tamper detection indexes for fragile and semi-fragile watermarking.

4.1 Image Quality Evaluation Indexes

Image quality evaluation indexes are applied to make the assessment on the quality of watermarked and original images. At present, there are two significant evaluation indexes adopted in most watermarking algorithms, peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) [12], to evaluate the quality of watermarked image.

(1) To measure the similarity between the original image $\boldsymbol{I}$ and the watermarked image $\boldsymbol{I}_{\mathrm{w}}$ with size of $M \times N$, PSNR is adopted, which is defined in Eq. (6):

$$\mathrm{PSNR} = 10\log_{10} \frac{M \times N \times \max\left[\boldsymbol{I}(i,j)^2\right]}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[\boldsymbol{I}(i,j) - \boldsymbol{I}_{\mathrm{w}}(i,j)\right]^2} (\mathrm{dB}), \tag{6}$$

where $\boldsymbol{I}(i,j)$ and $\boldsymbol{I}_{\mathrm{w}}(i,j)$ are the pixel value at the location of (i,j). If the value of PSNR is greater than 30 dB, it means that the watermarked image is of good quality.

(2) Owing to that PSNR does not consider the human visual system (HVS), many experimental results show that the value of PSNR is not completely consistent with the perceptual results of human eyes. An image with a larger PSNR value may look like worse than the one with smaller PSNR value. This is because the HVS is not absolutely sensitive to the visual error. In addition, it is affected by many other factors simultaneously. SSIM proposed by Wang et al. [18] overcomes the disadvantage of PSNR, becoming a useful index of the similarity detection, which is defined as Eq. (7):

$$\mathrm{SSIM} = \frac{2\mu_{\boldsymbol{I}}\mu_{\boldsymbol{I}_{\mathrm{w}}} + C_1}{\mu_{\boldsymbol{I}}^2 + \mu_{\boldsymbol{I}_{\mathrm{w}}}^2 + C_1} \frac{2\sigma_{\boldsymbol{I}}\sigma_{\boldsymbol{I}_{\mathrm{w}}} + C_2}{\sigma_{\boldsymbol{I}}^2 + \sigma_{\boldsymbol{I}_{\mathrm{w}}}^2 + C_2} \frac{\sigma_{\boldsymbol{I}\boldsymbol{I}_{\mathrm{w}}} + C_3}{\sigma_{\boldsymbol{I}}\sigma_{\boldsymbol{I}_{\mathrm{w}}} + C_3}, \tag{7}$$

where $\mu_{\boldsymbol{I}}$ and $\mu_{\boldsymbol{I}_{\mathrm{w}}}$ denote the mean of original image $\boldsymbol{I}$ and watermarked image $\boldsymbol{I}_{\mathrm{w}}$, respectively. Furthermore, $\sigma_{\boldsymbol{I}}$ and $\sigma_{\boldsymbol{I}_{\mathrm{w}}}$ are the variance of image $\boldsymbol{I}$ and $\boldsymbol{I}_{\mathrm{w}}$, respectively, while $\sigma_{\boldsymbol{I}\boldsymbol{I}_{\mathrm{w}}}$ is the covariance between $\boldsymbol{I}$ and $\boldsymbol{I}_{\mathrm{w}}$. C_1, C_2, and C_3 are positive parameters. The value of SSIM ranges from 0 to 1. When SSIM is equal to 1, $\boldsymbol{I}$ and $\boldsymbol{I}_{\mathrm{w}}$ are exactly the same.

4.2 Robustness Evaluation Indexes

To evaluate the robustness in robust and semi-fragile watermarking, normalized correlation (NC) was proposed to calculate the similarity between original watermark and extracted watermark. Besides, bit correction rate (BCR) is another measurement of the watermark schemes proposed to measure the correction ratio of the extracted watermark [19].

(1) NC is the measurement for quality of extracted watermark in the watermarking algorithm, which is presented by Eq. (8):

$$\mathrm{NC} = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[\boldsymbol{W}(i,j) \times \boldsymbol{W}_{\mathrm{e}}(i,j)\right]}{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[\boldsymbol{W}(i,j) \times \boldsymbol{W}(i,j)\right]}, \tag{8}$$

where $\boldsymbol{W}(i,j)$ and $\boldsymbol{W}_{\mathrm{e}}(i,j)$ are the pixel values of original watermark and extracted watermark at the location of (i,j), and the size of the watermark is $m\times n$. The higher NC values mean the better quality of the extracted watermark.

(2) BCR defined in Eq. (9) is applied to evaluate the correction ratio of the extracted watermark.

$$\mathrm{BCR}=\frac{\sum_{k=1}^{m\times n}\overline{\boldsymbol{w}(k)\oplus\boldsymbol{w}_{\mathrm{e}}(k)}}{m\times n}, \tag{9}$$

where $\boldsymbol{w}(k)$ and $\boldsymbol{w}_{\mathrm{e}}(k)$ denote the kth binary value of the original watermark vector and the extracted watermark vector, respectively; $\oplus$ indicates the exclusive-or operator. It is obvious that the higher BCR means the greater similarity between the original and the extracted watermark.

4.3 Tamper Detection Indexes

To evaluate the efficiency of watermarking algorithms for tamper detection and recovery, two evaluation indexes are demonstrated. The first type contains the rate of false negative detection (FND) R_{FND}, false positive detection (FPD) R_{FPD}, and average detection (AVD) R_{AVD} [13], which are defined as Eq. (10):

$$R_{\mathrm{FND}}=\frac{n_{\mathrm{t}}^{\mathrm{u}}}{N_{\mathrm{tp}}},\quad R_{\mathrm{FPD}}=\frac{n_{\mathrm{u}}^{\mathrm{t}}}{N_{\mathrm{up}}},\quad R_{\mathrm{AVD}}=\left(1-\frac{R_{\mathrm{FND}}+R_{\mathrm{FPD}}}{1+N_{\mathrm{tr}}}\right)\times 100\%, \tag{10}$$

where $n_{\mathrm{t}}^{\mathrm{u}}$ denotes the number of pixels determined to be untampered mistakenly in the tampered regions of the image, and $n_{\mathrm{u}}^{\mathrm{t}}$ is the number of pixels determined to be tampered in the regions that are not tampered. Besides, N_{tp} and N_{up} denote the total amount of tampered and untampered pixels, respectively. N_{tr} is the number of tampered regions.

The second type is the rate of tamper detection (TPD) R_{TPD}, which is expressed as Eq. (11):

$$R_{\mathrm{TPD}}=\frac{N_{\mathrm{db}}}{N_{\mathrm{tb}}}\times 100\%, \tag{11}$$

where N_{db} represents the number of detected blocks and N_{tb} is the number of tampered blocks. The higher R_{TPD} is, the better robustness against security attacks can be obtained.

5. Literature Review

In the last decades, many watermarking algorithms have been proposed. In this section, some SVD-based watermarking algorithms used for copyright protection, tamper detection, recovery, and application are concluded and analyzed.

5.1 Robust Watermarking Algorithms

The basic idea of watermarking algorithm based on SVD was firstly introduced by Liu and Tan [20]. In this method, using the SVD performed on the host image, the obtained singular values are modified for the purpose of embedding the watermark into the host image. With the combination of the watermark, the watermarked image can be sequentially generated. Correspondingly, the watermark extraction is executed inversely. Experimental results suggest that SVD-based watermarking algorithm has a good performance of transparency, and is robust to common attacks such as noise addition, filtering, and JPEG compression.

In [21], the authors proposed a watermarking algorithm based on SVD for RGB images. Although the proposed algorithm can achieve blind watermark extraction, one or more singular values must be modified to keep the order of singular values, which causes a great impact on the quality of watermarked image. Based on solving above problem, Su et al. [22] proposed a blind SVD-based dual color image watermarking algorithm. By analyzing the orthogonal matrix $\boldsymbol{U}$ generated from the SVD, a similarity correlation is found between the elements at second row first column and third row first column, which can be applied in the watermarking. Di et al. [23] proposed an SVD-based watermarking scheme, embedding the watermark bits by exchanging the quantization residues of a block's largest singular value. To overcome the false positive problem in most watermarking schemes based on SVD, Guo and Prasetyo [24] discussed about a false positive free SVD-based watermarking scheme, embedding the principal components of the watermark decomposed by shuffled SVD (SSVD) into the largest singular values of the blocks, which are obtained by performing block partition on low frequency sub-band after one level DWT. Considering the quantization process to conduct a comprehensive study, Liu et al. [19] proposed quantized SVD (QSVD) based blind watermarking algorithm, which realizes watermark embedding by modifying the quaternion elements in coefficients matrix. The color image is regarded as the matrix of pure quaternion numbers in the proposed algorithm. Next, this matrix is segmented into non-overlapping blocks and transformed by QSVD for each block to get $\boldsymbol{U}$ matrix. Watermark is embedded into the quaternion coefficient in the first column of the $\boldsymbol{U}$ matrix. This algorithm ensures the better stability, robustness, and resistant ability to attacks, which includes salt and pepper noise, sharpen, blurring, brightness adjustment, and clipping.

To improve the robustness and security of the watermark, basic SVD-based schemes can be combined with other transforms. Li et al. [6] proposed a hybrid watermarking algorithm based on SVD and DCT. After performing SVD on the original image, the macroblock which contains the first singular value of each sub-block is functioned by the DCT. In the meanwhile, by using the specific relationship between the pair of the pseudo-randomly selected DCT coefficients, the watermark is embedded into the high frequency band of SVD-DCT blocks. Zhang et al. [25] proposed a robust watermarking method based on all phase biorthogonal transform (APBT) and SVD, where the watermark information is embedded into singular values of the APBT coefficients matrix. A robust digital watermarking algorithm based on framelet and SVD was proposed by Xiao et al. [26]. In this method, framelet transform is performed on image blocks according to watermark's size. The scrambled watermark is embedded into the biggest singular values which are produced by performing

SVD transform on each coarse band gained from framelet transform. In [27], the authors made an analysis on DWT-based and DWT-SVD-based watermarking algorithms used in RGB images, and experimental results illustrate the superiority performance of hybrid DWT-SVD compared with DWT-based method. In [28], the authors proposed a blind watermarking scheme using DWT, SVD and DCT, where watermark is spilt into two parts according to four bits most significant bits (MSBs) and four bits LSBs. These MSBs and LSBs after DCT are embedded into middle singular values of the host image in DWT domain. Additionally, a robust watermarking algorithm based on multiple transforms, DWT, DCT, and SVD, was proposed by Fazli and Moeini [29], where the operation is performed on middle frequency component. Furthermore, owing to that data replication technique and Hamming code are adopted as error correction methods, this method aims mainly to correct the geometric attacks. Makbol et al. [30] introduced a block-based watermarking algorithm using DWT, SVD, and HVS characteristics. In this method, blocks with the lowest entropy and edge entropy values are utilized as the best regions for watermark embedding. Besides, SVD is performed on the low frequency sub-band after one level DWT to modify several elements in $\boldsymbol{U}$ matrix according to predefined conditions. Bekkouch and Faraoun [31] applied two watermarks, a reversible watermark used for verification and a watermark used for confidentiality, to propose a combined watermarking scheme based on DCT, DWT, and SVD.

The scaling factor in SVD-based schemes can be optimized by different optimization algorithms. Mishra et al. [4] proposed an image watermarking based on DWT-SVD with the Firefly optimization algorithm. The singular value of binary watermark is embedded into the third level low frequency sub-band by using scaling factors. While making use of the newly applied Firefly algorithm, the optimized scaling factors can be selected. Ansari et al. [32] proposed a robust watermarking using two level DWT to provide high capacity as well as principal components of host image and watermark decomposed by SVD for watermark embedding. Particle swarm optimization (PSO) is utilized to obtain the optimized multiple scaling factors for tradeoff between imperceptibility and robustness. Loukhaoukha et al. [33] presented to use the multi-objective ant colony optimization to select the optimized scaling factors in the lifting wavelet transform (LWT) and SVD based watermarking scheme. Similarly, Lai et al. [34] proposed an SVD-based watermarking algorithm using micro-genetic algorithm to select the optimized scaling factor. In [35], the authors proposed integer wavelet transform (IWT) and SVD based watermarking algorithm, making use of these transforms properties to solve false positive problem. Besides, the optimized scaling factor is obtained with artificial bee colony (ABC) algorithm to improve the quality of watermarking scheme. Lalani and Doye [36] presented the other DWT-SVD based robust watermarking scheme, where the adaptive fuzzy inference system is used to select the optimal scaling factor for watermark embedding. However, Guo and Prasetyo [37] proposed two special attacks on watermarking algorithm based on the wavelet transform (WT) and SVD, proving that WT-SVD-based watermarking cannot resist these two attacks or provide guarantee in the ownership protection, which leaves researchers a problem to be solved in the future.

For more intuitive understanding, the typical SVD-based robust watermarking algorithms are summarized in Table 1.

Table 1. SVD-based robust watermarking algorithms

Algorithm	Transform	SVD on watermark	Size of host image	Size of watermark	Type of watermark	Scaling factor optimization
[4]	DWT, SVD	Yes	256×256	32×32	Binary	Firefly algorithm
[6]	SVD, DCT	No	512×512	Not given	Binary	No
[19]	QSVD	No	256×256	64×64	Binary	No
[20]	SVD	No	200×200	50×50	Grayscale	No
[21]	SVD	No	256×256 512×512 1024×1024	32×32	RGB	No
[22]	SVD	No	512×512	32×32	RGB	No
[23]	SVD	No	Not given	Not given	Binary	No
[24]	DWT, SVD	Yes	512×512	64×64	Grayscale	No
[25]	APBT, SVD	No	512×512	64×64, 32×32	Binary	No
[26]	Framelet, SVD	No	512×512	64×64	Grayscale	No
[28]	DWT, DCT, SVD	No	1024×1024	128×128	Grayscale	No
[29]	DWT, DCT, SVD	No	512×512	32×32	Binary	No
[30]	DWT, SVD	No	512×512	32×32	Binary	No
[31]	DWT, DCT, SVD	No	256×256	1×206, 106×143	Binary	No
[32]	DWT, SVD	Yes	512×512	128×128	Not given	Particle swarm optimization
[33]	LWT, SVD	Yes	256×256	32×32	Binary	Ant colony optimization
[34]	SVD	No	256×256	64×64	Grayscale	Micro-genetic algorithm
[35]	IWT, SVD	No	512×512	256×256	Grayscale	Artificial bee colony
[36]	DWT, SVD	Yes	512×512	64×64	Grayscale	Fuzzy inference system

5.2 Fragile and Semi-Fragile Watermarking Algorithms

Correspondingly, SVD can still be applied in the perspective of fragile and semi-fragile watermarking algorithms. Sun et al. [38] presented a block-wise semi-fragile watermarking algorithm based on SVD, embedding the pseudo-random permutated binary watermark in the biggest singular value by quantization process. This scheme can resist JPEG compression and locate the tamper on the image. Byun et al. [39] proposed a fragile watermarking scheme based on SVD for image authentication, where SVD is applied to make binary authentication data by modular arithmetic. Binary bits, authentication data, are embedded into the LSBs of the original image. Zhang et al. [40] proposed a pixel-based fragile watermarking algorithm by analyzing the SVD characteristic to generate the watermarking information. Encrypted watermark by Arnold transform is embedded into the LSBs of the host image. To achieve tamper detection in watermarking algorithm, Dadkhah et al. [13] proposed an SVD-based

watermarking algorithm for image tamper detection and self-recovery, where SVD is performed on image blocks, generating two different tamper detection keys. Simultaneously, block mapping sequence generated randomly, and three optimization algorithms are applied to promote the tamper detection efficiency and robustness to various attacks, such as CA and CAA. Furthermore, to improve the ability of tamper location, the hybrid partition algorithm for blocks with sizes of 2×2 and 4×4 is applied in this method. The performance of tamper detection rate is accurate, and when the tampered region is less than 55%, this method has good robustness and recovery ability. Wu et al. [41] introduced an SVD-VQ-based semi-fragile watermarking scheme. The coefficients of matrices $\boldsymbol{U}$ and $\boldsymbol{V}$ derived from SVD can represent the image feature. SVD is performed on the host image, and image feature is extracted from SVD coefficients. VQ is then applied on these features, where indices are obtained and embedded into the significant singular values. Wu and Lin [42] presented an SVD-based image authentication scheme using quick response code features, where two self-embedding image authentication approaches were proposed using distinctive singular values, extracting characteristics of an image as the crucial authentication information. The authentication information is converted into the two-dimensional codes, which are then embedded into digital image pixels. With the capability of error correction in two dimensional codes, the extracted authentication data can be restored. In [5], a semi-fragile watermarking algorithm based on SVD for image authentication was proposed by Qi and Xin. In the way of performing the logic operation on the content-related watermark generated by SVD sequence as well as content-unrelated watermark obtained by the key sequence, the security watermarks can be obtained. In the watermark embedding, the watermark is embedded into the approximation sub-band of each 4×4 block with the help of adaptive quantization. Besides that, to achieve image content authentication and tampered regions location, a three-level process is performed to identify the malicious and unintentional operations, as well as determine the location of tampered regions under content-preserving modifications from mild intensity to severe intensity. Ansari et al. [43] proposed an SVD-based fragile watermarking for tamper location and self-recovery. Block-wise SVD is performed on blocks obtained by 4×4 block partition, and the trace of singular matrix is used to calculate the authentication bits for every block. Then, 4×4 blocks will be partitioned into 2×2 blocks further and self-recovery information is computed. The encrypted codes are embedded into the first and second LSBs of the parent block, which include tamper location information of parent block and self-recovery information of mapped block. This algorithm can resist VQ, CAA, CA, and four-scanning attack, and experimental results provide an average detection rate of more than 99.5% and average recovery of 28 dB for a 50% tamper. Besides, the SVD-based watermarking can be used to detect the criminals in the crime scene images. Moniruzzaman et al. [44] proposed watermarking algorithm based on SVD and chaotic system for crime scene images recovery. In this paper, the crime scene image can be segmented into two parts. One is the region of information (ROI), and the other is the region of background (ROB). The authenticated information is embedded into the ROB in the scrambled crime scene image. Using the logistic map and 2-D Arnold transform, the authenticated information and scrambled tampered scene image are obtained. Afterwards, DCT is performed on the ROI, and then SVD is executed to embed the ROI transformed by DCT into the ROB. In the extraction process, authentication information is extracted from the watermarked image. But in the condition that the extracted authenticated information is different from the embedded authenticated information, ROI will be recovered by extracting watermark from the ROB.

For more profound understanding, SVD-based fragile and semi-fragile watermarking algorithms reviewed above are summarized in Table 2.

Table 2. SVD-based fragile and semi-fragile watermarking algorithms

Algorithm	Type	Transform	Block	Size of host image	Image recovery	Watermark generation
[5]	Semi-fragile	DWT, SVD	4×4	512×512	No	Relationships of singular values
[13]	Semi-fragile	SVD	2×2, 4×4	512×512	Yes	Singular values computation
[38]	Semi-fragile	SVD	8×8	512×512	No	No
[40]	Fragile	SVD	4×4	256×256	No	Matrix product for texture information
[41]	Semi-fragile	SVD	Not given	512×512	No	Vector quantization
[42]	Fragile	SVD	4×4	256×256	Yes	Quick response encoding
[43]	Fragile	SVD	4×4, 2×2	Not given	Yes	Matrix calculation and block mapping

6. Conclusions

With the rapid development of the Internet, digital image, as the main source of information spreading, has been widely used in daily life. Therefore, it is urgent and important to achieve the authenticity and integrity protection of images, which becomes the focus of study. Digital watermarking algorithm is an effective method to solve this problem. In this paper, we make the review and analysis on different types of SVD-based watermarking algorithms for copyright protection, tamper detection, and image recovery. Besides, the SVD theory and features of image watermarking are demonstrated in this study. Further, we have discussed existing SVD-based watermarking algorithms and illustrated evaluation indexes usually used in watermarking algorithm. By comparing and analyzing different watermarking algorithms, we can be aware that, in SVD-based watermarking, a significant method that can meet all requirements does not exist. This problem still remains to be solved in the future.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (No. 61702303, No. 61201371), the Natural Science Foundation of Shandong Province, China (No. ZR2017MF020, No. ZR2015PF004), and the Research Award Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province, China (No. BS2013DX022).

References

[1] J. Dittmann, A. Steinmetz, and R. Steinmetz, "Content-based digital signature for motion pictures authentication and content-fragile watermarking," in *Proceedings of the IEEE International Conference on Multimedia Computing and Systems*, Florence, Italy, 1999, pp. 209-213.

[2] D. C. Lou and J. L. Liu, "Fault resilient and compression tolerant digital signature for image authentication," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 31-39, 2000.

[3] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20-46, 2000.

[4] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT–SVD and firefly algorithm," *Expert Systems with Applications*, vol. 41, no. 17, pp. 7858-7867, 2014.

[5] X. J. Qi and X. Xin, "A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization," *Journal of Visual Communication and Image Representation*, vol. 30, pp. 312-327, 2015.

[6] Z. Li, K. H. Yap, and B. Y. Lei, "A new blind robust image watermarking scheme in SVD-DCT composite domain," in *Proceedings of the 18th IEEE International Conference on Image Processing*, Brussels, Belgium, 2011, pp. 2757-2760.

[7] R. E. Curto and Y. M. Han, "Weyl's theorem, a-Weyl's theorem, and local spectral theory," *Journal of the London Mathematical Society*, vol. 67, no. 2, pp. 499-509, 2003.

[8] Y. H. Zhang, "Blind watermark algorithm based on HVS and RBF neural network in DWT domain," *WSEAS Transactions on Computers*, vol. 8, no. 1, pp. 174-183, 2009.

[9] O. Benrhouma, H. Hermassi, A. A. A. El-Latif, and S. Belghith, "Chaotic watermark for blind forgery detection in images," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8695-8718, 2016.

[10] O. Benrhouma, H. Hermassi, and S. Belghith, "Tamper detection and self-recovery scheme by DWT watermarking," *Nonlinear Dynamics*, vol. 79, no. 3, pp. 1817-1833, 2015.

[11] P. L. Lin, C. K. Hsieh, and P. W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery," *Pattern Recognition*, vol. 38, no. 12, pp. 2519-2529, 2005.

[12] Y. P. Zhang, C. Y. Wang, and X. Zhou, "RST resilient watermarking scheme based on DWT-SVD and scale-invariant feature transform," *Algorithms*, vol. 10, no. 2, article no. 41, pp. 1-21, 2017.

[13] S. Dadkhah, A. A. Manaf, Y. Hori, A. E. Hassanien, and S. Sadeghi, "An effective SVD-based image tampering detection and self-recovery using active watermarking," *Signal Processing: Image Communication*, vol. 29, no. 10, pp. 1197-1210, 2014.

[14] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," *IEEE Transactions on Image Processing*, vol. 9, no. 3, pp. 432-441, 2000.

[15] J. Fridrich, M. Goljan, and N. Memon, "Cryptanalysis of the Yeung-Mintzer fragile watermarking technique," *Journal of Electronic Imaging*, vol. 11, no. 2, pp. 262-274, 2002.

[16] P. W. Wong and N. Memon, "Secret and public key authentication watermarking schemes that resist vector quantization attack," in *Proceedings of the SPIE − Security and Watermarking of Multimedia Contents II*, San Jose, CA, USA, 2000, pp. 417-427.

[17] C. C. Chang, Y. H. Fan, and W. L. Tai, "Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery," *Pattern Recognition*, vol. 41, no. 2, pp. 654-661, 2008.

[18] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, 2004.

[19] F. Liu, H. Feng, and C. Lu, "Blind watermarking scheme based on U matrix through QSVD transformation," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 203-216, 2015.

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

[21] N. E. H. Golea, R. Seghir, and R. Benzid, "A bind RGB color image watermarking based on singular value decomposition," in *Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications*, Hammamet, Tunisia, 2010, article no. 5586967, pp. 1-5.

[22] Q. T. Su, Y. G. Niu, H. L. Zhou, and X. X. Liu, "A blind dual color images watermarking based on singular value decomposition," *Applied Mathematics and Computation*, vol. 219, no. 16, pp. 8455-8466, 2013.

[23] Y. F. Di, C. F. Lee, Z. H. Wang, C. C. Chang, and J. J. Li, "A robust and removable watermarking scheme using singular value decomposition," *KSII Transactions on Internet & Information Systems*, vol. 10, no. 12, pp. 5268-5285, 2016.

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

[25] Y. P. Zhang, C. Y. Wang, X. L. Wang, and M. Wang, "Feature-based image watermarking algorithm using SVD and APBT for copyright protection," *Future Internet*, vol. 9, no. 2, article no. 13, pp. 1-15, 2017.

[26] M. Y. Xiao, Z. B. He, and T. W. Quan, "A robust digital watermarking algorithm based on framelet and SVD," in *Proceedings of the SPIE − The 9th International Symposium on Multispectral Image Processing and Pattern Recognition*, Enshi, Hubei, China, 2015, article no. 981119, pp. 1-6.

[27] N. Narula, D. Sethi, and P. P. Bhattacharya, "Comparative analysis of DWT and DWT-SVD watermarking techniques in RGB images," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 8, no. 4, pp. 339-348, 2015.

[28] D. Singh and S. K. Singh, "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13001-13024, 2017.

[29] 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*, vol. 127, no. 2, pp. 964-972, 2016.

[30] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," *IET Image Processing*, vol. 10, no. 1, pp. 34-52, 2016.

[31] S. Bekkouch and K. M. Faraoun, "Robust and reversible image watermarking scheme using combined DCT-DWT-SVD transforms," *Journal of Information Processing Systems*, vol. 11, no. 3, pp. 406-420, 2015.

[32] I. A. Ansari, M. Pant, and C. W. Ahn, "PSO optimized and secured watermarking scheme based on DWT and SVD," in *Proceedings of the 5th International Conference on Soft Computing for Problem Solving*, Roorkee, India, 2015, pp. 411-424.

[33] K. Loukhaoukha, J. Y. Chouinard, and M. H. Taieb, "Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 4, pp. 303-319, 2011.

[34] C. C. Lai, C. C. Tsai, and S. T. Pan, "An SVD-based watermarking scheme using improved micro-genetic algorithm," in *Proceedings of the IEEE International Conference on Fuzzy Systems*, Jeju Island, Korea, 2009, pp. 1875-1878.

[35] I. A. Ansari, M. Pant, and C. W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," *Engineering Applications of Artificial Intelligence*, vol. 49, pp. 114-125, 2016.

[36] S. Lalani and D. D. Doye, "Discrete wavelet transform and a singular value decomposition technique for watermarking based on an adaptive fuzzy inference system," *Journal of Information Processing Systems*, vol. 13, no. 2, pp. 340-347, 2017.

[37] J. M. Guo and H. Prasetyo, "Security attacks on the wavelet transform and singular value decomposition image watermarking," in *Proceedings of the 17th IEEE International Symposium on Consumer Electronics*, Hsinchu, Taiwan, 2013, pp. 217-218.

[38] R. Sun, H. Sun, and T. R. Yao, "A SVD- and quantization based semi-fragile watermarking technique for image authentication," in *Proceedings of the 6th International Conference on Signal Processing*, Beijing, China, 2002, pp. 1592-1595.

[39] S. C. Byun, S. K. Lee, A. H. Tewfik, and B. H. Ahn, "A SVD-based fragile watermarking scheme for image authentication," in *Proceedings of the 1st International Workshop on Digital Watermarking*, Seoul, Korea, 2002, pp. 170-178.

[40] H. Zhang, C. Y. Wang, and X. Zhou, "Fragile watermarking for image authentication using the characteristic of SVD," *Algorithms*, vol. 10, no. 1, article no. 27, pp. 1-12, 2017.

[41] H. C. Wu, C. P. Yeh, and C. S. Tsai, "A semi-fragile watermarking scheme based on SVD and VQ techniques," in *Proceedings of the International Conference on Computational Science and Its Applications: Part III*, Glasgow, UK, 2006, pp. 406-415.

[42] W. C. Wu and Z. W. Lin, "SVD-based self-embedding image authentication scheme using quick response code features," *Journal of Visual Communication and Image Representation*, vol. 38, pp. 18-28, 2016.

[43] I. A. Ansari, M. Pant, and C. W. Ahn, "SVD based fragile watermarking scheme for tamper localization and self-recovery," *International Journal of Machine Learning and Cybernetics*, vol. 7, no. 6, pp. 1225-1239, 2016.

[44] M. Moniruzzaman, M. A. K. Hawlader, M. F. Hossain, and M. A. Rashid, "SVD and chaotic system based watermarking approach for recovering crime scene image," in *Proceedings of the 8th International Conference on Electrical and Computer Engineering*, Dhaka, Bangladesh, 2014, pp. 132-135.

Chengyou Wang http://orcid.org/0000-0002-0901-2492

He received 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 at Shandong University, Weihai, China. His current research interests include image/video coding, digital watermarking, and tamper detection.

Yunpeng Zhang http://orcid.org/0000-0002-6697-1024

He received his B.E. degree in communication engineering from Shandong Agricultural University, China, in 2015. He is currently pursuing his M.E. degree in signal and information processing at Shandong University, China. His current research interests include image/video watermarking and tamper detection.

Xiao Zhou http://orcid.org/0000-0002-1331-7379

She received her M.E. degree in information and communication engineering from Inha University, Republic of 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 at Shandong University, Weihai, China. Her current research interests include channel estimation, image communication, and image watermarking.