Expert Systems with Applications 39 (2012) 673–689

Contents lists available at SciVerse ScienceDirect

Expert Systems with Applications

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

An improved SVD-based watermarking technique for copyright protection [☆]

Ray-Shine Run[a,b], Shi-Jinn Horng[a,*], Jui-Lin Lai[b], Tzong-Wang Kao[c], Rong-Jian Chen[b]

[a] Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan
[b] Department of Electronic Engineering, National United University, Miao-Li, Taiwan
[c] Department of Electronic Engineering, Technology and Science Institute of Northern Taiwan, Taipei, Taiwan

ARTICLE INFO

Keywords:
Singular value decomposition
Principal component
Watermarking
False positive problem
Ambiguous situation
Particle swarm optimization

ABSTRACT

The drawbacks of SVD-based image watermarking are false positive, robust and transparency. The former can be overcome by embedding the principal components of the watermark into the host image, the latter is dependent on how much the quantity (i.e., scaling factor) of the principal components is embedded. For the existing methods, the scaling factor is a fixed value; actually, it is image-dependent. Different watermarks need the different scaling factors, although they are embedded in the same host image. In this paper, two methods are proposed to improve the reliability and robustness. To improve the reliability, for the first method, the principal components of the watermark are embedded into the host image in discrete cosine transform (DCT); and for the second method, those are embedded into the host image in discrete wavelets transform (DWT). To improve the robustness, the particle swarm optimization (PSO) is used for finding the suitable scaling factors. The experimental results demonstrate that the performance of the proposed methods outperforms than those of the existing methods.

1. Introduction

The invention of internet has changed the human life style. Acquisition, exchange, and transmission the multimedia data over internet become a simple task. However, making digital data accessible to others through networks also creates opportunities for the piracy. Someone can easily download the multimedia data from the internet and make salable copies of copyrighted content without the permission of the content owner (Cox et al., 1997; Liu & Tan, 2002; Seitz & Jahnke, 2005).

Digital image watermarking has been proposed in recent years as a method to protect the copyright of multimedia documents in the networked environments (Cox et al., 1997; Liu & Tan, 2002; Seitz & Jahnke, 2005). There are two important issues that watermarking algorithms need to address. First, watermarking scheme required to provide trustworthy evidence for protecting the rightful ownership. The perceptual difference between the watermarked and the original documents should be unnoticeable to the human observer. Second, good watermarking scheme should satisfy the requirement of robustness and resist distortions due to common image manipulations (such as filtering, histogram equalization, edge detection, etc.). The watermark should be detectable and extractable after image manipulations were applied to the watermarked image.

1.1. Motivation

Most existing watermarking schemes focus on robustness issues which mean to make watermark imperceptible rather than on addressing the important issue of how to resolve the rightful ownership of an image embedded with multiple signatures (or watermarks, labels, etc.) (Liu & Tan, 2002). The singular value decomposition (SVD) based image watermarking has been proposed (Abdallah, Ben Hamza, & Bhattacharya, 2007; Alexander, Scott, & Ahmet, 2005; Bhatnagar & Raman, 2009; Chandra, 2002; Ganic & Eskicioglu, 2004; Ghazy, El-Fishawy, Hadhoud, Dessouky, & El-Samie, 2007; Huang & Guan, 2004; Jain, Arora, & Panigrahi, 2008; Liu & Tan, 2002; Liu et al., 2008; Mohammad, Alhaj, & Shaltaf, 2008; Ouhsain & Ben Hamza, 2009; Patra, Soh, Ang, & Meher, 2006; Shieh, Lou, & Chang, 2006; Sverdlov, Dexter, & Eskicioglu, 2005) for solving the ownership problem. The key point of the SVD-based image watermarking is the stability property of the singular value matrix. Several authors have been conducted experiments in the SVD-based watermarking to find the robust watermarking scheme (Abdallah et al., 2007; Alexander et al., 2005; Bhatnagar & Raman, 2009; Chandra, 2002; Ganic & Eskicioglu, 2004; Ghazy et al., 2007; Huang & Guan, 2004; Jain et al., 2008; Liu & Tan, 2002; Liu et al., 2008; Mohammad et al., 2008; Ouhsain & Ben Hamza, 2009; Patra et al., 2006; Shieh et al., 2006; Sverdlov et al., 2005).

In most of literature (Abdallah et al., 2007; Alexander et al., 2005; Bhatnagar & Raman, 2009; Ganic & Eskicioglu, 2004; Ghazy

[☆] This work was supported in part by the National Science Council under contract number NSC-98-2219-E-011-002, NSC-98-2221-E-011-133-MY3, NSC-98-2923-E-011-004-MY3, and NSC-99-2916-I-011-002-A1.

[*] Corresponding author.
E-mail addresses: run5116@ms16.hinet.net (R.-S. Run), horngsj@yahoo.com.tw (S.-J. Horng), jllai@nuu.edu.tw (J.-L. Lai), tkao@tsint.edu.tw (T.-W. Kao), rjchen@nuu.edu.tw (R.-J. Chen).

0957-4174/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2011.07.059

et al., 2007; Huang & Guan, 2004; Liu et al., 2008; Ouhsain & Ben Hamza, 2009; Patra et al., 2006; Shieh et al., 2006; Sverdlov et al., 2005), only the singular values of watermark are embedded into the host image. This strategy causes the false positive problem. A false positive problem may also occur when a specific watermark is detected from a content in which a different watermark was embedded, causing an *ambiguous situation*. The attackers can easily prove the ownership of the arbitrary watermarked image without knowing the original watermark embedded in the host image. The image watermarking schemes based on SVD operation as proposed in Liu and Tan (2002), Chandra (2002), Ouhsain and Ben Hamza (2009), Bhatnagar and Raman (2009), Abdallah et al. (2007), Shieh et al. (2006), Huang and Guan (2004), Alexander et al. (2005), Ghazy et al. (2007), Patra et al. (2006), Sverdlov et al. (2005), Liu et al. (2008), Ganic and Eskicioglu (2004), Mohammad et al. (2008) and Jain et al. (2008) have a good stability and robust against the common image manipulation (such as histogram equalization, filtering, adding noise, etc.). Unfortunately, most of SVD-based image watermarking scheme (Abdallah et al., 2007; Alexander et al., 2005; Liu & Tan, 2002; Liu et al., 2008; Bhatnagar & Raman, 2009; Ganic & Eskicioglu, 2004; Ghazy et al., 2007; Huang & Guan, 2004; Ouhsain & Ben Hamza, 2009; Patra et al., 2006; Shieh et al., 2006) has a major drawback as mention before (the false positive problem). Any reference watermark that is being searched for in an arbitrary image can be easily found by attackers.

In Jain et al. (2008), the authors suggested a new approach for the reliable SVD-based image watermarking scheme. The author tried to embed not only the singular value of the watermark, but also the principal component of watermark into the host image. This algorithm is based on the fact that SVD subspace (left and right singular vectors, matrix U and V^T) can preserve significant amount of information of an image. Using this simple idea, the ownership problem occurred in Ouhsain and Ben Hamza (2009), Bhatnagar and Raman (2009), Abdallah et al. (2007), Shieh et al. (2006), Huang and Guan (2004), Alexander et al. (2005), Ghazy et al. (2007), Patra et al. (2006), Sverdlov et al. (2005), Liu et al. (2008), Ganic and Eskicioglu (2004) can be solved. Another problem occurs when only scalar value of the scaling factor used in this reliable SVD-based image watermarking. Using the small value for scaling factor, the invisibility of the watermark is achieved (high PSNR of watermarked image), but the watermarked image is less robust with several common attacks. By incorporating the high scaling factor, the quality of watermarked image is unacceptable, but the watermark is robust.

In Jain et al. (2008), scaling factor plays an important role to control the transparency and robustness of the watermarked image. There is no exact algorithm to choose the value of scaling factor. Most of them are based on trial-and-error method. It is necessary to design an efficient algorithm to find the suitable scaling value for achieving the robust and reliable SVD-based image watermarking.

1.2. Research focus and contribution

This research focuses on the transparency and robustness of the reliable SVD-based image watermarking. We propose new methods in the reliable SVD-based image watermarking by incorporating the discrete wavelet transform (DWT) and discrete cosine transform (DCT), respectively. The principal components of the watermark are inserted into the host image. The scaling factor used is in a matrix form, not in a scalar value. To overcome the scaling factor problem, the metaheuristic algorithm is chosen to find the suitable scaling factor. In this research, the particle swarm optimization (http://www.swarmintelligence.org/) (one of the metaheuristic algorithm) is chosen for finding the scaling factor to achieve the robustness and imperceptible of watermarked image.

The rest of this paper is organized in the following. We will first briefly discuss the basic concept of the singular value decomposition (SVD). The existing methods for SVD-based image watermarking and drawbacks are presented in Section 2. The method to overcome the common drawback of SVD-based image watermarking is given in Section 3. Section 4 provides the detailed explanation of the proposed methods. The experimental results and conclusion are discussed in Sections 5 and 6, respectively.

2. SVD-based image watermarking and its drawbacks

The basic concept of singular value decomposition (SVD) operation is discussed in Section 2.1. The existing methods in the SVD-based image watermarking and their major drawbacks will be discussed later in the following sections.

2.1. Singular value decomposition (SVD)

From the perspective of image processing, an image can be viewed as a matrix with non negative scalar entries. The singular value decomposition (SVD) on an image A of size $N \times M$ is defined in the following (Ientilucci & Emmett, 2003).

$$A = U\Sigma V^T, \tag{2.1}$$

where $A \in \Re^{N\times M}$, $U \in \Re^{N\times N}$, $\Sigma \in \Re^{N\times M}$ and $V \in \Re^{M\times M}$. The matrix U and V are called the left and right singular vectors. U and V matrices are orthogonal matrices. So, the following conditions are always satisfied.

$$UU^T = U^TU = I_N, \tag{2.2}$$

$$VV^T = V^TV = I_M. \tag{2.3}$$

The matrix Σ is diagonal and also known as singular value matrix and Σ_r is a square diagonal matrix in $\Re^{r\times r}$.

$$\Sigma = \begin{bmatrix} \Sigma_r & 0 \\ 0 & 0 \end{bmatrix} \quad \text{where } \Sigma_r = diag(\sigma_1, \sigma_2, \ldots, \sigma_r).$$

A simple example of the SVD operation is given below:

$$A = \begin{bmatrix} 50 & 100 \\ 110 & 20 \\ 110 & 20 \\ 50 & 100 \end{bmatrix} = \begin{bmatrix} -0.5000 & 0.5000 & -0.1544 & -0.6901 \\ -0.5000 & -0.5000 & -0.6901 & 0.1544 \\ -0.5000 & -0.5000 & 0.6901 & -0.1544 \\ -0.5000 & 0.5000 & 0.1544 & 0.6901 \end{bmatrix} \times \begin{bmatrix} 200 & 0 \\ 0 & 100 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} -0.8 & -0.6 \\ -0.6 & 0.8 \end{bmatrix}^T$$

The SVD operation can be presented in another representation by denoting U and V as the column matrices in (2.4) and (2.5).

$$U = [\underbrace{u_1, u_2, \ldots, u_r}_{U_r}, \underbrace{u_{r+1}, u_{r+2}, \ldots, u_N}_{\widetilde{U}_r}] = [U_r, \widetilde{U}_r], \tag{2.4}$$

$$V = [\underbrace{v_1, v_2, \ldots, v_r}_{V_r}, \underbrace{v_{r+1}, v_{r+2}, \ldots, v_N}_{\widetilde{V}_r}] = [V_r, \widetilde{V}_r]. \tag{2.5}$$

By using (2.4) and (2.5), the SVD of matrix A can be rewritten as in (2.6).

$$\begin{aligned} A = U\Sigma V^T &= [u_1, u_2, \ldots, u_r, u_{r+1}, u_{r+2}, \ldots, u_N] \\ &\quad \times \begin{bmatrix} \Sigma_r & 0 \\ 0 & 0 \end{bmatrix} [v_1, v_2, \ldots, v_r, v_{r+1}, v_{r+2}, \ldots, v_N]^T \\ &= [U_r, \widetilde{U}_r] \begin{bmatrix} \Sigma_r & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} V_r^T \\ \widetilde{V}_r^T \end{bmatrix} = U_r \Sigma_r V_r^T. \end{aligned} \tag{2.6}$$

Eq. (2.6) can also be written in the summation form as:

$$A = \sum_{i=1}^{r} u_i \sigma_i v_i^T = \sum_{i=1}^{r} \sigma_i u_i v_i^T. \tag{2.7}$$

The following example shows the SVD representation and its another representation.

$$A = \begin{bmatrix} 50 & 100 \\ 110 & 20 \\ 110 & 20 \\ 50 & 100 \end{bmatrix} = \begin{bmatrix} -0.5000 & 0.5000 & -0.1544 & -0.6901 \\ -0.5000 & -0.5000 & -0.6901 & 0.1544 \\ -0.5000 & -0.5000 & 0.6901 & -0.1544 \\ -0.5000 & 0.5000 & 0.1544 & 0.6901 \end{bmatrix} \times \begin{bmatrix} 200 & 0 \\ 0 & 100 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} -0.8 & -0.6 \\ -0.6 & 0.8 \end{bmatrix}^T.$$

If we choose the rank, $r = 2$, the matrix A can be represented in another form as follows:

$$\begin{bmatrix} -0.5 & 0.5 \\ -0.5 & -0.5 \\ -0.5 & -0.5 \\ -0.5 & 0.5 \end{bmatrix} \begin{bmatrix} 200 & 0 \\ 0 & 100 \end{bmatrix} \begin{bmatrix} -0.8 & -0.6 \\ -0.6 & 0.8 \end{bmatrix}^T = \begin{bmatrix} 50 & 100 \\ 110 & 20 \\ 110 & 20 \\ 50 & 100 \end{bmatrix} = A.$$

The computation of SVD can be done by multiplying both A^TA and AA^T. The multiplication can be derived as (2.8) and (2.9).

$$A^TA = (U\Sigma V^T)^T(U\Sigma V^T) = V\Sigma^T U^T U\Sigma V^T = V\Sigma^T I\Sigma V^T = V(\Sigma^T\Sigma)V^T, \tag{2.8}$$

$$AA^T = (U\Sigma V^T)(U\Sigma V^T)^T = U\Sigma V^T V\Sigma^T U^T = U\Sigma I\Sigma^T U^T = U(\Sigma\Sigma^T)U^T, \tag{2.9}$$

where $\Sigma^T\Sigma = \Sigma^2 = \begin{bmatrix} \Sigma_r^2 & 0 \\ 0 & 0 \end{bmatrix} \in \Re^{M\times M}$ and

$\Sigma\Sigma^T = \Sigma^2 = \begin{bmatrix} \Sigma_r^2 & 0 \\ 0 & 0 \end{bmatrix} \in \Re^{N\times N}$.

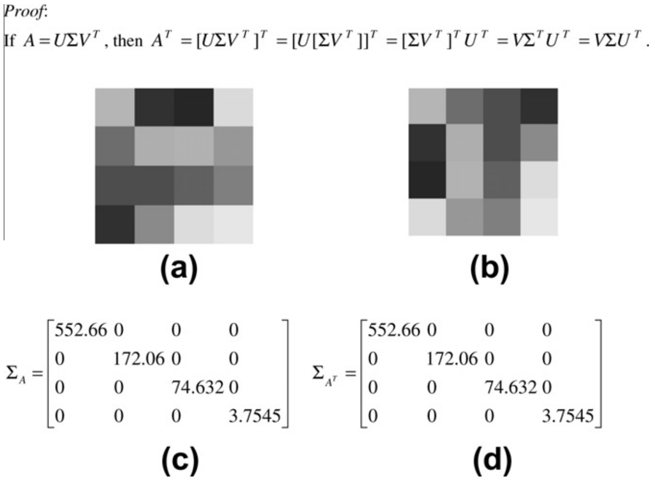
Since the result of multiplication A^TA and AA^T are symmetric matrix, the problem $A^TA = V\Sigma^2V^T$ in (2.8) and $AA^T = U\Sigma^2U^T$ in (2.9) can be viewed and solved by using Eigen-decomposition operation.

There are several important properties of SVD, such as transpose, stability, etc. For the space reason, only three properties are explained in this paper. Following are the main properties of SVD operation:

- *Transpose*: Every real matrix A and its transpose A^T have the same non-zero singular values. Fig. 2.1 shows the transpose property of SVD operation. Fig. 2.1 (a) and (b) are the original image and its rotation version. Fig. 2.1 (c) and (d) show the singular value matrix for A and A^T. Using simple linear algebra, we can prove this property.

Proof. If $A = U\Sigma V^T$, then $A^T = [U\Sigma V^T]^T = [U[\Sigma \quad V^T]]^T = [\Sigma V^T]^TU^T = V\Sigma^TU^T = V\Sigma U^T$.

- *Flip*: Given an image A, row-flipped of A, *rf* and column-flipped A, *cf* have the same non-zero singular values. Fig. 2.2 shows an example of the flip property of SVD operation.
- *Stability:* The SVs (Singular Values) of an image have very good stability, i.e. when a small perturbation is added to an image, its SVs do not vary rapidly. Fig. 2.3 shows an example of the stability property of SVD. □



Proof:

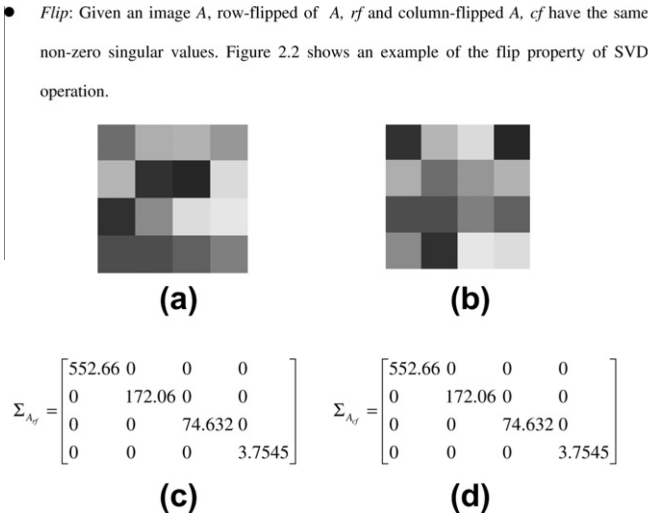
If $A = U\Sigma V^T$, then $A^T = [U\Sigma V^T]^T = [U[\Sigma V^T]]^T = [\Sigma V^T]^T U^T = V\Sigma^T U^T = V\Sigma U^T$.

(a) (b)

$$\Sigma_A = \begin{bmatrix} 552.66 & 0 & 0 & 0 \\ 0 & 172.06 & 0 & 0 \\ 0 & 0 & 74.632 & 0 \\ 0 & 0 & 0 & 3.7545 \end{bmatrix} \quad \Sigma_{A^T} = \begin{bmatrix} 552.66 & 0 & 0 & 0 \\ 0 & 172.06 & 0 & 0 \\ 0 & 0 & 74.632 & 0 \\ 0 & 0 & 0 & 3.7545 \end{bmatrix}$$

(c) (d)

Fig. 2.1. The transpose property of SVD operation.



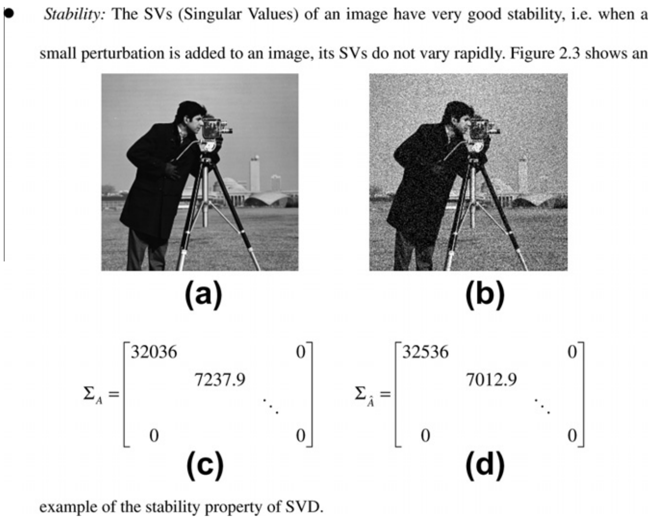
- *Flip*: Given an image *A*, row-flipped of *A*, *rf* and column-flipped *A*, *cf* have the same non-zero singular values. Figure 2.2 shows an example of the flip property of SVD operation.

(a) (b)

$$\Sigma_{A_{rf}} = \begin{bmatrix} 552.66 & 0 & 0 & 0 \\ 0 & 172.06 & 0 & 0 \\ 0 & 0 & 74.632 & 0 \\ 0 & 0 & 0 & 3.7545 \end{bmatrix} \quad \Sigma_{A_{cf}} = \begin{bmatrix} 552.66 & 0 & 0 & 0 \\ 0 & 172.06 & 0 & 0 \\ 0 & 0 & 74.632 & 0 \\ 0 & 0 & 0 & 3.7545 \end{bmatrix}$$

(c) (d)

Fig. 2.2. The flip property of SVD operation.



- *Stability:* The SVs (Singular Values) of an image have very good stability, i.e. when a small perturbation is added to an image, its SVs do not vary rapidly. Figure 2.3 shows an example of the stability property of SVD.

(a) (b)

$$\Sigma_A = \begin{bmatrix} 32036 & & & 0 \\ & 7237.9 & & \\ & & \ddots & \\ 0 & & & 0 \end{bmatrix} \quad \Sigma_{\hat{A}} = \begin{bmatrix} 32536 & & & 0 \\ & 7012.9 & & \\ & & \ddots & \\ 0 & & & 0 \end{bmatrix}$$

(c) (d)

Fig. 2.3. The stability property of SVD operation.

2.2. SVD-based image watermarking

Several SVD-based image watermarking methods have been proposed recently (Abdallah et al., 2007; Alexander et al., 2005; Bhatnagar & Raman, 2009; Chandra, 2002; Ganic & Eskicioglu, 2004; Ghazy et al., 2007; Huang & Guan, 2004; Jain et al., 2008; Liu & Tan, 2002; Liu et al., 2008; Mohammad et al., 2008; Ouhsain & Ben Hamza, 2009; Patra et al., 2006; Shieh et al., 2006; Sverdlov et al., 2005) for solving the ownership problem. All methods only embed the singular values of the watermark into the host image. The singular values of the watermark are directly inserted in the singular values of the host image as reported in Mohammad et al. (2008). Another way for watermark embedding is to insert the watermark into the host image in the transform domain.

Fig. 2.4 shows an example of watermark embedding algorithm using discrete wavelet transform-fast hadamard transform-SVD (DWT-FHT-SVD) scheme as reported in Abdallah et al. (2007). First, an image is decomposed using discrete wavelet transform (DWT) operation into four sub-bands (LL, LH, HL, and HH). For each sub-band, the fast hadamard transform (FHT) is applied by block-based wise. The singular values of the watermark are inserted into the DC-component in each block of FHT result.

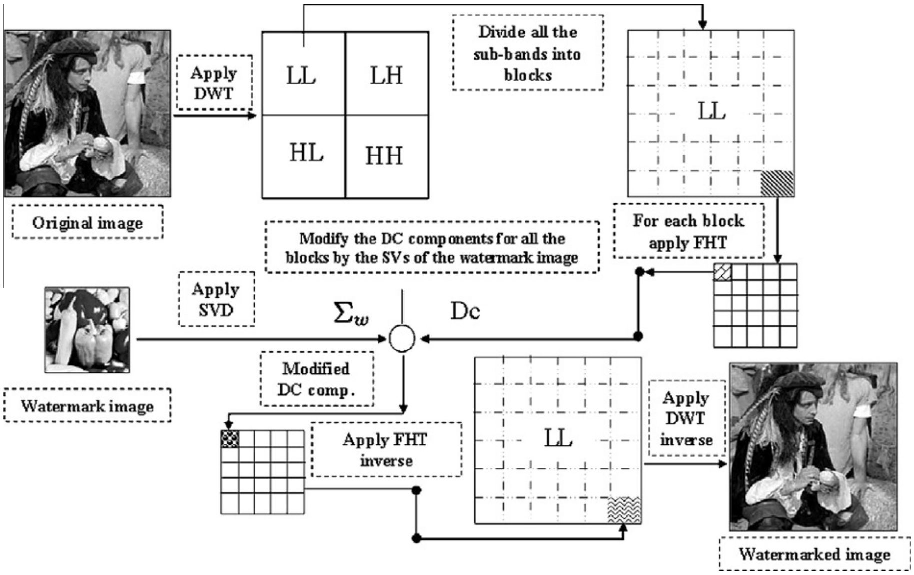


Fig. 2.4. Watermark Embedding in Abdallah et al. (2007).

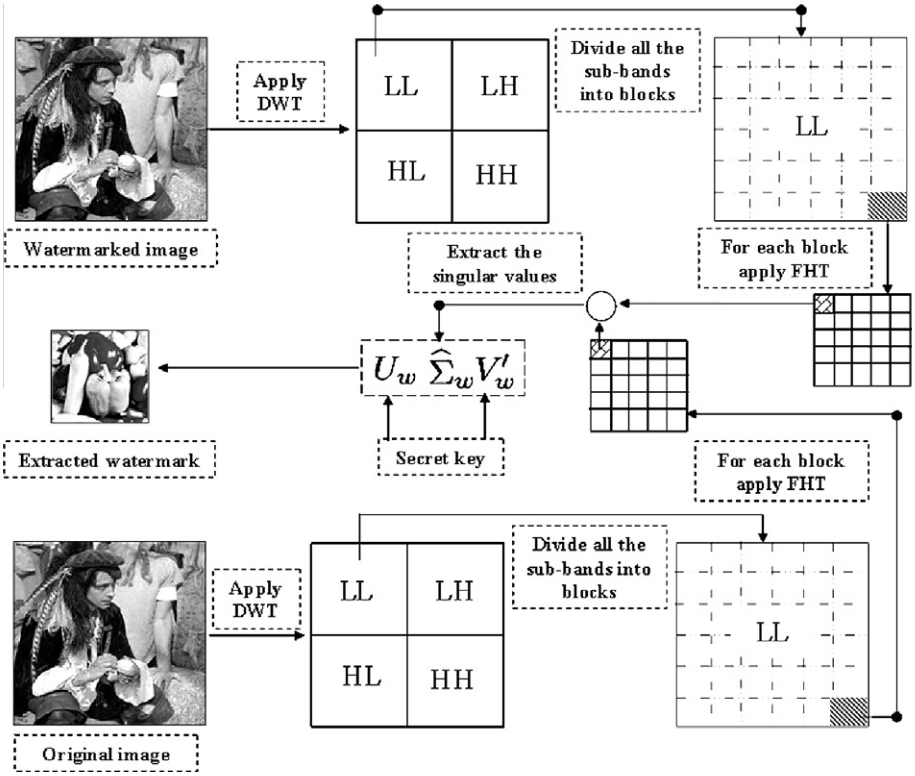


Fig. 2.5. Watermark extraction in Abdallah et al. (2007).

Fig. 2.5 depicts the watermark extraction algorithm in DWT-FHT-SVD scheme (Abdallah et al., 2007). The all subsequence steps in the watermarking extraction algorithm are only the reverse version of watermark embedding.

In the watermark embedding, only the singular values of watermark are inserted in the host image.

2.3. Drawbacks in SVD-based image watermarking

The major drawback in SVD-based image watermarking is false positive problem. Because only the singular values of the watermark are embedded into the host image, the false positive problem occurs when the extracted watermark is detected from the host image without knowing the original watermark. We can use arbitrary reference image to extract the watermark. So, this situation leads the *ambiguous situation* and the ownership problem cannot be solved. Someone can claim the other image by his/her reference image.

Fig. 2.6 shows the drawback of discrete cosine transform (DCT-SVD) based image watermarking as proposed in Alexander et al. (2005). Fig. 2.6(a) and (b) are the host image of size 512 × 512 and the watermark of size 256 × 256. Fig. 2.6(d) is the extracted watermark using reference image 2.6 (c). The extracted watermark using reference image 2.6 (e) can be seen in Fig. 2.6(f).

The DWT-FHT-SVD scheme proposed by Abdallah et. al. in (Abdallah et al., 2007) also faced the same false positive problem as that faced by Sverdlov et. al. in (Alexander et al., 2005).

Strictly speaking, both DCT-SVD (Alexander et al., 2005) and DWT-FHT-SVD (Abdallah et al., 2007) image watermarking schemes are totally not working.

Unfortunately, most of SVD-based image watermarking schemes (Abdallah et al., 2007; Alexander et al., 2005; Bhatnagar & Raman, 2009; Ganic & Eskicioglu, 2004; Ghazy et al., 2007; Huang & Guan, 2004; Liu et al., 2008; Ouhsain & Ben Hamza, 2009; Patra et al., 2006; Shieh et al., 2006; Sverdlov et al., 2005)

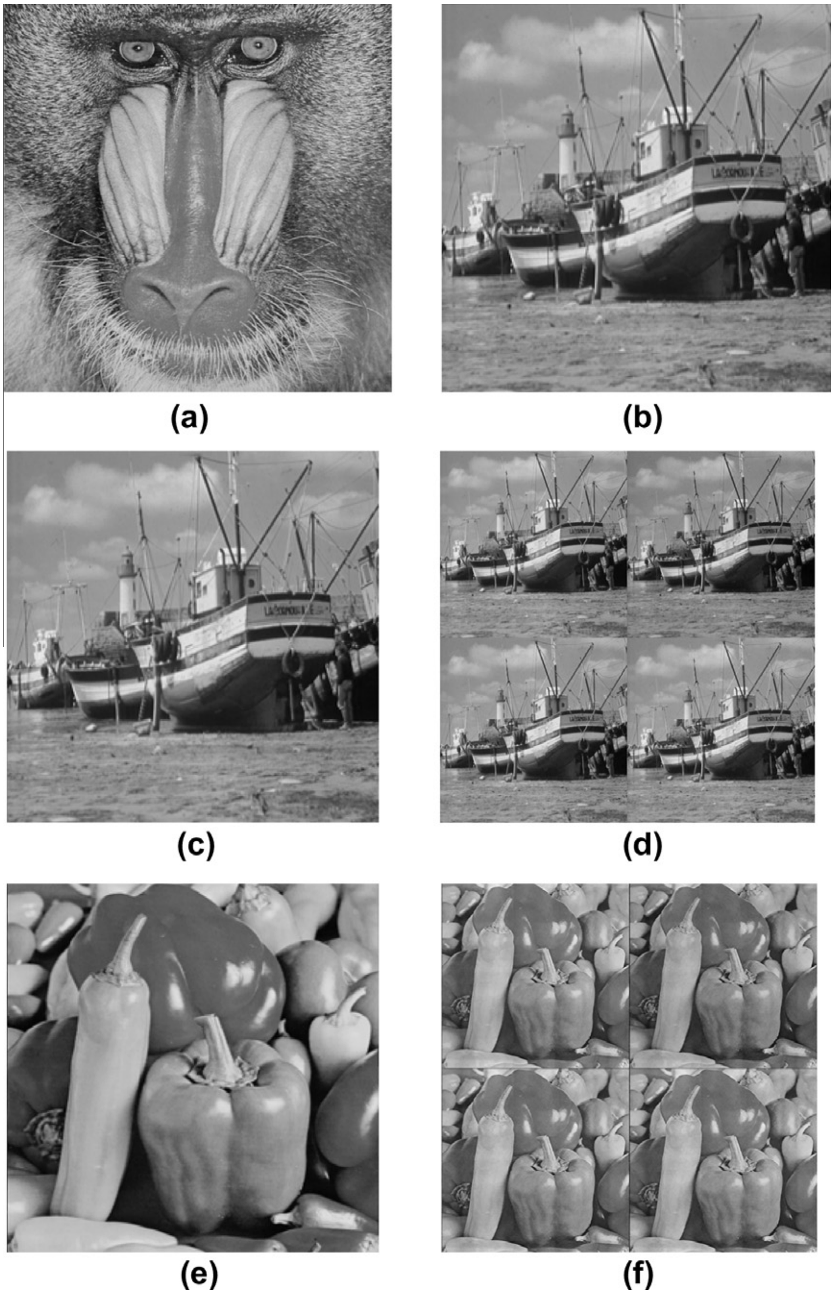


Fig. 2.6. The drawback of Alexander et al. (2005).

have a major drawback as mention before. Any reference watermark that is being searched for in an arbitrary image can be found.

3. Reliable SVD-based watermarking

In this section, we will discuss the reliable image watermarking and the minor problem occurred in this method. This method can easily solve the false positive problem occurred in Ouhsain and Ben Hamza (2009), Bhatnagar and Raman (2009), Abdallah et al. (2007), Shieh et al. (2006), Huang and Guan (2004), Alexander et al. (2005), Ghazy et al. (2007), Patra et al. (2006), Sverdlov et al. (2005), Liu et al. (2008) and Ganic and Eskicioglu (2004). But, the robustness and transparency is still a big problem. In Section 3.1, we will discuss about a reliable SVD-based watermarking scheme. The minor problem for this method will be explained in Section 3.2.

3.1. A Reliable SVD-based watermarking scheme

Taking into consideration, the major flaws in Ouhsain and Ben Hamza (2009), Bhatnagar and Raman (2009), Abdallah et al. (2007), Shieh et al. (2006), Huang and Guan (2004), Alexander et al. (2005), Ghazy et al. (2007), Patra et al. (2006), Sverdlov et al. (2005), Liu et al. (2008) and Ganic and Eskicioglu (2004) is caused by embedding the singular values of the watermark into the host image. Given two images A and B, and perform SVD operation for these two image, $A \Rightarrow U_A\Sigma_A V_A^T$ and $B \Rightarrow U_B\Sigma_B V_B^T$. If we exchange the singular values between images A and B, we will get $U_A\Sigma_B V_A^T \approx A$ and $U_B\Sigma_A V_B^T \approx B$, respectively. Based on this reason, the false positive problem will always occur in SVD-based image watermarking if only singular values are embedded in the host image. In fact, the singular vectors U and V have majority of image information.

In Jain et al. (2008), Chirag et. al. proposed the reliable SVD-based watermarking scheme for solving the problem occurred in Ouhsain and Ben Hamza (2009), Bhatnagar and Raman (2009), Abdallah et al. (2007), Shieh et al. (2006), Huang and Guan (2004), Alexander et al. (2005), Ghazy et al. (2007), Patra et al. (2006), Sverdlov et al. (2005), Liu et al. (2008) and Ganic and Eskicioglu (2004). The authors make use the fact that the SVD subspace can preserve the significant amount of information of an image. The principal components of the watermark are embedded into the singular values of the host image.

Given the host image, A, and visual watermark, W, the main step of Jain et al. (2008) can be explained in the following.

3.1.1. Watermark embedding algorithm

- Perform SVD operation on the host image and watermark image, $A \Rightarrow U\Sigma V^T$, and $W \Rightarrow U_w\Sigma_w V_w^T$.
- Multiply the left singular vector and the singular value of the watermark to get the principal component of the watermark, $A_{wa} = U_w\Sigma_w$.
- Insert the principal component of the watermark into the singular value of the host image, $\Sigma_1 = \Sigma + \alpha A_{wa}$.
- Obtain the watermarked image, $A_w \Leftarrow U\Sigma_1 V^T$.

We need to record the right singular vector, V_m, for the watermark extraction. Note that the scaling factor, α, is a scalar value. The matrix, A_{wa}, is also known as principal components.

3.1.2. Watermark extraction algorithm

Suppose A_w^* denotes the possibly distorted watermarked image. For extracting back the watermark, W^*, from, A_w^*, the following steps are involved:

- Subtract the possibly distorted watermarked image with the original host image, $A_1 = A_w^* - A$.
- Obtain the distorted principal component, $A_{wa}^* = \frac{1}{\alpha}(U^{-1}A_1(V^T)^{-1})$
- Construct the extracted watermark by multiplying the distorted principal component with the right singular vector of the original watermark image, $W^* \Leftarrow A_{wa}^* V_w^T$.

Fig. 3.1 demonstrates the reliable SVD-based watermarking scheme. The host and watermark image are shown in Fig. 3.1(a)

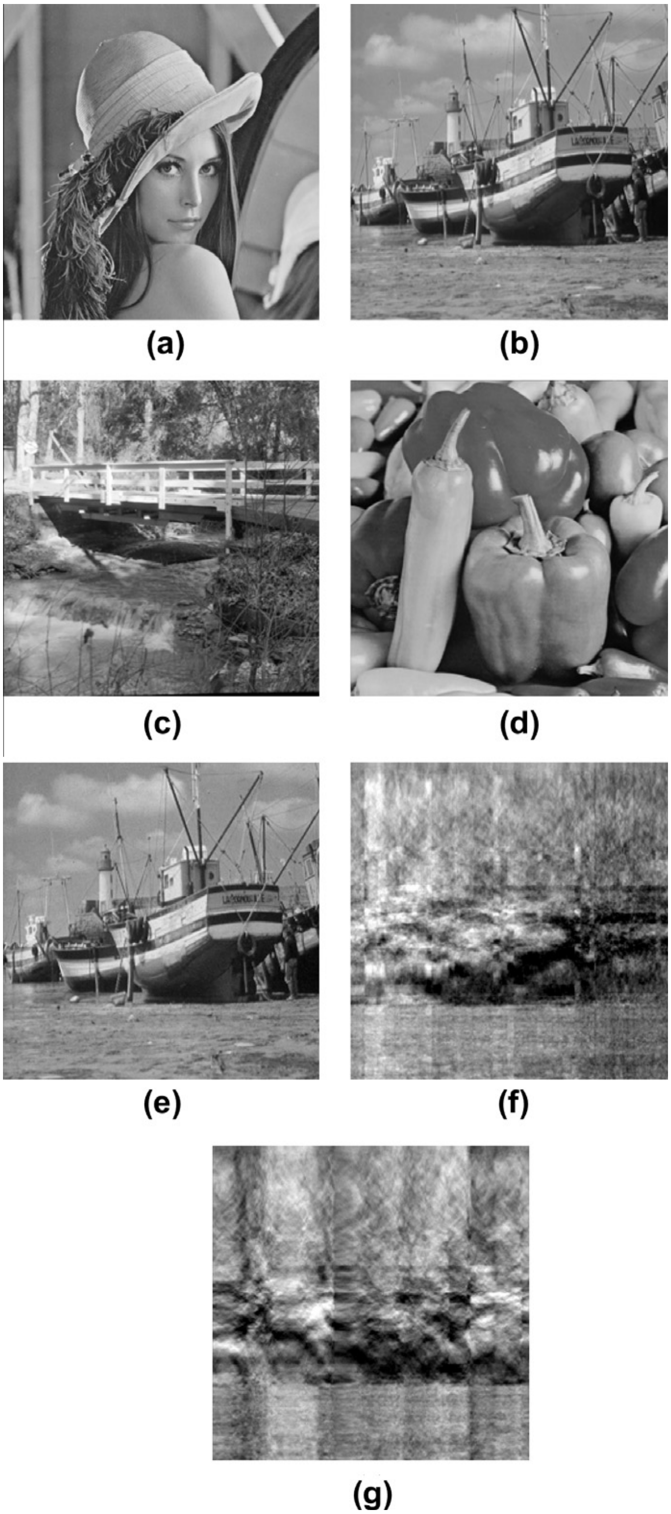


Fig. 3.1. A reliable SVD-based image watermarking.

and (b), respectively. Fig. 3.1(c) and (d) show two reference images for the validation in the watermark extraction step. Fig. 3.1(e) is the extracted watermark obtained using the matrix V_m^T from Fig. 3.1(b). Fig. 3.1(f) shows the extracted watermark by incorporating the right singular vector V_m^T from reference image in Fig. 3.1(c). By using the matrix V_m^T from Fig. 3.1(d), the extracted watermark is shown in Fig. 3.1(g).

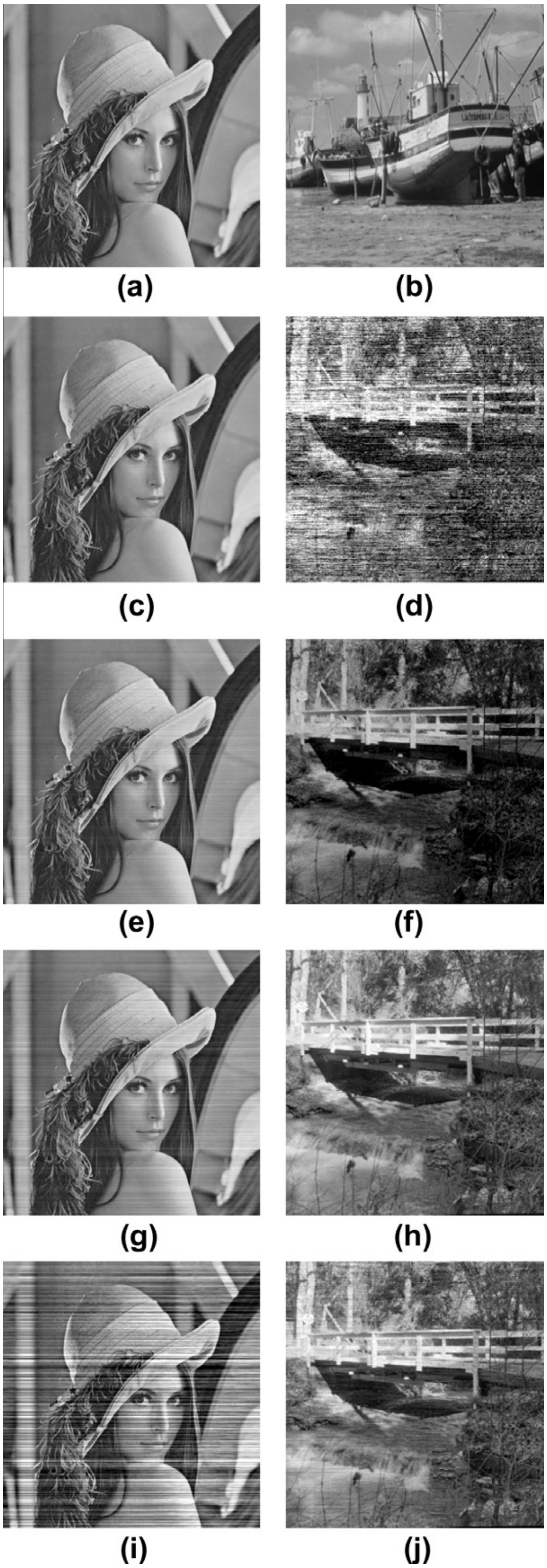


Fig. 3.2. The scaling factor problem.

Table 3.1
PSNR of the watermarked image and correlation coefficient of extracted watermark.

Scaling factor α	PSNR of watermarked image	Correlation coefficient of extracted watermark
0.01	38.3987	0.5107
0.05	31.1601	0.5929
0.1	20.1663	0.7032
0.5	18.3621	0.8171

Without knowing the original principal component and the right singular vectors, it is impossible to get the watermark from any arbitrary reference image.

3.2. Problem with the reliable SVD-based watermarking scheme

The minor problem occurred in the reliable SVD-based watermarking scheme is about the transparency, because Jain et al. (2008) only used the scaling factor in the scalar value. In most of literature the scaling factor is chosen between 0 and 1, $0 < \alpha \leqslant 1$. It is actually a hard step for choosing the suitable scaling factor. Usually, the scaling factor is chosen to be a scalar value.

Fig. 3.2(a) and (b) show the original and watermark images. Fig. 3.2(c), (e), and (g), and (i) show the watermarked images using different scaling factors, i.e. $\alpha = 0.01$, 0.05, 0.1, and 0.5, respectively. The extracted watermarks are shown in Fig. 3.2(d), (f), (h), and (j).

Table 3.1 shows the PSNR of the watermarked image and the correlation coefficient of the extracted watermark for several scaling factors. From this table, the higher scaling factor is, the worse the robustness and invisibility of watermark will be.

Based on this experiment, the reliable SVD-based watermarking scheme can solve the ownership problem, but choosing the suitable scaling factor is a crucial issue in this scheme. In this paper, the metaheuristic algorithm is incorporated for selecting the suitable scaling factor to satisfy the robustness and invisibility.

4. The proposed method

The basic idea of the proposed method is presented in Section 4.1. The first and second proposed methods are discussed in Section 4.2. The method for obtaining the suitable scaling factor using metaheuristic algorithm is presented in Section 4.3.

4.1. Basic idea

By leading the fact that SVD subspace can preserve the significant amount of information of an image, the new method for image watermarking is proposed. In the proposed method, the principal components of the watermark are embedded into the host image in the transform domain (either DCT or DWT). The insertion of principal components of the watermark image can solve the main drawback in the SVD-based image watermarking.

The scaling factor in the matrix form is chosen rather than in the scalar value. The scaling factor can be represented as:

$$\Delta = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{bmatrix}. \tag{4.1}$$

The values of scaling factor are obtained by implementing a metaheuristic algorithm. In this paper, the particle swarm optimization is chosen for the metaheuristic algorithm.

4.2. The reliable SVD-based image watermarking scheme

The principal components of the watermark image are imbedded into the host image in the transformed domain; two methods are proposed. In the first method, the host image is transformed first using the discrete cosine transform (DCT). In the second method, the host image is transformed by applying the discrete wavelet transform (DWT). Then the principal components of the watermark are inserted into the transformed host image.

Let A be the host image of size $M \times M$, and W be the watermark of size $\frac{M}{2} \times \frac{M}{2}$. For the simplicity, the host and watermark images are square matrix.

4.2.1. First method: DCT-SVD based image watermarking

The watermark embedding and extraction algorithms are stated as follows:

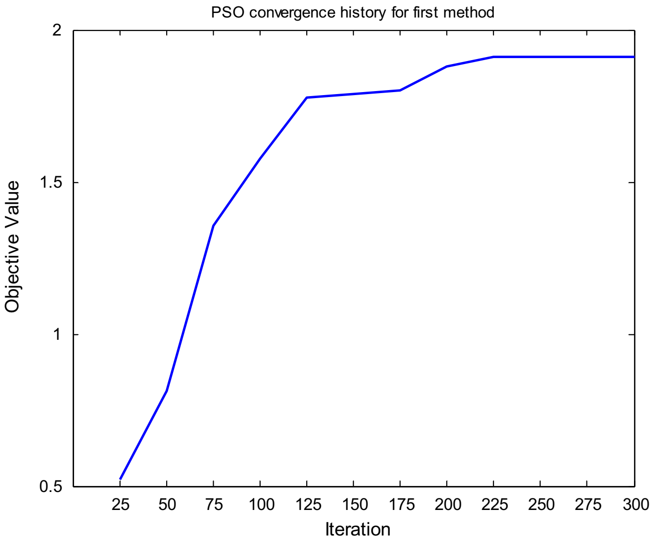


Fig. 5.1. PSO convergence history for the first method.

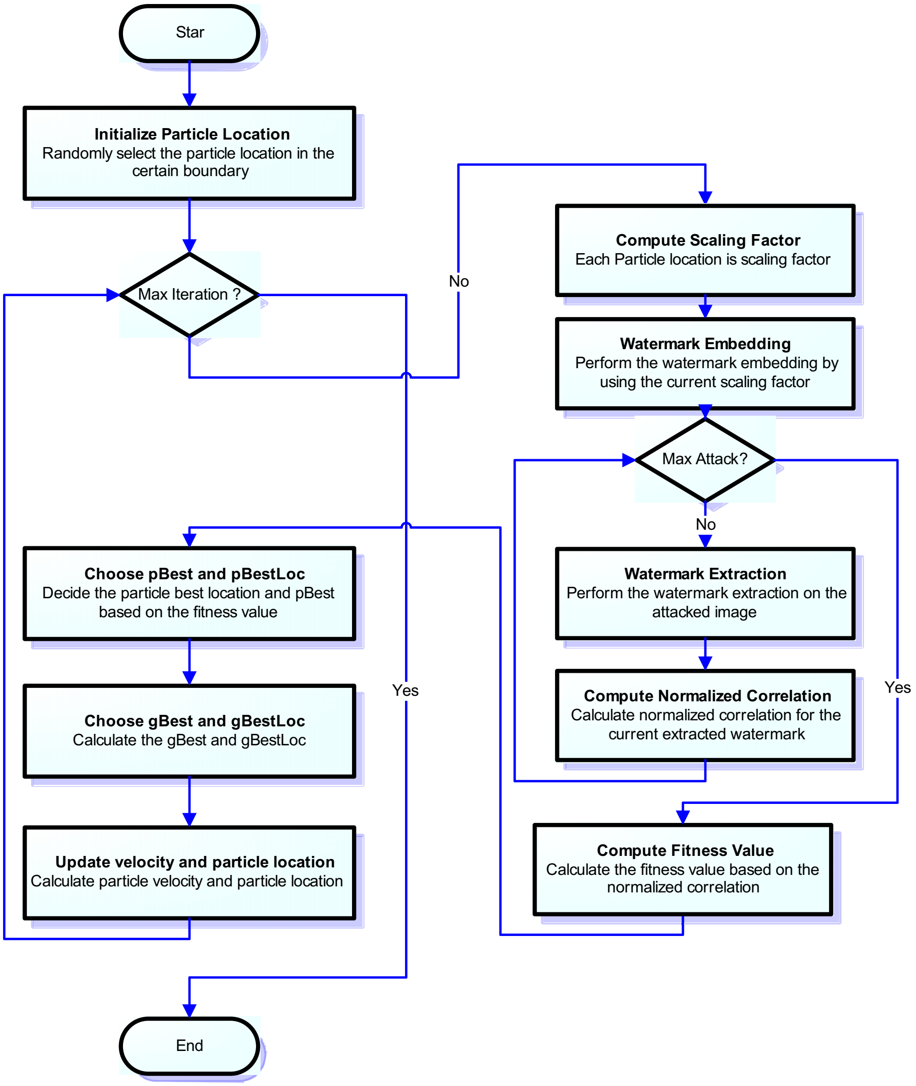

Star
Initialize Particle Location
Randomly select the particle location in the certain boundary
Max Iteration ?
No
Yes
Compute Scaling Factor
Each Particle location is scaling factor
Watermark Embedding
Perform the watermark embedding by using the current scaling factor
Max Attack?
No
Yes
Watermark Extraction
Perform the watermark extraction on the attacked image
Compute Normalized Correlation
Calculate normalized correlation for the current extracted watermark
Compute Fitness Value
Calculate the fitness value based on the normalized correlation
Choose pBest and pBestLoc
Decide the particle best location and pBest based on the fitness value
Choose gBest and gBestLoc
Calculate the gBest and gBestLoc
Update velocity and particle location
Calculate particle velocity and particle location
End

Fig. 4.1. Flowchart for PSO algorithm for finding scaling factor.

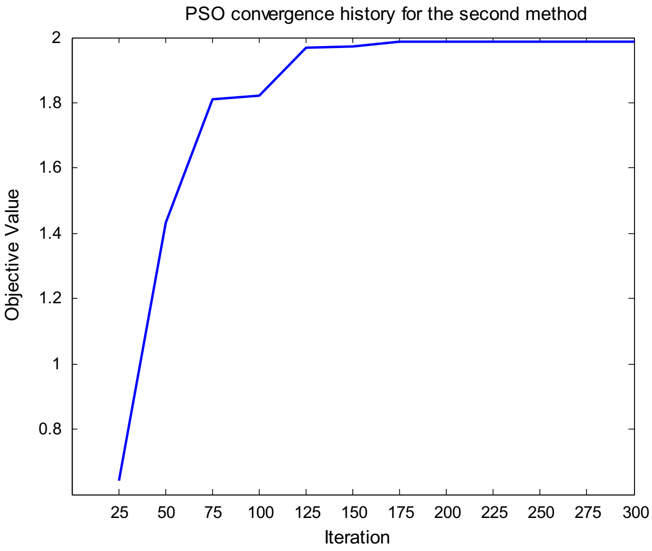
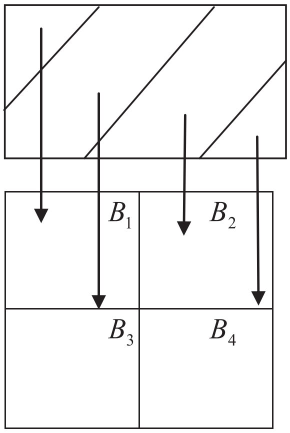


Fig. 5.2. PSO convergence history for the second method.

4.2.1.1. Watermark embedding algorithm.

1. Perform the discrete cosine transform to the host image, A.
2. Using the zig-zag sequence, map the DC coefficients into four quadrants: B_1, B_2, B_3, B_4.



3. Apply the SVD to each sub-band, $B_k \Rightarrow U_k \Sigma_k V_k^T$, where $k = \{1,2,\ldots,4\}$.
4. Perform the SVD on the watermark image, $W \Rightarrow U_w \Sigma_w V_w^T$.
5. Calculate the principal components of the watermark image, $A_{wa} = U_w \Sigma_w$.
6. Modify the singular values of the DCT transformed host image with the principal components, $\Sigma_1^k = \Sigma_k + \Delta \bullet A_{wa}$, where $k = \{1,2,\ldots,4\}$. The symbol $\bullet$ denotes the dot product multiplication. In this step, the scaling factors in the matrix form, Δ, are obtained using particle swarm optimization (PSO).
7. Perform $A_w^k = U_k \Sigma_1^k V_k^T$ for $k = \{1,2,\ldots,4\}$.

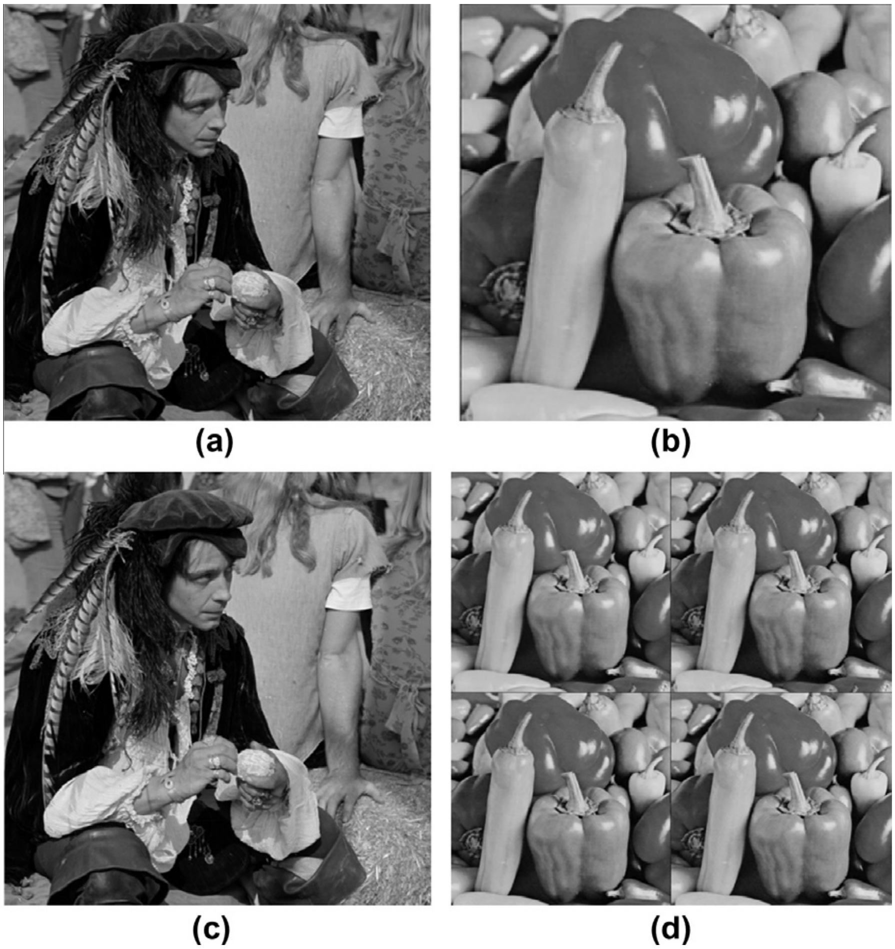


Fig. 5.3. Result of the first proposed method.

8. Map the A_w^k coefficients back to their original positions, where $k = \{1,2,\ldots,4\}$.
9. Apply the inverse discrete cosine transform to produce the watermarked image, A_w.

4.2.1.2. Watermark extraction algorithm.

1. Apply the discrete cosine transform (DCT) on the possibly distorted watermarked image, A_w^*.
2. Using the zig-zag sequence, map the DCT coefficients into four quadrants, $B_1^*,\ B_2^*,\ B_3^*,\ B_4^*$.
3. Subtract each quadrant with the original transformed quadrants, $A_1^k = B_k^* - B_k$, where $k = \{1,2,\ldots,4\}$.
4. Obtain the distorted principal components for each sub-band, $A_{wa}^{k*} = U_k^T A_1^k V_k \circ \Delta$, where $k = \{1,2,\ldots,4\}$. The symbol $\circ$ means the division operation using the element-by-element wise. In Jain et al. (2008), for computing possibly distorted principal components, the author used $A_{wa} = \frac{1}{\alpha}(U^{-1}A_1(V^T)^{-1})$. Based on the orthogonality of left and right singular vectors, $UU^T = U^TU = I_M$ and $VV^T = V^TV = I_N$, the inverse matrix of U and V are the same with its transpose matrix, i.e. $U^T = U^{-1}$ and $V^T = V^{-1}$. So, in this paper, we use $A_{wa} = \frac{1}{\alpha}(U^TA_1V)$ rather than $A_{wa} = \frac{1}{\alpha}(U^{-1}A_1(V^T)^{-1})$. It then can improve the running time.
5. Construct the extracted watermark image for each sub-band, $W^{k*} \Leftarrow A_{wa}^{k*}V_w^T$, where $k = \{1,2,\ldots,4\}$.

4.2.2. Second method: DWT-SVD based image watermarking

The algorithms for the discrete wavelet transform-singular value decomposition (DWT-SVD) image watermarking are described in the following.

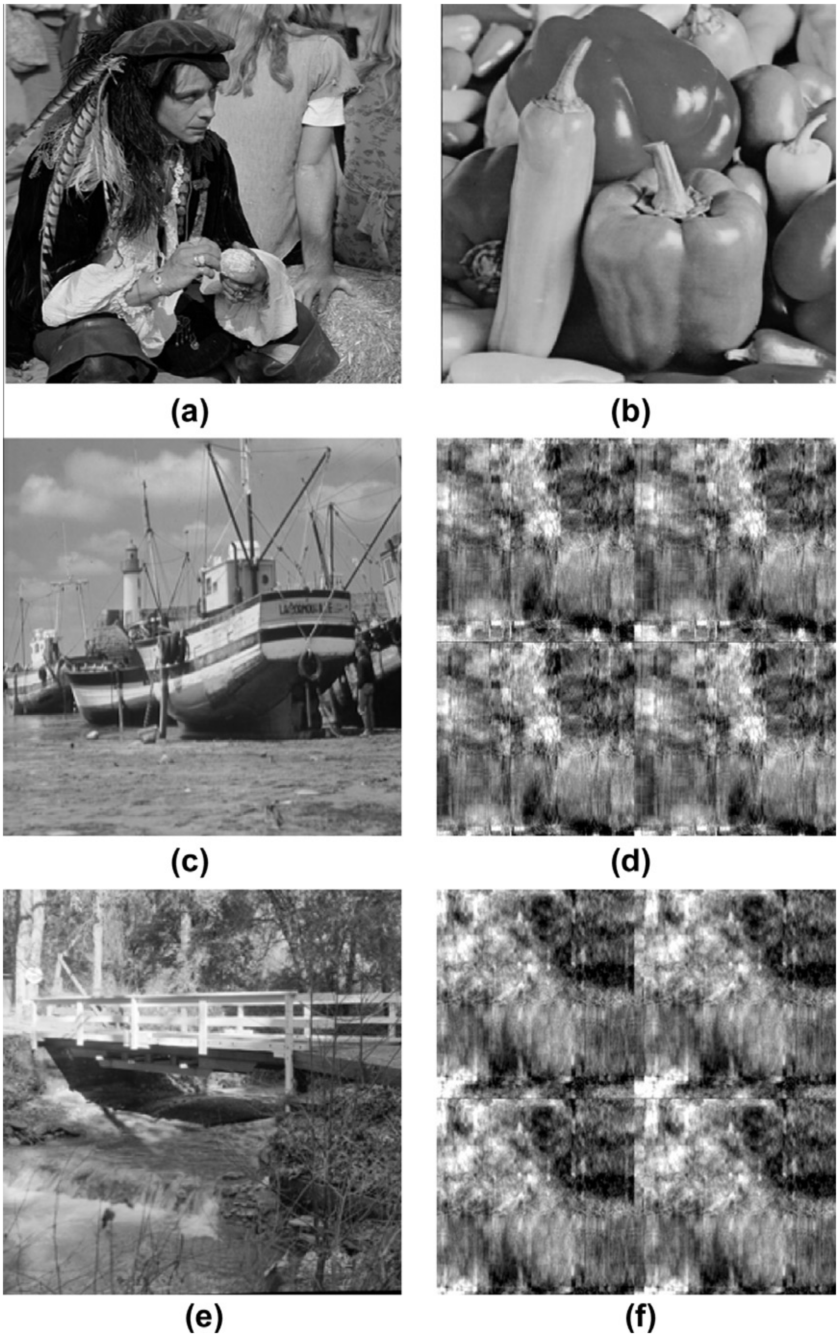
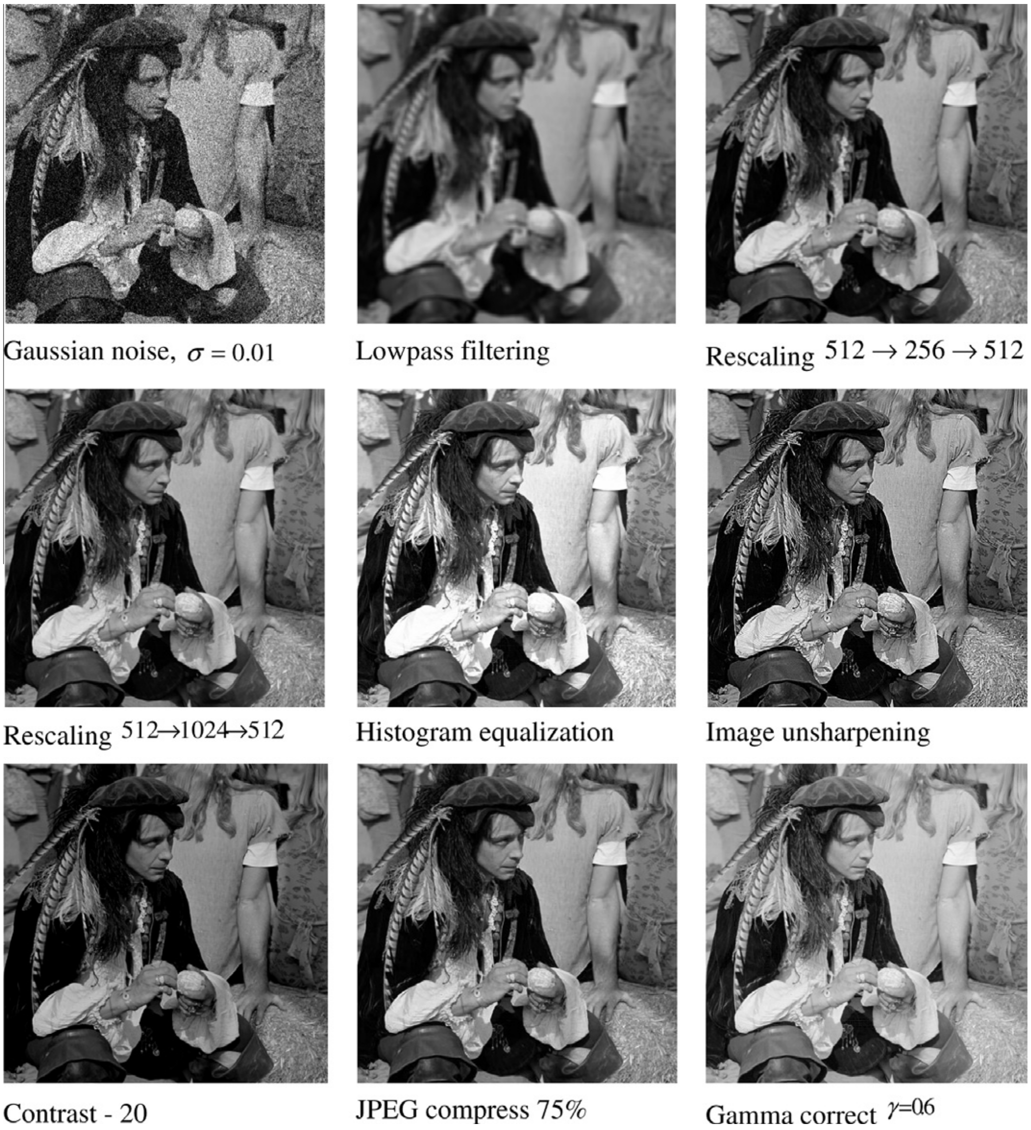

(a)
(b)
(c)
(d)
(e)
(f)

Fig. 5.4. Reliability test of the first proposed method.



Gaussian noise, $\sigma = 0.01$

Lowpass filtering

Rescaling $512 \to 256 \to 512$

Rescaling $512 \to 1024 \to 512$

Histogram equalization

Image unsharpening

Contrast - 20

JPEG compress 75%

Gamma correct γ=0.6

Fig. 5.5. Attacked watermarked images for the first proposed method.

4.2.2.1. Watermark embedding algorithm.

1. The host image A is decomposed using the discrete wavelet transform (DWT) into four sub-bands: the approximation coefficients LL, and the detailed coefficients HL, LH, HH. $A \Rightarrow \{A^{LL}, A^{LH}, A^{HL}, A^{HH}\}$.

LL	LH
HL	HH

2. Perform SVD operation for each sub-band of the host image, $A^k \Rightarrow U_k \Sigma_k V_k^T$, where $k = \{LL, LH, HL, HH\}$.
3. Apply SVD operation on the watermark image, $W \Rightarrow U_w \Sigma_w V_w^T$.
4. Compute the principal components of the watermark imageA_{wa}, $A_{wa} = U_w \Sigma_w$.
5. Insert the principal components of the watermark into the singular values of the host image in each sub-band, $\Sigma_1^k = \Sigma_k + \Delta \bullet A_{wa}$, where $k = \{LL, LH, HL, HH\}$. Here, the scaling factor Δ is obtained from the PSO algorithm. In this step, multiplication between the principal components and the scaling factor is a dot product.
6. Compute the modified coefficients for each sub-band, $A_w^k = U_k \Sigma_1^k V_k^T$, where $k = \{LL, LH, HL, HH\}$.
7. Perform the inverse discrete wavelet transform (IDWT) on the modified coefficients for each sub-band,A_w^k, where, $k = \{LL, LH, HL, HH\}$, to obtain the watermarked image, A_w.

4.2.2.2. Watermark extraction algorithm.

1. Apply the discrete wavelet transform (DWT) on the possibly attacked watermarked image, $A_w^* \Rightarrow \left\{A_w^{LL*}, A_w^{LH*}, A_w^{HL*}, A_w^{HH*}\right\}$.
2. Subtract the possibly attacked watermarked image for each sub-band with the original sub-band coefficients, $A_1^k = A_w^{k*} - A^k$, where $k = \{LL, LH, HL, HH\}$.

3. Compute the distorted principal components for each sub-band, $A_{wa}^{k*} = U_k^T A_1^k (V_k) \circ \Delta$, where $k = \{LL, LH, HL, HH\}$. In this step, the division operation on Δ is performed on element-by-element wise.
4. Obtain the extracted watermark for each sub-band, $W^{k*} \Leftarrow A_{wa}^{k*} V_w^T$, where $k = \{LL, LH, HL, HH\}$.

4.3. Computing scaling factor using particle swarm optimization

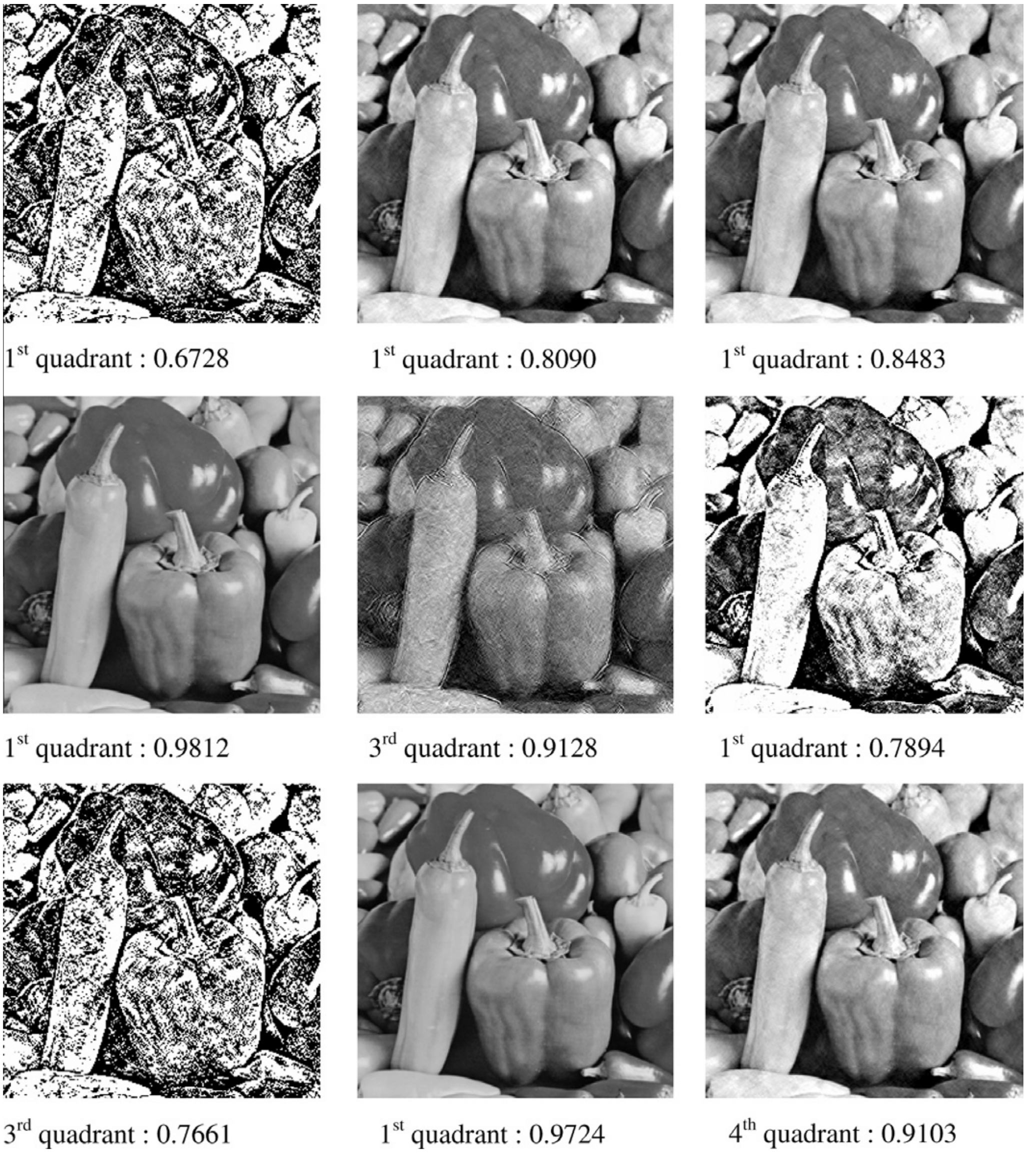
The scaling factor is a key point in the SVD-based image watermarking. This value controls the robustness and transparency of the watermarked image. In most of literatures, the scaling factor is chosen to be a positive value, i.e., 0.2. We argue that the scaling factor is image-dependent. Different watermarks need the different scaling factors, although they are embedded in the same host image.

Because of the difficulty for finding the suitable value of scaling factor, Δ, the metaheuristic algorithm can be used to find the scaling value. There are several kinds of metaheuristic algorithms, e.g. genetic algorithm, ant colony, particle swarm optimization, and etc. In this paper, the particle swarm optimization algorithm is used. Particle swarm optimization (PSO) is an evolutionary computation technique and population driven algorithm, inspired by social behavior of swarm or bird flocking. In PSO, each particle keeps track of its coordinates in the problem space which are associated with the best solution (fitness) it has achieved so far.

In this paper, the scaling factor Δ is obtained using single objective function PSO. For each iteration in PSO, the value of Δ is examined for several attacks, such as histogram equalization, sharpening, noise additive, and etc. At the end of PSO iteration, we will obtain the near optimum scaling factor. PSO cannot guarantee to find the exact value for the scaling factor, Δ. Fig. 4.1 shows the flowchart of PSO algorithm for finding the suitable scaling factor, Δ.

The mathematical modeling for PSO to find the scaling factor is given as follows:

- Objective function: $\max\left\{\frac{1}{R}\sum_{t=1}^{R} Corr_t(W, W^*) + Corr(A, A_w)\right\}$, where W and W^* (A and A_w) are the original watermark (host image) and extracted watermark (watermarked image), respec-



1st quadrant : 0.6728

1st quadrant : 0.8090

1st quadrant : 0.8483

1st quadrant : 0.9812

3rd quadrant : 0.9128

1st quadrant : 0.7894

3rd quadrant : 0.7661

1st quadrant : 0.9724

4th quadrant : 0.9103

Fig. 5.6. Extracted watermark images with several attacks.

tively.$Corr_t(W,W^*)$ denotes the normalized correlation between the original watermark W and extracted watermark W^* (when the watermarked image is attacked with specific attack t). The value $Corr(A,A_w)$ denotes the normalized correlation between the host image and the watermarked image.

- Decision variable: scaling factor,

$$\Delta=\begin{bmatrix}\alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn}\end{bmatrix}.$$

- Constraint: $-100 \leqslant \alpha_{ij} \leqslant 100$, for $1 \leqslant i,j \leqslant n$ and $\alpha_{ij} \neq 0$ (this constraint is to avoid the division by zero in the watermark extraction step).

5. Experimental results

This section presents the experimental setup and results for the reliable SVD-based image watermarking. The image used in the experiment is explained in Section 5.1. The PSO parameters are described in Section 5.2. The experimental results are shown in Section 5.3.

5.1. Host image and watermark image

The images used in the experiments are of size 512 × 512 for the cover images and of size 256 × 256 for the watermark images. The similarity between W (the original watermark) and W^* (the extracted watermark) can be measured by means of normalized correlation. The normalized correlation is defined as:

$$Corr(W,W^*)=\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(W_{ij}-\bar{W})\left(W_{ij}^{*}-\overline{W^*}\right)}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(W_{ij}-\overline{W})^2}\cdot\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}\left(W_{ij}^{*}-\overline{W^*}\right)^2}}, \tag{5.1}$$

$$\overline{W}=\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}W_{ij},$$

$$\overline{W^*}=\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}W_{ij}^{*}.$$

The quality of the watermarked image can be estimated using peak signal-to-noise ratio (PSNR) in (5.2).

$$PSNR=10\log\frac{255^2}{MSE}, \tag{5.2}$$

$$MSE=\frac{1}{MM}\sum_{i=1}^{M}\sum_{j=1}^{M}(A-A_w)^2,$$

where A and A_w are the original host image and the watermarked image.

5.2. The PSO parameters

We choose the PSO algorithm with the linearly inertia weight. The parameters for the PSO algorithm are chosen to be:

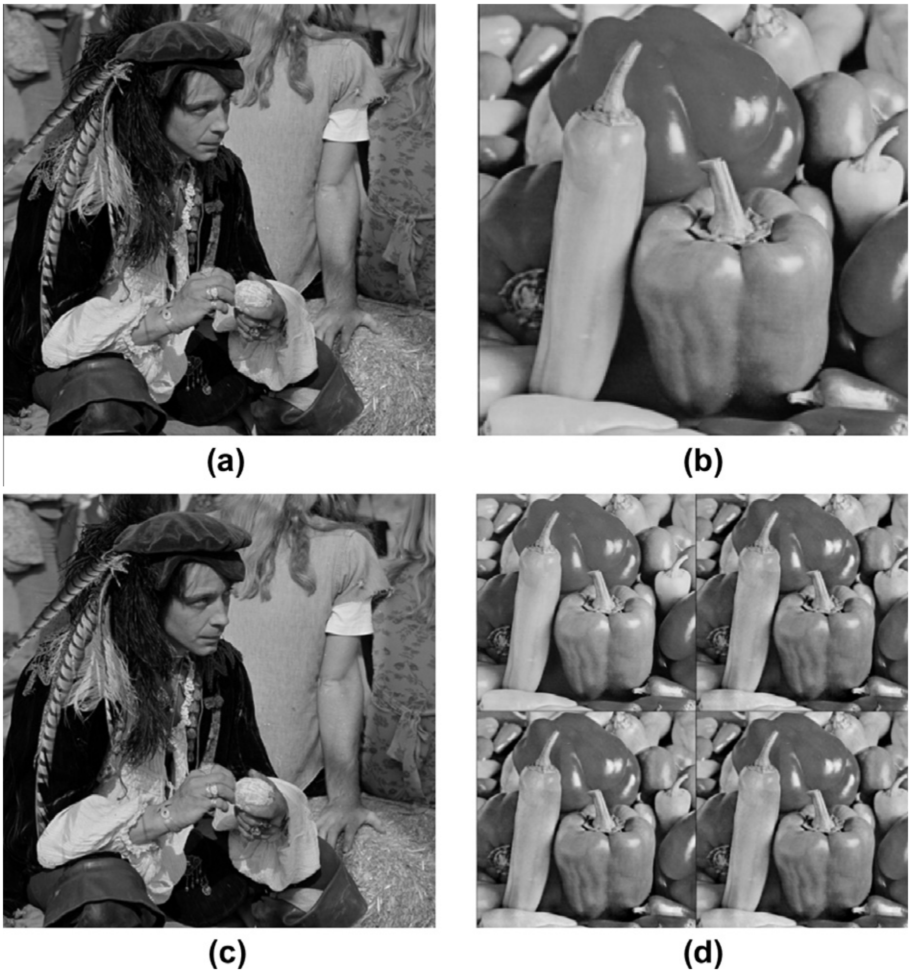


Fig. 5.7. Result of the second proposed method.

- The value of acceleration constant, c_1, is set to be 2.
- The value of acceleration constant, c_2, is set to be 2.
- The lower bound weight, $\underline{w}$, is set to be 0.
- The upper bound weight, $\bar{w}$, is set to be 1.
- The maximum velocity (velocity limit), $v^{\max}$, is set to be 0.5.
- The decision variable is set randomly in the range $\alpha_{ij} = [-100, 100]$, where $1 \leqslant i, j \leqslant 256$ for each particle.
- Maximum iteration is 300.
- The number of particles is 50.

Because of the computation time burden, we only set the maximum iteration and the number of particles to be 300 and 50, respectively.

5.3. Results of PSO algorithm

The PSO convergence history for the first and second method can be shown in Figs. 5.1 and 5.2, respectively. In this experiment, Man and Peppers images are chosen to be the host and watermark images. For saving the computation time, only 9 attacks are used in this experiment. After several iterations, the PSO algorithm will converge in a specific value. We use this value as scaling factor.

5.4. Robustness test for the first method

In this experiment, we investigate the robustness of the first proposed method. The Man and Peppers are chosen to be the host

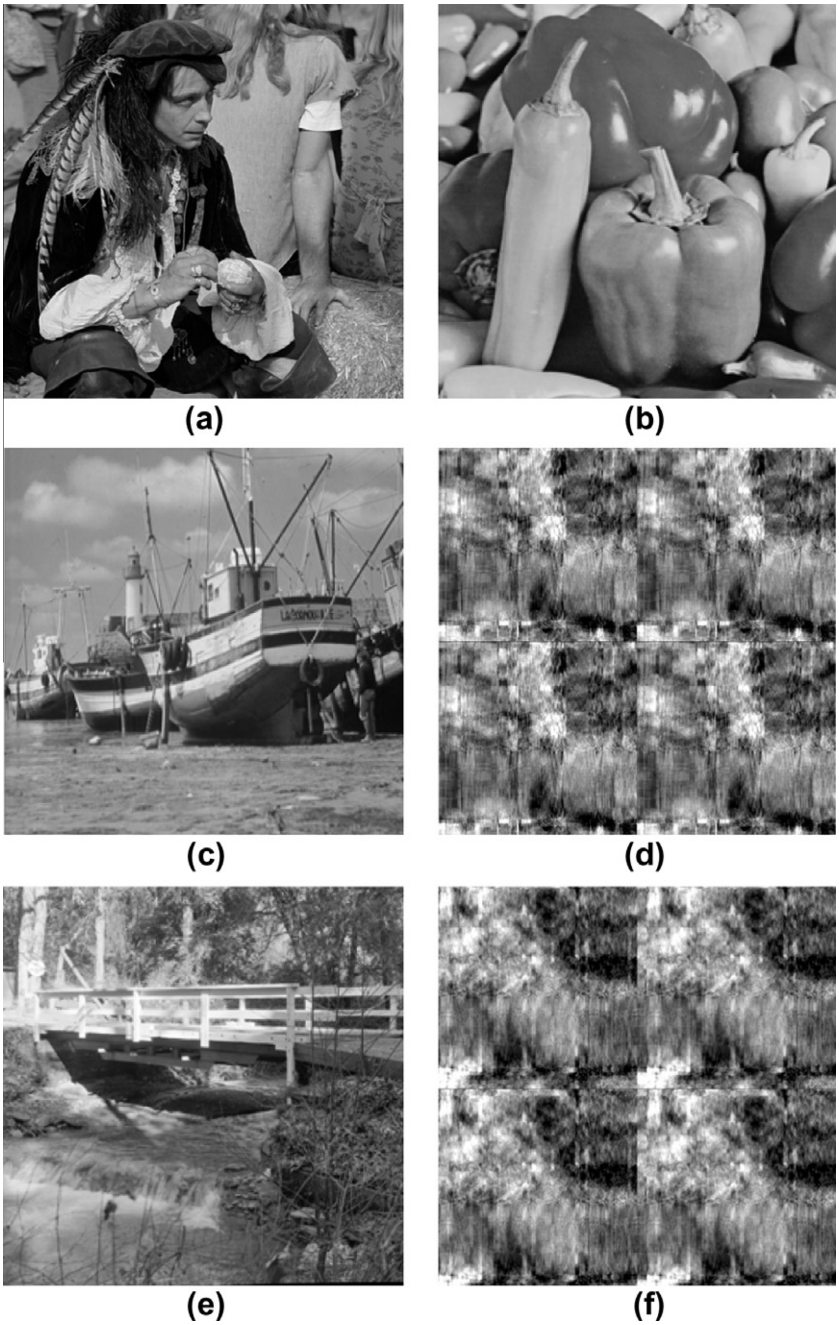


Fig. 5.8. Reliability test for the second proposed method.

image of size 512 × 512 and watermark image of size 256 × 256, respectively.

Fig. 5.3(a) and (b) show the original host image and watermark image, respectively. The watermarked image is given in Fig. 5.3(c). The PSNR value between the original host image and watermarked image is 32.17. It means that the quality of watermarked image is acceptable and watermark image is invisible for human visual. Fig. 5.3(d) shows the extracted watermark for each quadrant. Since we embed the watermark for all quadrants, in the watermark detection stage we will get the four extracted watermarks. The correlation coefficients for the 1st, 2nd, 3rd, and 4th quadrant are 0.9871, 0.9912, 0.9772, and 0.9861, respectively. Based on these values, the extracted watermark is nearly the same with the original watermark image.

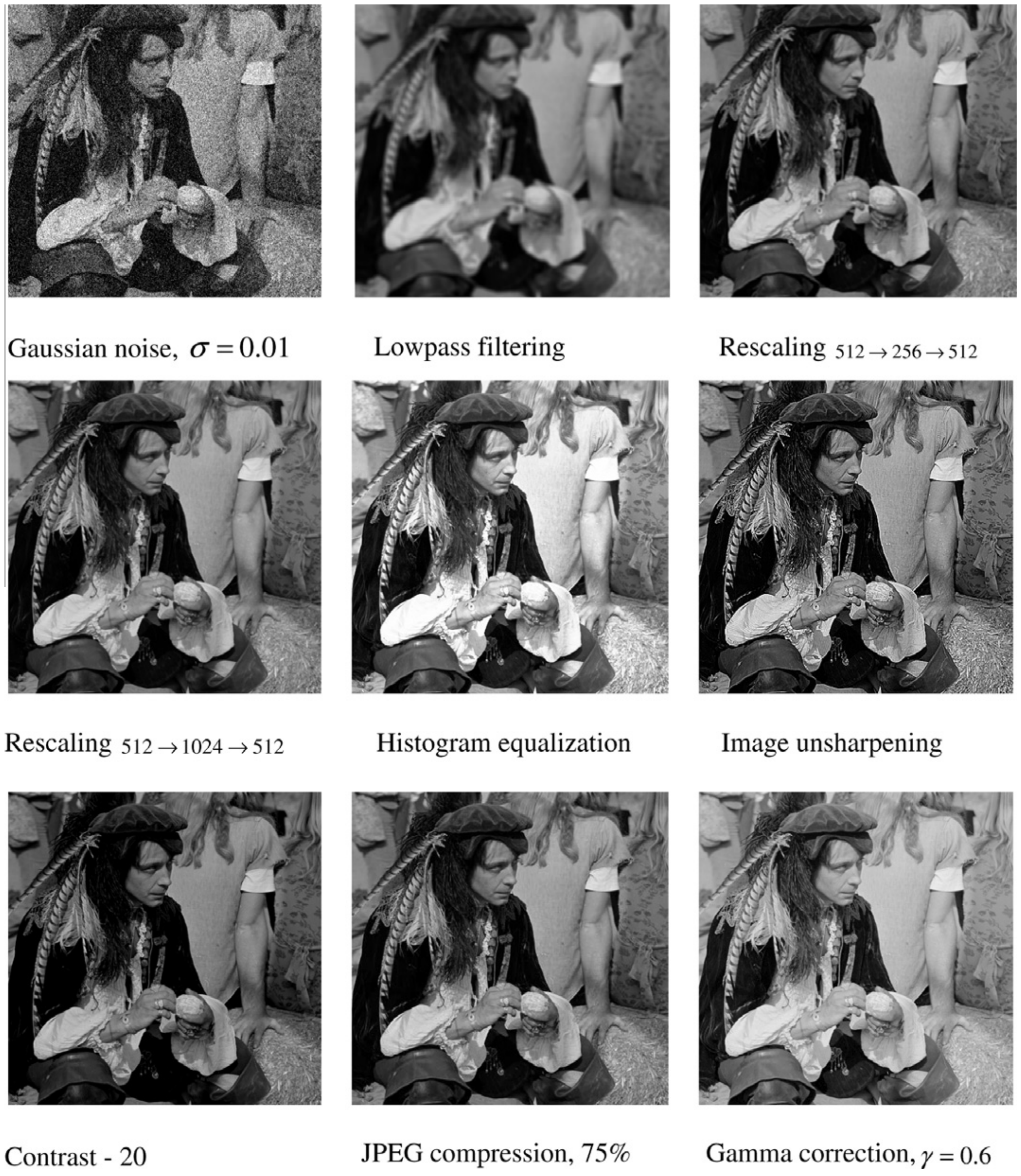
Another experiment is conducted for testing the reliability of the first proposed method. Fig. 5.4(a) and (b) show the watermarked image and original watermark image. In the watermark extraction stage, the extracted watermark is shown in Fig. 5.4(d) if Boat image, as shown in Fig. 5.4(c), is used for detection. Fig. 5.4(f) is the extracted watermark if Bridge image shown in Fig. 5.4(e) is chosen for extraction. Fig. 5.4(d) and (f) show the reliability of the first proposed method. The original watermark image cannot be detected using arbitrary reference image.

The robustness of the first proposed method against the image manipulation is also carried out in the experiment. Fig. 5.5 shows the attacked watermarked image with several attacks in common image processing. Because of the computation expense in the PSO algorithm step, we only use 9 attacks.

Fig. 5.6 shows the extracted watermark when the watermarked image is attacked with the image manipulation. Only the extracted watermarks with the maximum correlation coefficient are given in Fig. 5.6. The extracted watermark from 1st sub-band has the maximum correlation coefficient (0.6728) against Gaussian noise. In several attacks, the 1st quadrant is more robust rather than the other quadrants.

5.5. Robustness test for the second method

Fig. 5.7 shows the watermark result using the second proposed method. Fig. 5.7(a) and (b) show the original host image and origi-


Gaussian noise, $\sigma = 0.01$

Lowpass filtering

Rescaling $512 \rightarrow 256 \rightarrow 512$

Rescaling $512 \rightarrow 1024 \rightarrow 512$

Histogram equalization

Image unsharpening

Contrast - 20

JPEG compression, 75%

Gamma correction, $\gamma = 0.6$

Fig. 5.9. Attacked watermark images for the second proposed method.

nal watermark image, respectively. The watermarked image and extracted watermark are given in Fig. 5.7(c) and (d). In the watermark extraction step, we will get four extracted watermark images, because we embed the watermark in all sub-bands, LL, LH, HL, and HH. The correlation coefficients of the extracted watermark are 0.9778, 0.9823, 0.9899, and 0.9917, for LL, LH, HL, and HH sub-bands, respectively.

Reliability test for the second proposed method is given in Fig. 5.8. Any arbitrary reference images cannot be used for extracting the watermark image. The Boat and Bridge images cannot detect the original watermark image, Peppers.

Fig. 5.9 shows the attacked watermarked image with embedding process as suggested in the second proposed method.

The extracted watermark images and the corresponding maximum correlation coefficients are given in Fig. 5.10. For several attacks, the LL sub-band is more robust than the other sub-bands.

5.6. Comparison

Fig. 5.11 depicts the comparison result between the correlation coefficient of the proposed method and that of the pure SVD-based

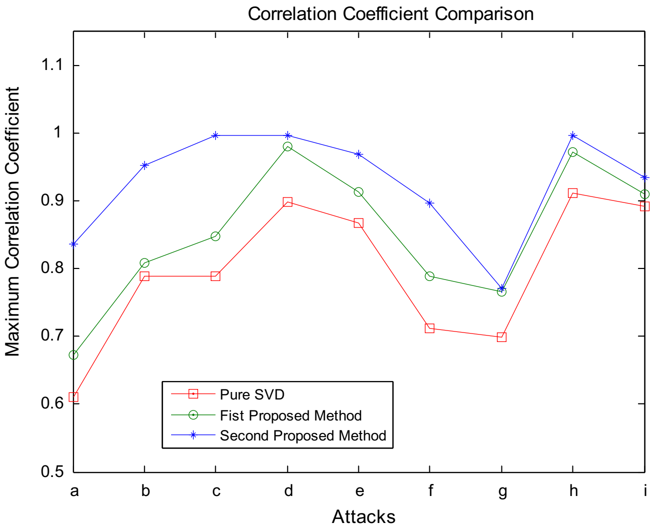
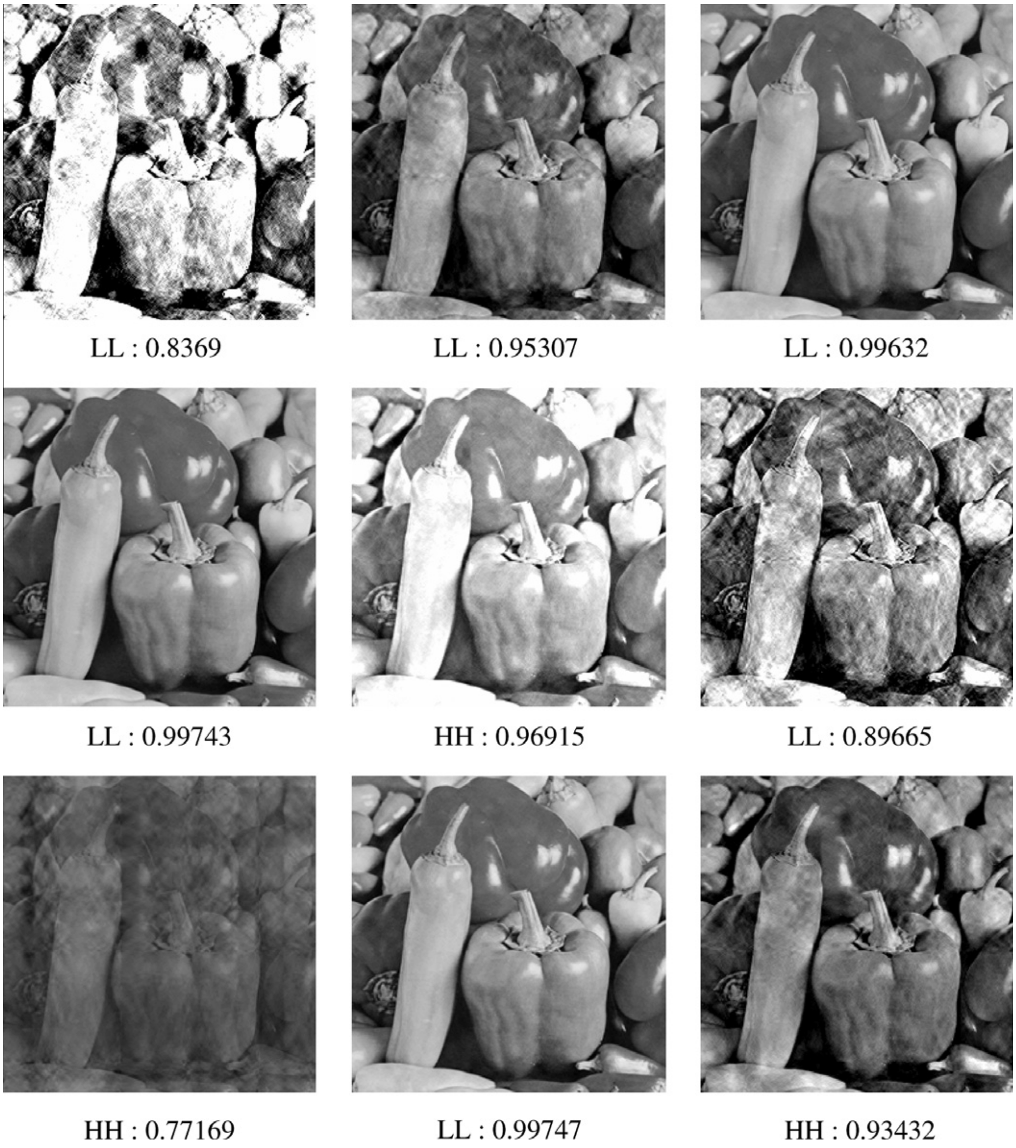


Fig. 5.11. Correlation coefficient comparison.


LL : 0.8369

LL : 0.95307

LL : 0.99632

LL : 0.99743

HH : 0.96915

LL : 0.89665

HH : 0.77169

LL : 0.99747

HH : 0.93432

Fig. 5.10. Extracted watermark images with several attacks.

Table 5.1
PSNR for several watermarking technique.

Watermarking technique	PSNR
Second method	33.93
First method	32.17
Pure SVD	30.79

image watermarking (Jain et al., 2008) using PSO for choosing the suitable scaling factor. For the comparison purpose, the pure SVD is implemented using scaling factor in matrix form (we obtain this value using PSO algorithm also) rather than in a scalar value as suggested in Jain et al. (2008). In Fig. 5.11, the first and second methods have the better correlation than that of the pure SVD. For the attack g, the correlation coefficient drops significantly for all methods. Attacks a-i in Fig. 5.11 are the same attacks in Figs. 5.5 and 5.9.

Table 5.1 shows the PSNR comparison result between the first method, second method, and pure SVD-based image watermarking by incorporating PSO for finding the suitable scaling factor. From this table, the watermarked image quality using the first and second methods is nearly the same. There is no meaningful difference between the first, second and pure SVD-based watermarking in the image quality aspect. The PSNR of watermarked image using the first, second proposed methods and the pure SVD is higher than 30 and acceptable.

6. Conclusions

Based on the experimental results, we derive the conclusions in the following. The proposed method can solve the ambiguities situation and false positive problem. An attacker cannot get the desired watermark image without knowing the original watermark. The invisibility and robustness of the watermarked image are satisfied by employing the first and second proposed methods. The second method gives the better correlation coefficient under several attacks than the first method and pure SVD based. The maximum correlation coefficient for the first method is better than the pure SVD based. The PSNR for the second method is the best but the other two are also acceptable.

References

Abdallah, Emad E., Ben Hamza, A., & Bhattacharya, Prabir (2007). Improved image watermarking scheme using fast Hadamard and discrete wavelet transforms. *Journal of Electronic Imaging, 16*(3), 0330201–0330209.

Alexander, S., Scott, D., & Ahmet, M. E. (2005). Robust DCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies. In *Proceedings of the 13th European Signal Processing Conference (EUSIPCO2005)*, Antalya, Turkey.

Bhatnagar, Gaurav, & Raman, Balasubramanian (2009). A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces, 31*(5), 1002–1013.

Chandra, D. 2002. Digital image watermarking using singular value decomposition, In *Proceedings of the IEEE 45th Midwest Symposium on Circuits and Systems*, Oklahoma State University, USA, (Vol. 3, August 4–7, pp. 264–267).

Cox, I., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). *Secure spread spectrum watermarking for multimedia. IEEE Transaction on Image Processing* (6). New Jersey, USA: Piscataway, pp. 1673–1687.

Ganic, E., & Eskicioglu, A. M. 2004. Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In *Proceedings of the ACM Multimedia and Security workshop*, Magdeburg, Germany (pp. 166–174).

Ghazy, R., El-Fishawy, N., Hadhoud, M., Dessouky, M., & El-Samie, F. 2007. An efficient block-by block SVD-based image watermarking scheme, In *Proceedings of the 24th National Radio Science Conference*, Cairo, Egypt (pp. 1–9).

Huang, Fangjun, & Guan, Zhi-Hong (2004). A hybrid SVD-DCT watermarking method based on LPSNR. *Pattern Recognition Letters, 25*(15), 1769–1775.

Ientilucci, Emmett J. (2003). Using Singular Value Decomposition. <http://www.cis.rit.edu/~ejipci/Reports/svd.pdf>.

Jain, C., Arora, S., & Panigrahi, P. K., (2008). A reliable SVD based watermarking scheme, adsabs.harvard.edu/abs/2008arXiv0808.0309J.

Liu, F., & Liu, Y. 2008. A watermarking algorithm for digital image based on DCT and SVD, In *IEEE Congress on Image and Signal Processing*, Sanya, Hainan, China, 1 (pp. 380–383).

Liu, R., & Tan, T. (2002). *An SVD-based watermarking scheme for protecting rightful ownership. IEEE Transactions on Multimedia* (4). New Jersey, USA: Piscataway, pp. 121–128.

Mohammad, Ahmad A., Alhaj, Ali, & Shaltaf, Sameer (2008). An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Processing, 88*(9), 2158–2180.

Ouhsain, Mohamed, & Ben Hamza, A. (2009). Image watermarking scheme using nonnegative matrix factorization and wavelet transform. *Expert Systems with Applications, 36*(2), 2123–2129. Part 1.

Patra, J. C., Soh, W., Ang, E. L., & Meher, P. K. 2006. An Improved SVD-based watermarking technique for image and document authentication. In *IEEE Asia Pacific Circuits and Systems (APCCAS 2006)*, Singapore (pp. 1984–1987).

Seitz, J., & Jahnke, T. (2005). Digital watermarking: An introduction. In *Digital watermarking for digital media* (pp. 19–20). Hershey, Pennsylvania, USA: Information Science Publishing.

Shieh, Jieh-Ming, Lou, Der-Chyuan, & Chang, Ming-Chang (2006). A semi-blind digital watermarking scheme based on singular value decomposition. *Computer Standards & Interfaces, 28*(4), 428–440.

Sverdlov, A., Dexter, S., & Eskicioglu, A. M. 2005. Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies. In *Proceedings of 13th European Signal Processing Conference (EUSIPCO2005), Antalya*, Turkey (pp. 4–8).