Signal Processing 88 (2008) 2158–2180

Contents lists available at ScienceDirect

Signal Processing

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

An improved SVD-based watermarking scheme for protecting rightful ownership

Ahmad A. Mohammad *, Ali Alhaj, Sameer Shaltaf

Princess Sumaya University for Technology, P.O. Box 2226, Al-Jubailha, Amman 11941, Jordan

ARTICLE INFO

Article history:
Received 11 December 2006
Received in revised form
4 February 2008
Accepted 29 February 2008
Available online 15 March 2008

Keywords:
Singular value decomposition
Digital watermarking
Ownership protection
Multimedia

ABSTRACT

In this paper, a new SVD-based digital watermarking scheme for ownership protection is proposed. The proposed algorithm solves the problem of false-positive detection. In addition, it enjoys all the advantages of SVD-based schemes. Instead of using a randomly generated Gaussian sequence, a meaningful text message is used. Thus, clarity of the extracted message determines the performance of the algorithm. Analytical and experimental developments show that the proposed algorithm is robust and secure. Comparisons with other algorithms indicate that the proposed algorithm is robust against most common attacks. In particular, the algorithm proved to be extremely robust against geometrical distortion attacks.

1. Introduction

With the widespread use of computers and Internet, access and exchange of digital data became an extremely simple task [1–3]. As a result, illegal reproduction of digital information started to pose a real problem. This has raised questions and concerns about ownership rights [2]. Digital watermarking provides a solution for this problem [2].

In short, digital watermarking refers to embedding a secret imperceptible signal (watermark) in the original data [1]. Basic characteristics of watermarking techniques are [1]:

- Perceptual transparency: This means that human eyes should not be able to detect the presence of the watermark in a watermarked image. In other words, a watermarking algorithm is imperceptible if one cannot distinguish original (cover) data from that with the embedded watermark.
- Capacity or payload: This is the number of bits that an algorithm can embed in a watermark. One should note that capacity is application dependant [4,5].
- Watermark granularity: This defines the amount of host data needed to embed one unit of watermark information.
- Robustness: In many applications, the watermark needs to withstand intentional and unintentional attacks on host data. In these applications, the watermark should be detectable after attacks. Examples of such attacks include filtering, resizing, lossy compression, and the addition of noise. So far there is no precise measure of robustness. However, robustness means that an attacker should not be able to remove or destroy the watermark without causing a large degradation to host data. In authenticity applications, the watermark is required to be fragile. In this case, any change to host data should damage the watermark [1,2].
- Security: Just like encryption techniques, the use of a secret code (key) increases watermarking techniques security.

1.1. The problem of ownership protection

One of the most important applications of watermarking is protecting digital data ownership rights [1–22]. As was shown in [17], extracting the watermark

* Corresponding author.
E-mail address: atawayha@psut.edu.jo (A.A. Mohammad).

0165-1684/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2008.02.015

from a watermarked image is not enough to prove ownership. More specifically, authors of [17] have shown that most existing watermarking techniques are not capable of providing an unambiguous answer to ownership rights. For most of these techniques, there exists a counterfeit attack. Authors of [6] gave a set of sufficient conditions that watermarks and watermarking schemes must meet in order to resolve the problem of ownership proof. Two main conditions are given. The first one requires the use of meaningful watermarks instead of using random sequences. The second one requires the use of non-invertible watermarking algorithms. The next section discusses the concept of invertibility in more details. Thus far, it is fair to say that none of the existing watermarking techniques can give a trustworthy solution to the ownership problem [2,11,12,20]. In summary, the use of meaningful watermarks and non-invertible watermarking algorithms can be combined with cryptography in order to give a well-accepted notion of security [2,12,19].

1.2. Classification of watermarking schemes

There are two main categories of watermarking techniques [23]. The first one is the spatial domain methods and the second is the transform methods. In general, spatial domain methods are less complex but are more fragile (not robust). On the other hand, transform domain methods are more robust, more complex, and numerically demanding. Typical transform methods used discrete cosine transform (DCT) [24–29], discrete wavelet transform [23,30–35], discrete Fourier transform [9,36–39], and singular value decomposition (SVD) [2,5,8,27,28,33,40–56]. Examples of spatial domain methods can be found in [1,3,57–64].

This paper presents an SVD-based watermarking technique. This technique is an improved version of the SVD-based technique proposed by Liu and Tan [2]. As will be shown, the proposed technique is non-invertible. Hence, its main application is in protecting rightful ownership. Simulation results show that the proposed method is robust and can resist common attacks such as rotation, resizing, cropping, noise, and JPEG compression.

1.3. Organization

The rest of this paper proceeds as follows: Section 2 introduces the problem of rightful ownership. Section 3 introduces SVD and its use in watermarking. Section 4 presents the proposed method. Section 5 presents experimental results. Finally, Section 6 gives the conclusion.

2. Invertibility and the problem of rightful ownership

As was mentioned earlier, the problem of ownership protection has received a great deal of researchers' attention [1–22]. One should notice that non-invertibility is a necessary but not sufficient condition for using a watermarking technique in copyright protection. In short, non-invertibility means that it is computationally unfeasible to decompose the watermarked image into a faked image and a faked watermark [2]. In order to understand non-invertibility, we present the definition of invertible watermarking schemes. Following the notations of Liu and Tan [2], assume that the $N\times M$ matrix A represents the original un-watermarked image, the $Q\times R$ matrix W represents the watermark and the $N\times M$ matrix A_W represents the watermarked image. Let the $\oplus$ symbol represent the watermark embedding operation as follows:

$$A \oplus W \rightarrow A_W \tag{1}$$

or

$$A_W = E(A, W), \tag{2}$$

where $E(.)$ denotes some embedding algorithm.

Now, and without having A, if an attacker can obtain a counterfeit watermark W_f and a counterfeit original A_f that satisfies

$$A_W = E(A_f, W_f), \tag{3}$$

then the attacker can claim ownership of A_W by claiming that the original cover image is A_f and the watermark is W_f. A watermarking scheme satisfying (3) is said to be invertible; otherwise, it is non-invertible [2].

3. SVD domain watermarking

As was mentioned earlier, there are several SVD-based watermarking algorithms. This type of algorithms has proven to be robust. Refs. [64–67] give detailed properties and other applications for SVD. The following two sections present SVD and the SVD-based watermarking scheme.

3.1. Singular value decomposition (SVD)

Although SVD works for any $N\times M$ matrix A, and without loss of generality, our discussion will be limited for the $N\times N$ matrix. The SVD of the $N\times N$ matrix A is

$$A = U\Sigma V^{\mathrm{T}}, \tag{4}$$

where U and $V\in R^{N\times N}$ are unitary, and $\Sigma\in R^{N\times N}$ is a diagonal matrix and the superscript T denotes matrix transposition. The diagonal elements of Σ, denoted by σ_i's are called the singular values of A and are assumed to be arranged in decreasing order $\sigma_i > \sigma_{i+1}$. The columns of U denoted by U_i's are called the left singular vectors while the columns of V denoted by V_i's are called the right singular vectors of A. It is easy to see that σ_i, V_i and U_i satisfy:

$$AV_i = \sigma_i U_i, \tag{5}$$

$$U_i^{\mathrm{T}} A = \sigma_i V_i^{\mathrm{T}}. \tag{6}$$

3.2. SVD-based watermarking

Liu and Tan [2] proposed an SVD-based watermarking scheme for rightful ownership protection. Without loss of generality, A and W are assumed to be $N\times N$ square

matrices. Their algorithm consists of the following three steps:

1. Perform SVD on the original un-watermarked image

$$A = U\Sigma V^{\mathrm{T}}. \tag{7}$$

2. Add the watermark image W to Σ and obtain the reference watermark Σ_n as

$$\Sigma_n = \Sigma + \alpha W. \tag{8}$$

Then perform SVD on the reference watermark Σ_n as

$$\Sigma_n = \Sigma + \alpha W = U_W \Sigma_W V_W^{\mathrm{T}}. \tag{9}$$

3. Obtain the watermarked image A_W as

$$A_W = U\Sigma_W V^{\mathrm{T}}. \tag{10}$$

Here, α is a scale factor that controls the strength (energy) of the embedded watermark.

To extract the watermark from a possibly distorted watermarked image A_W^*, their algorithm proceeds as follows:

1. Perform SVD on the possibly distorted watermarked image A_W^* as

$$A_W^* = U^* \Sigma_W^* V^{*\mathrm{T}}. \tag{11}$$

2. Use U_W, V_W as obtained from (9) to obtain

$$D^* = U_W \Sigma_W^* V_W^{\mathrm{T}}. \tag{12}$$

3. Get the possibly distorted watermark W^* as

$$W^* = \tfrac{1}{\alpha}(D^* - \Sigma). \tag{13}$$

This algorithm requires U_W, Σ, and V_W to be available for detection.

Zhang and Li [44] have shown that this algorithm is fundamentally flawed. This is because it only embeds the diagonal matrix Σ_W. The detection algorithm simply extracts a possibly distorted diagonal matrix Σ_W^*. After that, the detection algorithm utilizes (does not extract) the singular vectors of the reference watermark (U_W and V_W). Zhang and Li [44] have shown that, by using the reference watermark SVD pair (U_W, V_W) in the detection stage, false-positive detection will have a probability of one. In other words, using the singular vectors of any fake watermark in the detection stage, one can always claim that this watermark was the embedded one. Hence, he can claim ownership of the watermarked image. In this paper, we propose a variation of Liu and Tan's algorithm. As opposed to their algorithm, the proposed algorithm overcomes the problem of false-positive detection. In addition, the proposed algorithm is robust and non-invertible.

4. The proposed SVD-based watermarking scheme

In this section, we present two versions of our algorithm. The first one assumes the size of the watermark W to be equal to the size of the original image A. The analysis of the technique uses this version. The second version partitions the original image into $M \times M$ blocks. This technique embeds one bit of the watermark in each block.

4.1. Technique 1

The following three steps summarize the embedding algorithm:

1. Perform SVD on the original image A:

$$A = U\Sigma V^{\mathrm{T}}. \tag{14}$$

2. Add the watermark image W to Σ, with a scale factor α as

$$\Sigma_n = \Sigma + \alpha W. \tag{15}$$

3. Obtain the watermarked image A_W:

$$A_W = U\Sigma_n V^{\mathrm{T}}. \tag{16}$$

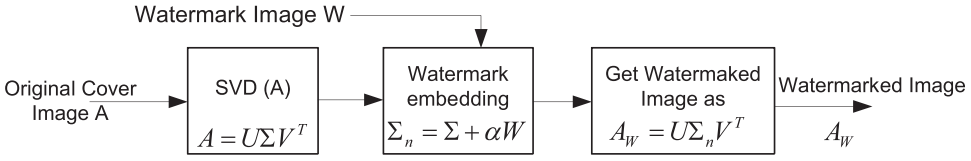


Fig. 1. Embedding sequence for technique 1.

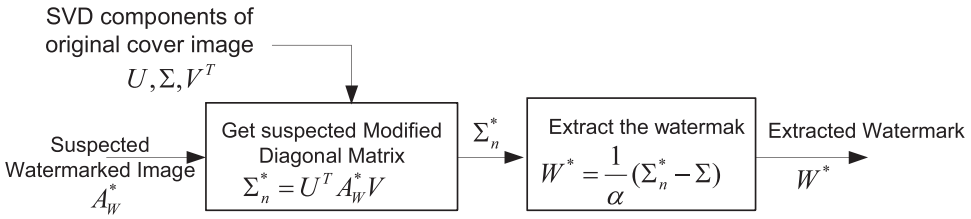


Fig. 2. Extraction sequence for technique 1.

Fig. 1 gives a block diagram for the embedding sequence. The main difference between this technique and that of Liu and Tan is that their algorithm only embeds the singular values of Σ_n while our algorithm embeds Σ_n. As was shown in [44], this is why Liu and Tan's algorithm turned out to be flawed. Notice also that while Liu and Tan's algorithm performs two SVD decompositions for A and Σ_n, our algorithm performs one SVD for A only. This means that our algorithm saves up to $15(N)^3$ computations (Flops).

Given the SVD components of the original un-watermarked image $A = U\Sigma V^T$ and a possibly corrupted watermarked image A_W^*, the extraction sequence proceeds as follows:

1. Obtain the corrupted matrix Σ_n^*as

$$\Sigma_n^* = U^T A_W^* V. \tag{17}$$

This will undo step 3 of the embedding algorithm.

2. Reverse step 2 of the embedding procedure to get a possibly distorted watermark W^* as follows:

$$W^* = \frac{1}{\alpha}(\Sigma_n^* - \Sigma). \tag{18}$$

Fig. 2 gives a block diagram for the extraction sequence. Note that, only the original cover image or its SVD components U, Σ, and V need to be available for extraction. This is another difference with Liu and Tan's algorithm. Their algorithm uses both the cover image and the singular vectors' matrices of Σ_n for extraction.

In order to measure the similarity between the original watermark W and the extracted watermark W^*, we calculate the correlation between W and W^*. For simplicity, W and W^* are converted to one-dimensional row vectors X and X^*. Eq. (19) defines the correlation

Table 1

	Liu and Tan's algorithm	Proposed algorithm
Embedding	a. Perform SVD $A = U\Sigma V^T$ b. Find $\Sigma_n = \Sigma + \alpha W$ c. Perform SVD $\Sigma_n = U_W \Sigma_W V^T{}_W$ *This will require $15(N)^3$ Flops more d. Watermarked image $A_W = U\Sigma_n V^T$ *Only Σ_W, the diagonal matrix of Σ_n, is embedded *Singular vectors U_W and V_W are not embedded	a. Perform SVD $A = U\Sigma V^T$ b. Find $\Sigma_n = \Sigma + \alpha W$ *No SVD of Σ_n is performed *This will save $15(N)^3$ Flops c. Watermarked image $A_W = U\Sigma_n V^T$ *Whole watermark is embedded
Extraction	a. Undo step d. of embedding to get the diagonal matrix $\Sigma_W = U^T A_W V$ *Only Σ_W, the diagonal matrix of Σ_n, is extracted b. Undo step c. of embedding to obtain the non-diagonal matrix $\Sigma_n = U_W \Sigma_W V^T{}_W$ *Σ_n is almost completely determined by reference watermark singular vectors U_W and V_W c. Undo step b. of embedding to obtain the watermark $W = (\Sigma_n - \Sigma)/\alpha = (U_W \Sigma_W V^T{}_W - \Sigma)/\alpha$ *Notice that W is almost completely determined by singular vectors U_W and V_W *This is the reason for false-positive detection; any pair of singular vectors U_W and V_W can be used forcing a false-positive detection	– a. Undo step c. of embedding to get the non-diagonal matrix $\Sigma_n = = U^T A_W V$ *The complete non-diagonal matrix Σ_n is extracted b. Undo step b. of embedding to obtain the watermark $W = (\Sigma_n - \Sigma)/\alpha$ *The complete watermark is extracted *This eliminates false-positive detection

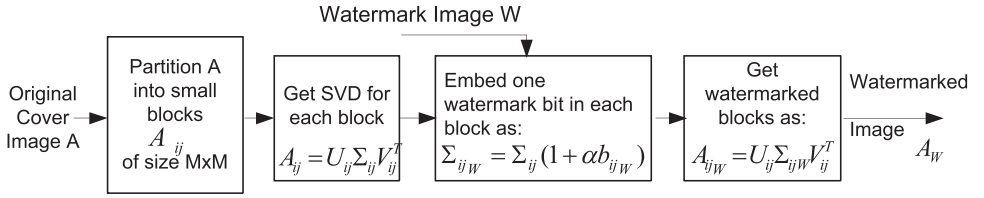


Fig. 3. Embedding sequence for technique 2.

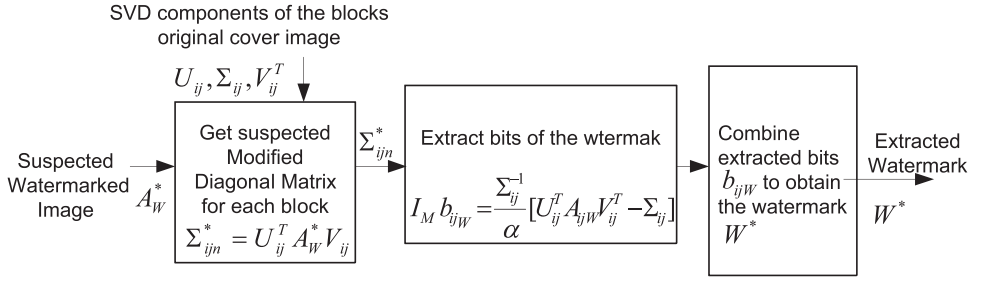


Fig. 4. Extraction sequence for technique 2.

coefficient $C(W, W^*)$ as

$$C(W, W^*) = \frac{X^* X^{\mathrm{T}}}{\sqrt{XX^{\mathrm{T}}}}. \tag{19}$$

Another method for measuring similarity between W and W^* is using the peak signal-to-noise ratio (PSNR) given by

$$\mathrm{PSNR}(W, W^*) = 10 \log_{10} L \frac{\text{Maximum } (X(i)^2)}{\sum_{i=1}^{L} (X(i) - X^*(i))^2}, \tag{20}$$

where L is the length of the vectors X and X^*. It is pointed out that both measures are used in the literature. Actually, one can use any similarity measure. The simulation section uses both measures.

4.2. Non-invertibility of the proposed technique

Suppose an attacker gets a watermarked image A_W without knowing the cover image A. The algorithm is invertible if an attacker can find a counterfeit watermark W_F and a counterfeit original A_F so that A_F and W_F satisfy:

$$A_F = U_F \Sigma_F V_F^{\mathrm{T}} \tag{21}$$

and

$$A_W = U_F \Sigma_{WF} V_F^{\mathrm{T}}, \tag{22}$$

$$A_W = U_F (\Sigma_F + \alpha W_F) V_F^{\mathrm{T}}, \tag{23}$$

$$A_W = U_F \Sigma_F V_F^{\mathrm{T}} + \alpha U_F W_F V_F^{\mathrm{T}}, \tag{24}$$

where (21) gives the SVD of A_F, and $\Sigma_{WF} = \Sigma_F + \alpha W_F$ is obtained from (22) as $\Sigma_{WF} = U_F^{\mathrm{T}} A_W V_F$. To accomplish this, the attacker may try to obtain a fake original A_F and a fake watermark W_F using one of the following two choices:

Choice 1: Starting with a known fake original A_F and given A_W, the attacker finds a fake watermark W_F by solving (24) for W_F by applying the following two steps:

a. Obtain SVD for the assumed fake original as

$$A_F = U_F \Sigma_F V_F^{\mathrm{T}}. \tag{25}$$

b. Find W_F from (23) as

$$W_F = \frac{1}{\alpha} (U_F^{\mathrm{T}} A_W V_F - \Sigma_F). \tag{26}$$

The solution in this case is easy to find and the algorithm is invertible. In addition, the resulting fake watermark W_F will not usually be meaningful.

Choice 2: Start with a known meaningful non-trivial fake watermark W_F and solve (24) for the SVD components of $A_F = U_F \Sigma_F V_F^{\mathrm{T}}$. If the SVD components of A_F are treated as three general independent components, Eq. (24) will have infinite number of solutions. One can find these solutions by assuming two of the three unknowns (U_F, Σ_F, and V_F) and solving (24) for the third one. However, only one of the solutions will correspond to the SVD components of A_F. The SVD components of this solution (U_F, Σ_F, and V_F) must satisfy the following three equations:

$$U_F^{\mathrm{T}} A_F = \Sigma_F V_F^{\mathrm{T}}, \tag{27}$$

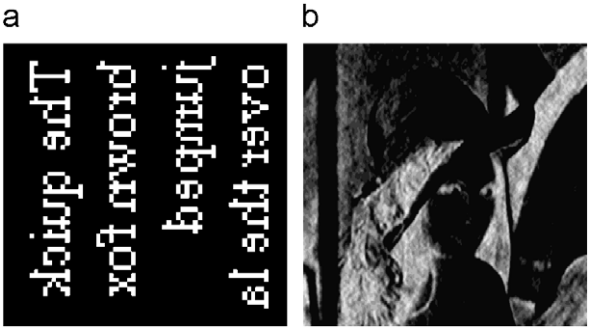


Fig. 7. Absolute error image: (a) via SVD and (b) via Cox.

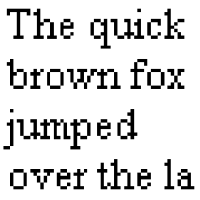


Fig. 5. Original watermark.

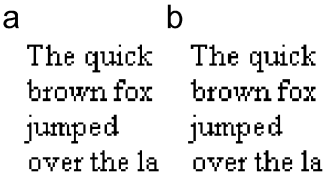


Fig. 8. Extracted watermark: (a) via SVD and (b) via Cox.

Fig. 6. Digital watermarking for Lena image: (a) original image, (b) watermarked image via SVD, and (c) watermarked image via Cox.

$$U_F U_F^{\mathrm{T}} = I, \tag{28}$$

$$V_F V_F^{\mathrm{T}} = I. \tag{29}$$

Here, I denotes the identity matrix. In order to find the desired solution, given A_W and W_F only, the attacker must simultaneously solve the equations:

$$A_W = U_F \Sigma_F V_F^{\mathrm{T}} + \alpha U_F W_F V_F^{\mathrm{T}}, \tag{30}$$

$$U_F^{\mathrm{T}} A_F = \Sigma_F V_F^{\mathrm{T}}, \tag{31}$$

$$U_F U_F^{\mathrm{T}} = I, \tag{32}$$

$$V_F V_F^{\mathrm{T}} = I. \tag{33}$$

These equations include terms of two and three unknown matrices multiplied by each other. This is highly nonlinear and has no closed form solution. Thus, the solution of these equations is not feasible, and for all practical purposes, the algorithm is non-invertible.

The previous development suggests that in order to have a non-invertible algorithm, we need to impose some conditions on the watermarking algorithm in addition to some restrictions on the watermark itself. These conditions are:

1. In order to use a watermarking algorithm in copyright protection, it must be inherently nonlinear. This means that simple addition of watermarks into the cover object is not acceptable. Instead, one must use a more complex algorithm such as transform-based algorithms. As was stated by Craver et al. [19] and Wu [8], the watermark must be a function of the cover object. Examples of transform methods are DFT, DCT, DWT, and SVD.

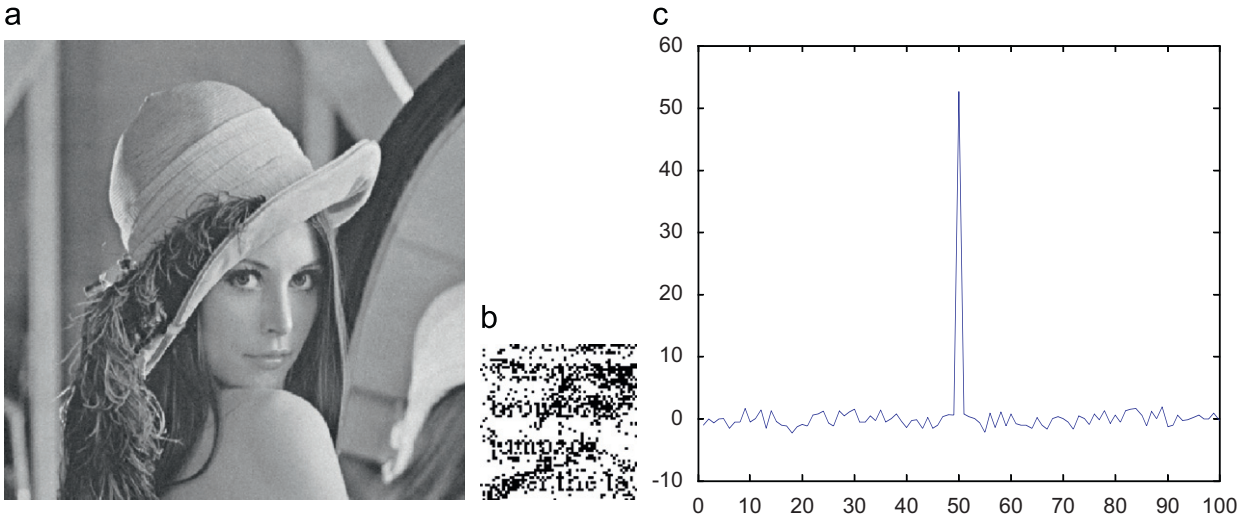


Fig. 9. Addition of Gaussian noise using SVD: (a) corrupted watermarked image, (b) extracted watermark, and (c) correlation coefficient.

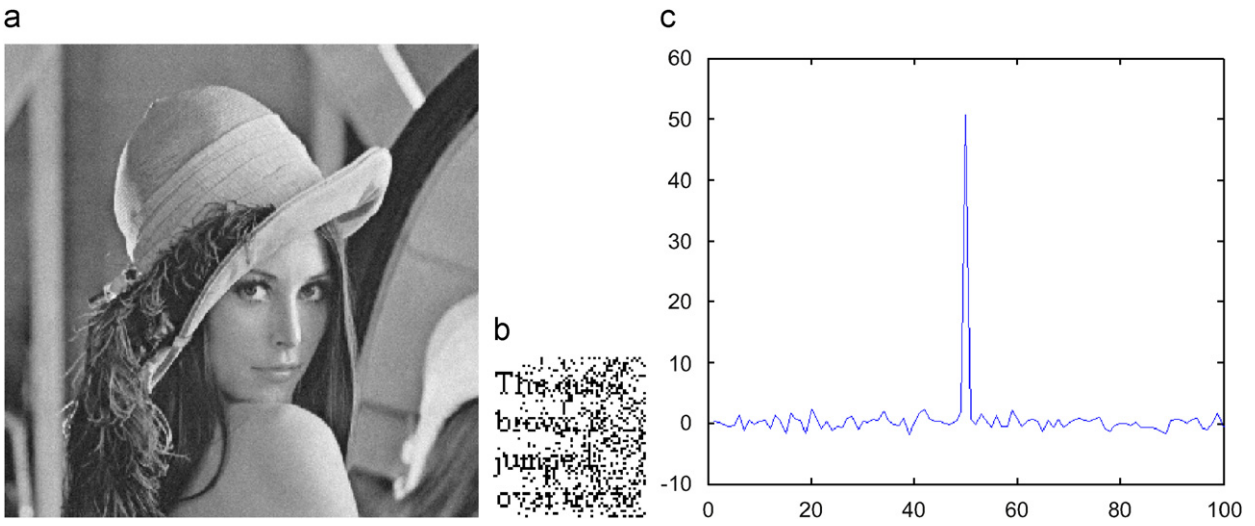


Fig. 10. Addition of Gaussian noise using Cox: (a) corrupted watermarked image, (b) extracted watermark, and (c) correlation coefficient.

2. The extraction algorithm must undo the embedding procedure in a pre-specified manner. Thus, if watermarking is carried out using DCT, the extraction must use inverse DCT, and if the embedding uses DWT, the extraction must use inverse DWT. In our case, SVD is used for watermarking and the fake original and the fake watermark A_F and W_F must satisfy:

$$A_W = U_F \Sigma_F V_F^{\mathrm{T}} + \alpha U_F W_F V_F^{\mathrm{T}} = A_F + \alpha U_F W_F V_F^{\mathrm{T}}. \quad (34)$$

Thus, the extraction technique is required to provide $A_F = U_F \Sigma_F V_F^{\mathrm{T}}$ and use this to solve for W_F as

$$W_F = \frac{1}{\alpha} U_F^{\mathrm{T}} (A_W - A_F) V_F. \quad (35)$$

This was shown to be almost impossible if A_F and W_F are required to be non-trivial and semantically or visually sound.

3. As was suggested in the previous section, the counterfeit watermark W_F must be semantically or visually sound. In order to make the solution for the counterfeit cover image A_F more difficult, W_F must not be of any simple special form such as diagonal form. Instead, it must be dense enough to make the solution for A_F extremely difficult.
4. Embedding needs to be strong enough to 'saturate' the original image so that it will be extremely difficult to:
   a. Remove the watermark without degrading the watermarked image.

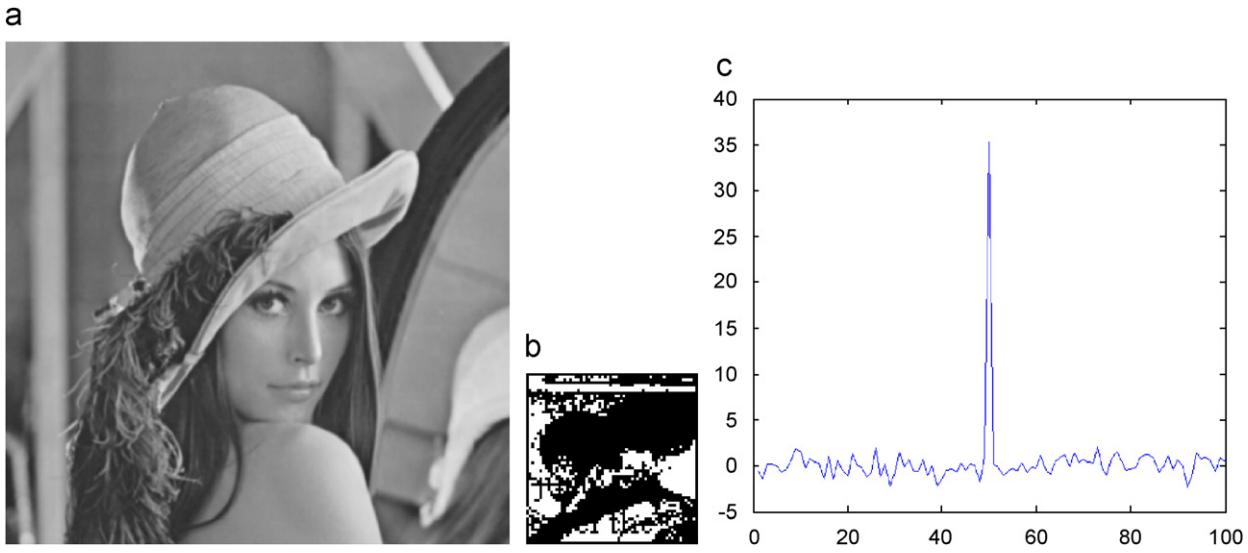


Fig. 11. Low pass filtering for SVD method only watermarked image is filtered: (a) filtered watermarked image, (b) extracted watermark, and (c) correlation coefficient.

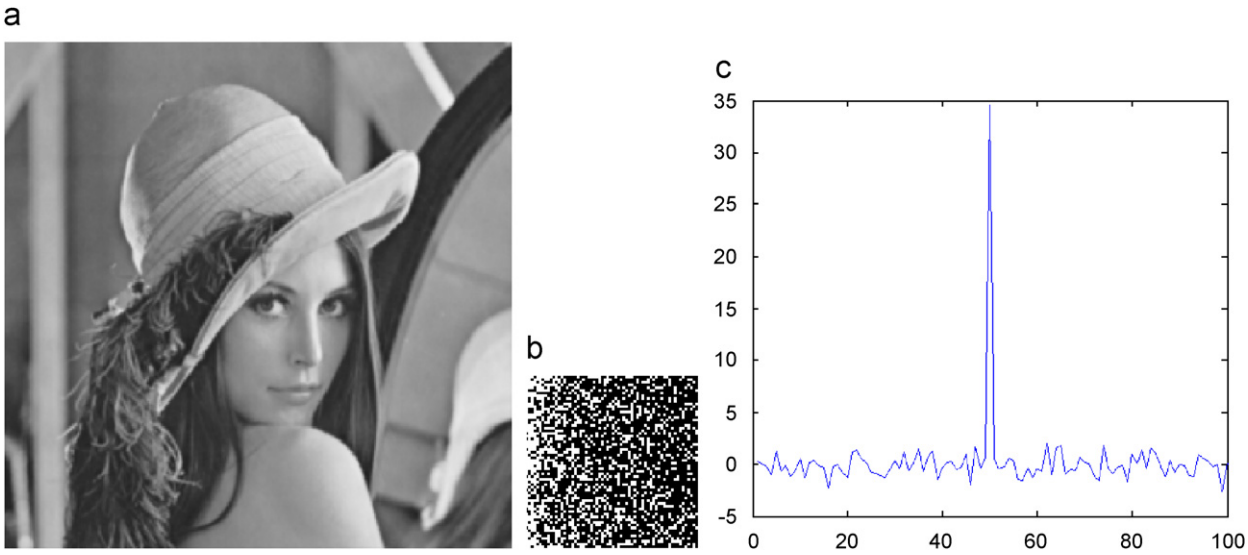


Fig. 12. Low pass filtering for Cox method only watermarked image is filtered: (a) filtered watermarked image, (b) extracted watermark, and (c) correlation coefficient.

b. Add another watermark in order to prevent multiple ownership claims. This means that one should choose the scaling factor α as large as possible without sacrificing transparency. In effect, this will increase robustness and make the addition of other watermarks harder.

4.2.1. Comparison with Liu and Tan's algorithm

In this section, we give a brief comparison between our algorithm and that of Liu and Tan. Table 1 gives a brief comparison between these two algorithms.

The previous developments show that the proposed algorithm has the following advantages over that of Liu and Tan:

1. Our algorithm prevents false-positive detection by embedding and extracting the whole watermark.
2. For a cover image and a watermark of size $N \times N$ each, Liu and Tan's algorithm requires $15(N)^3$ more calculations compared to the proposed algorithm. This is mainly because that the latter performs one SVD operation while the former one performs two SVD operations.

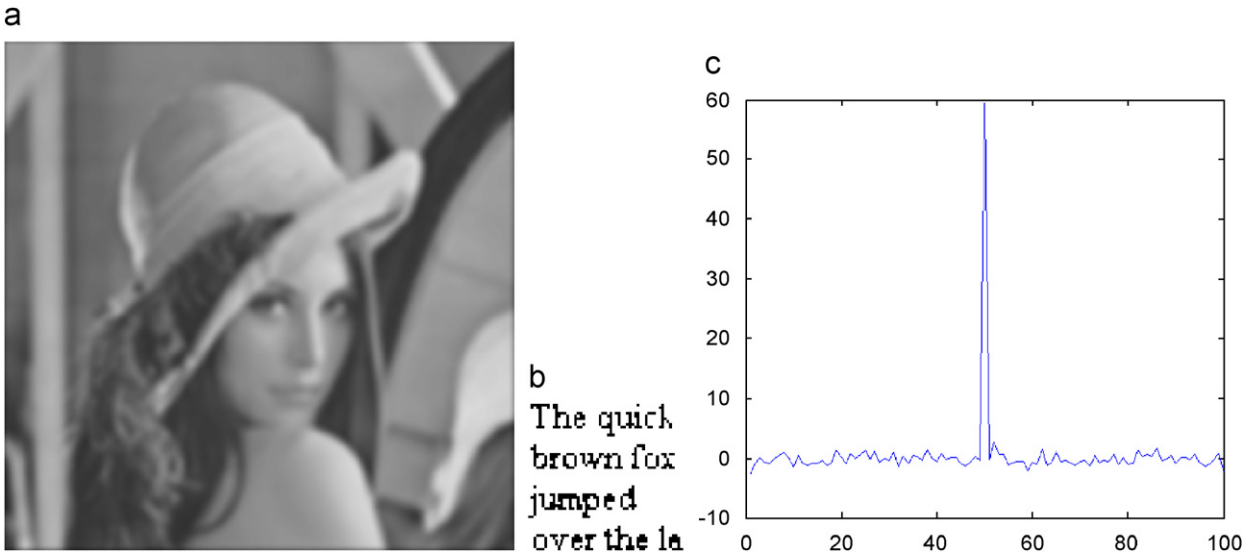


Fig. 13. Low pass filtering for SVD method both original and watermarked images are filtered: (a) filtered watermarked image, (b) extracted watermark, and (c) correlation coefficient.

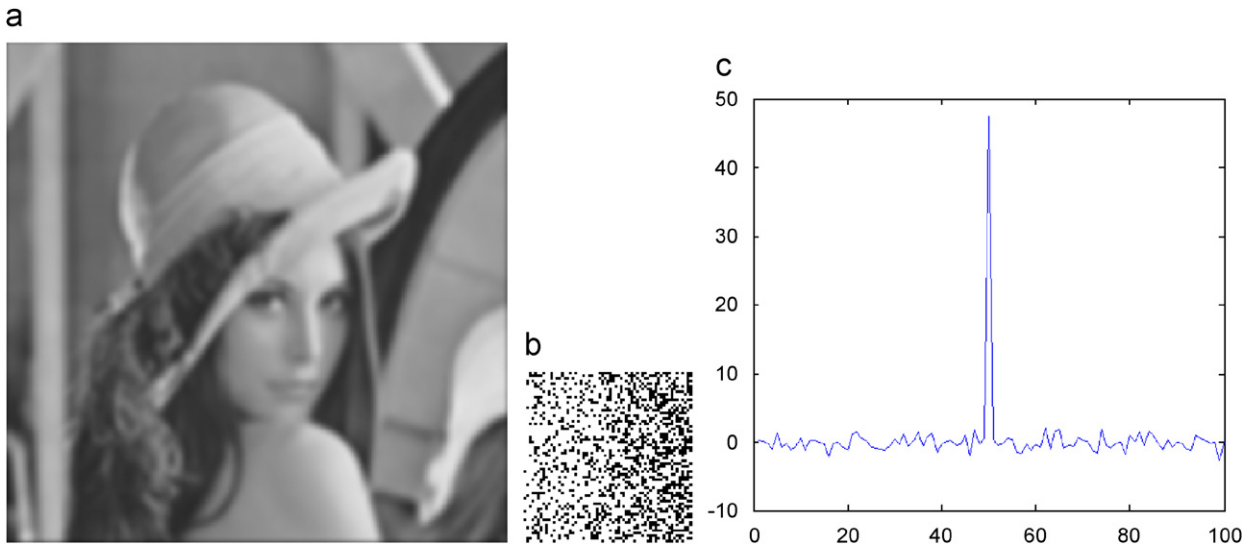


Fig. 14. Low pass filtering for Cox method both original and watermarked images are filtered: (a) filtered watermarked image, (b) extracted watermark, and (c) correlation coefficient.

4.3. Technique 2: the proposed SVD-based watermarking technique

In the previous section, we presented the analysis using the first technique. In this section, we present the second technique. Instead of performing SVD on the original un-watermarked image $A = U\Sigma V$ as one block, this technique partitions the cover object into smaller blocks A_{ij}. Without the loss of generality, we assume these blocks to be square $M \times M$ blocks. Each bit of the watermark modifies one block of the cover object. Embedding proceeds as follows:

1. Partition the original image A into $M \times M$ blocks A_{ij}.
2. Perform SVD on each block as
$$A_{ij} = U_{ij}\Sigma_{ij}V_{ij}^{T}. \quad (36)$$
3. Embed one bit of the watermark in each block as
$$A_{ijW} = U_{ij}[\Sigma_{ij}(1 + \alpha b_{ijW})]V_{ij}^{T}. \quad (37)$$

Here, b_{ijW} is the watermark bit embedded into block A_{ij}. The constant α determines the strength of the embedded signal. Note that bits b_{ijW} will only have values of zero or one. It is clear that this algorithm is similar to the previous one. Thus, all the previous developments still hold here. However, this algorithm is more flexible. The use of different scaling factors α for each bit results in a more robust embedding. In addition, one can embed watermark

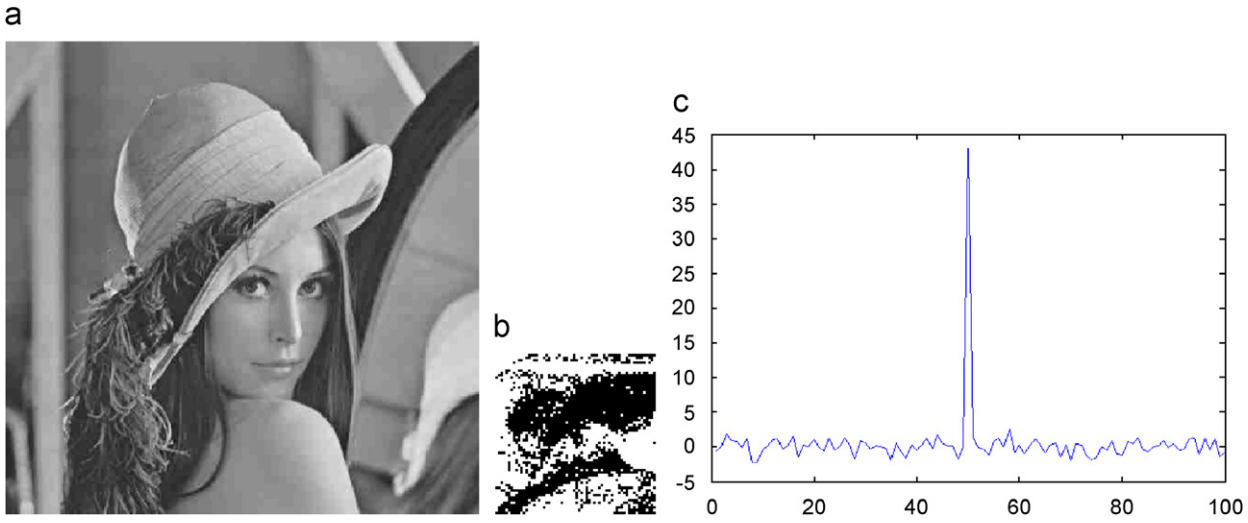


Fig. 15. The 20% lossy jpeg compression for SVD method only watermarked image is compressed: (a) compressed watermarked image, (b) extracted watermark, and (c) correlation coefficient.

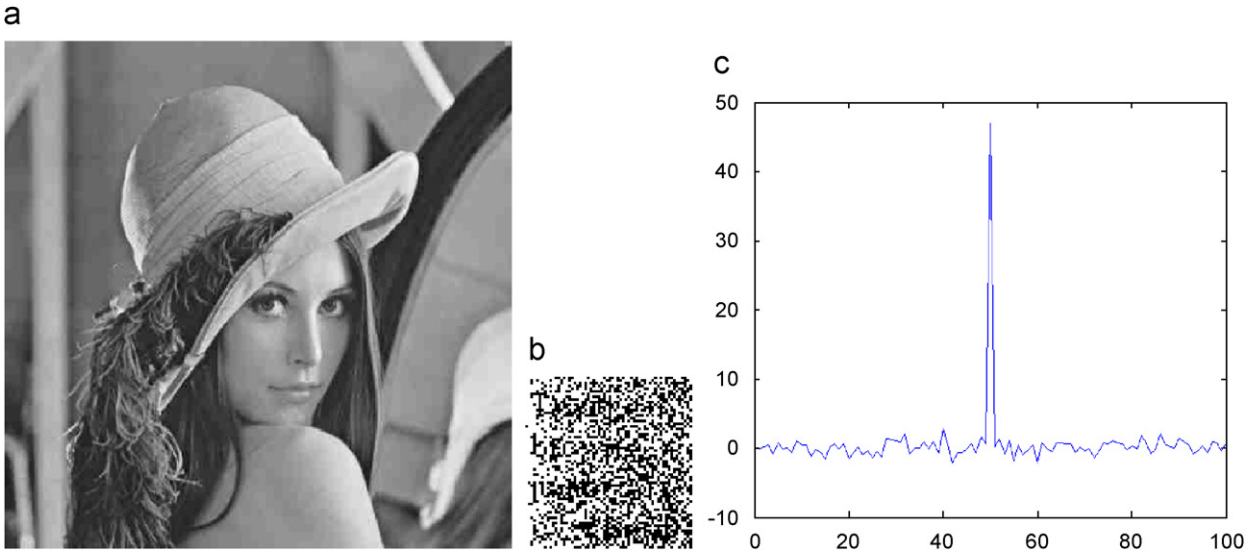


Fig. 16. The 20% lossy jpeg compression for Cox method only watermarked image is compressed: (a) compressed watermarked image, (b) extracted watermark, and (c) correlation coefficient.

bits $b_{ijW}=1$ in blocks A_{ij} that have larger singular values while embedding the zero bits in blocks with smaller singular values. Of course, this will need an extra matrix to register which block A_{ij} is used to embed the watermark bit b_{ijW}. Combining hash and quantization algorithms [5] makes this algorithm more secure. Fig. 3 gives a block diagram for the embedding steps.

The extraction sequence consists of the following four steps:

1. Partition the watermarked image A_W and the original image A into blocks in the same fashion used for embedding the original image.
2. Perform SVD on each block $A_{ij}=U_{ij}\Sigma_{ij}V_{ij}^{T}$.
3. The embedded watermark bit is found from

$$I_M b_{ijW}=\frac{\sum_{ij}^{-1}}{\alpha}[U_{ij}^{T}A_{ijW}V_{ij}^{T}-\Sigma_{ij}], \tag{38}$$

where I_M denotes the $M\times M$ Identity matrix. This leads to

$$b_{ijW}=\frac{\text{Trace}\,(I_M b_{ijW})}{M}. \tag{39}$$

In simulations, a slightly modified form for the third step is used. Instead of solving for b_{ijW} exactly, we used

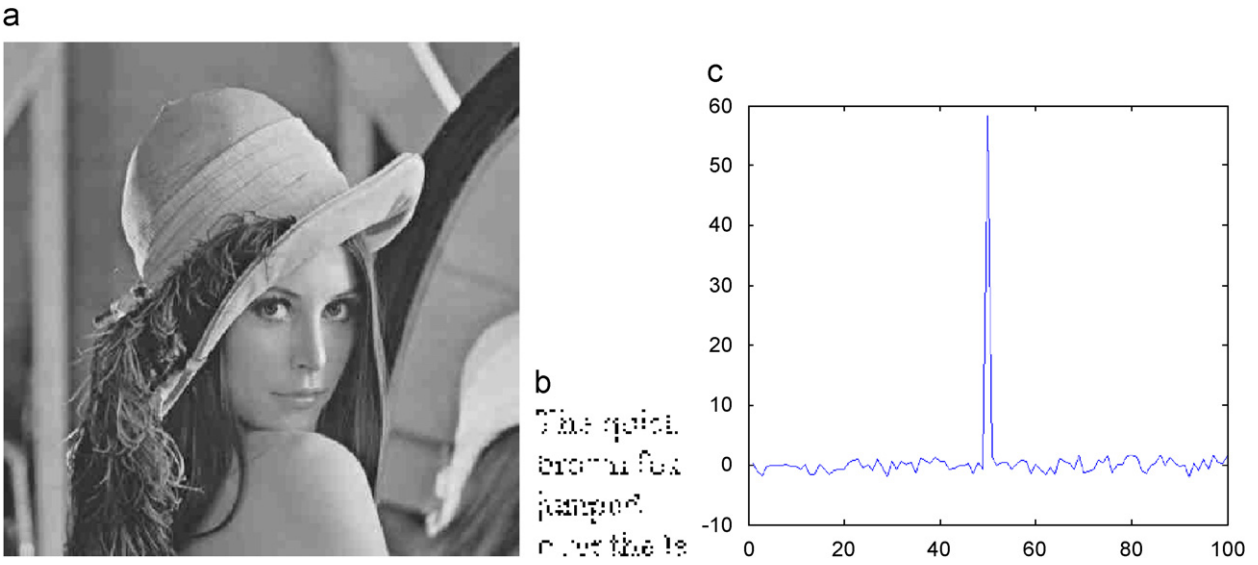


Fig. 17. The 20% lossy jpeg compression for SVD method both original and watermarked images are compressed: (a) compressed watermarked image, (b) extracted watermark, and (c) correlation coefficient.

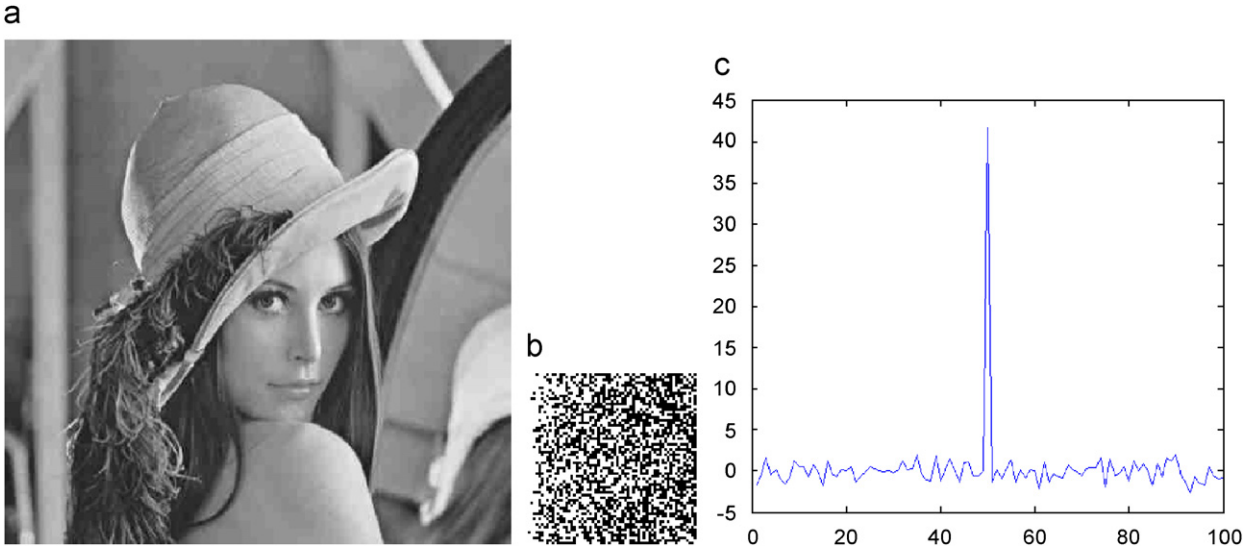


Fig. 18. The 20% lossy jpeg compression for Cox method both original and watermarked images are compressed: (a) compressed watermarked image, (b) extracted watermark, and (c) correlation coefficient.

a measure of b_{ijW} as follows:

$$b^*_{ijW} = \frac{\text{diag}\,(I_M b_{ijW}) \times \text{diag}\,(I_M b_{ijW})^{\mathrm{T}}}{\sqrt{\text{diag}\,(\Sigma_{ij}) \times \text{diag}\,(\Sigma_{ij})^{\mathrm{T}}}}. \quad (40)$$

Here, *diag*(*matrix*) is a row vector containing the diagonal elements of that matrix. One should notice that Eq. (40) uses a type of a normalized norm that is similar to the correlation coefficient used to detect a certain pattern. Experimental results have shown that the use of Eq. (40) is more robust than the use of Eq. (39). Thus, we will be using (40).

4. Let the average of all the bits b^*_{ijW} obtained from (40) be $\bar{b}^*_{ijW}$. Now, a threshold parameter α_{T} is used to round the bits b^*_{ijW} to zero or one using the relation:

$$b^*_{ijW} = \begin{cases} 0 & \text{if } b^*_{ijW} \geqslant \alpha_{\mathrm{T}} \bar{b}^*_{ijW}, \\ 1 & \text{if } b^*_{ijW} < \alpha_{\mathrm{T}} \bar{b}^*_{ijW}. \end{cases}$$

One should also notice that this method embeds the bits in one's complement form just as done by Cox [9]. In our algorithm, we assume that the watermark is a normalized gray scale image. Thus, it will only take values of zero or one. Fig. 4 gives a block diagram for the extraction steps.

5. Experimental results

In this section, we investigate the robustness of the proposed SVD algorithm against different attacks. Extensive

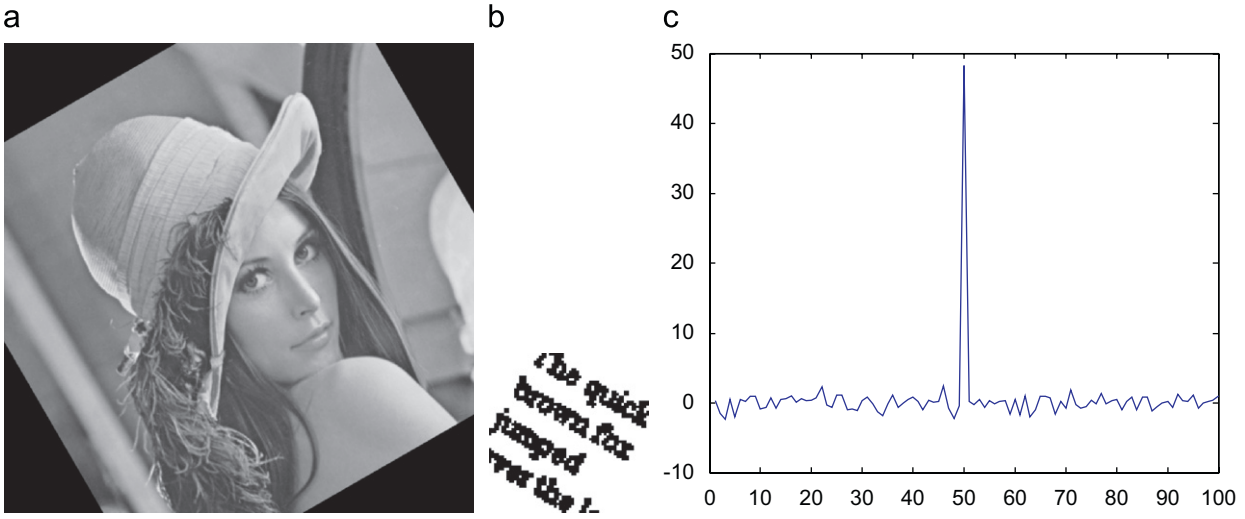


Fig. 19. Rotation test for SVD (first method) both original and watermarked images are rotated by 30°: (a) rotated watermarked image, (b) extracted watermark, and (c) correlation coefficient.

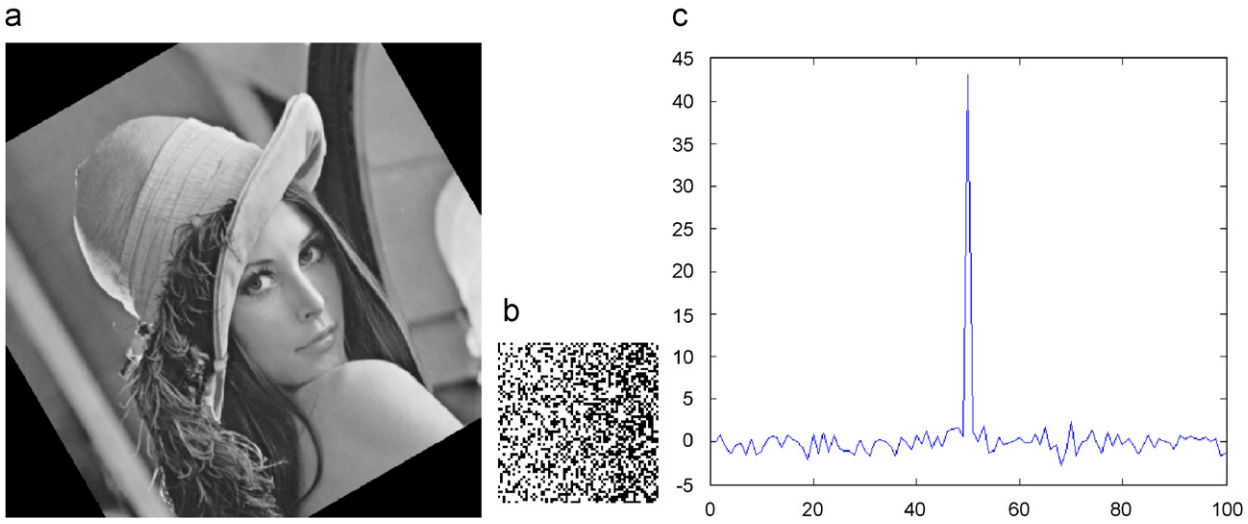


Fig. 20. Rotation test for Cox (first method) both the original and watermarked images are rotated by 30° for Cox: (a) rotated watermarked image, (b) extracted watermark, and (c) correlation coefficient.

simulations compare the results obtained via the proposed SVD algorithm with the results obtained via different types of algorithms. Section 5.1 gives a detailed comparison with the DCT-based algorithm proposed by Cox [9]. Section 5.2 presents a comparison with the blind hybrid DWT–SVD algorithm proposed by Bao and Ma [55].

5.1. Comparison with the Cox DCT-based algorithm

The cover image used for testing is a 512-by-512 gray scale Lena image. Rather than using a pseudo-Gaussian random numbers watermark, we used a 64-by-64 text message shown in Fig. 5. The use of text messages makes it easy to test robustness. Testing robustness boils down to reading the extracted message and comparing it with the original watermark. In addition, the use of a visually sound watermark makes a stronger case in a court. We used the one-dimensional correlation coefficient to measure the similarity between the embedded and extracted watermarks. The proposed algorithm embeds one watermark bit in an 8-by-8 block of the cover Lena image. In the Cox method, bits are embedded in the first highest 4096 DCT coefficients of the Lena image. As was suggested by Cox, the scaling factor α that controls the energy of the embedded watermark was set to 0.1. In order to ensure

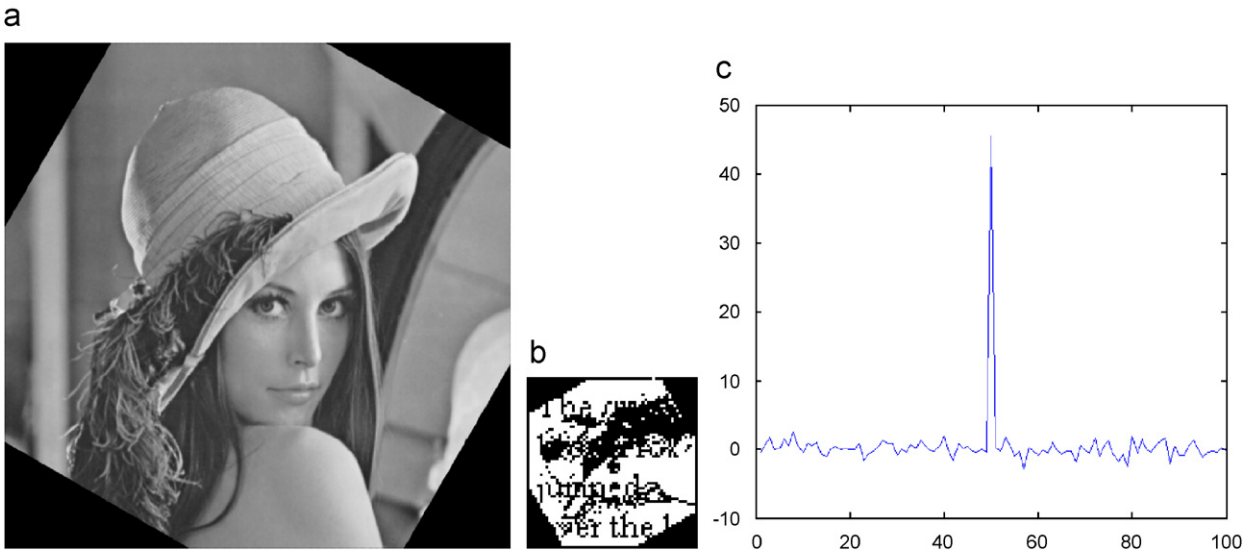


Fig. 21. Rotation test for the SVD (second method) only watermarked image is rotated by 30° and then by −30°: (a) rotated watermarked image, (b) extracted watermark, and (c) correlation coefficient.

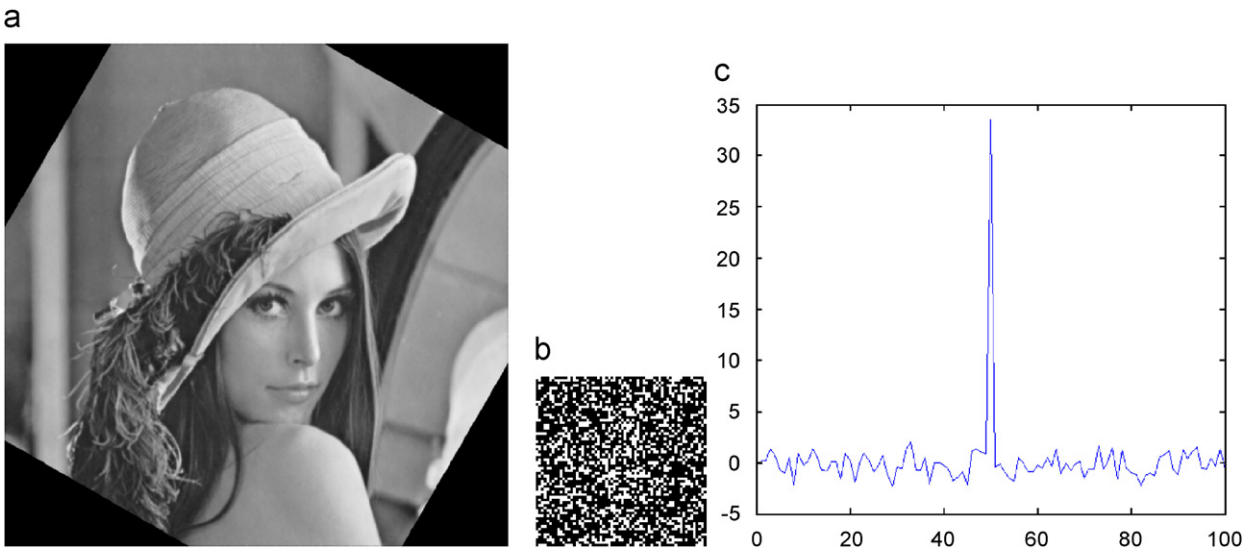


Fig. 22. Rotation test for Cox (second method) watermarked image is rotated by 30 and then by −30°: (a) rotated watermarked image, (b) extracted watermark, and (c) correlation coefficient.

comparable transparency between our algorithm and that of Cox, the scaling factor α for our SVD algorithm was set to 0.02. In the correlation coefficient plots, a set of 100 64-by-64 watermarks was used. The 50th one is the correct watermark while the rest are randomly generated Gaussian numbers. The correlation coefficient between each of these 100 watermarks and the extracted watermark is calculated and plotted. We scaled down the plots in order to save space. This will have the drawback of not showing the actual effects of different attacks on the watermarked image. However, these effects become clearer by enlarging the images to their original sizes. Simulations show that the use of the correlation coefficient as an indicator for the existence or absence of a watermark may be deceiving. This becomes clear by noticing that the correlation coefficient between a gray scale image and an all white gray scale image of the same size can be as large as the correlation coefficient between the gray image and the image itself.

Fig. 6 shows the original image (a), the watermarked image via proposed SVD algorithm (b), and the watermarked image via the Cox method (c). Note that one cannot notice any difference between the three images.

Fig. 7 shows the absolute error image using the SVD method (a) and using the Cox method (b). One should notice that the details of the absolute error image would not appear without spreading its intensity. Fig. 8 shows the extracted watermark for the proposed SVD algorithm (a) and using the Cox method (b). Notice that both extracted watermarks are very clear. This is because there are no attacks on the watermarked images.

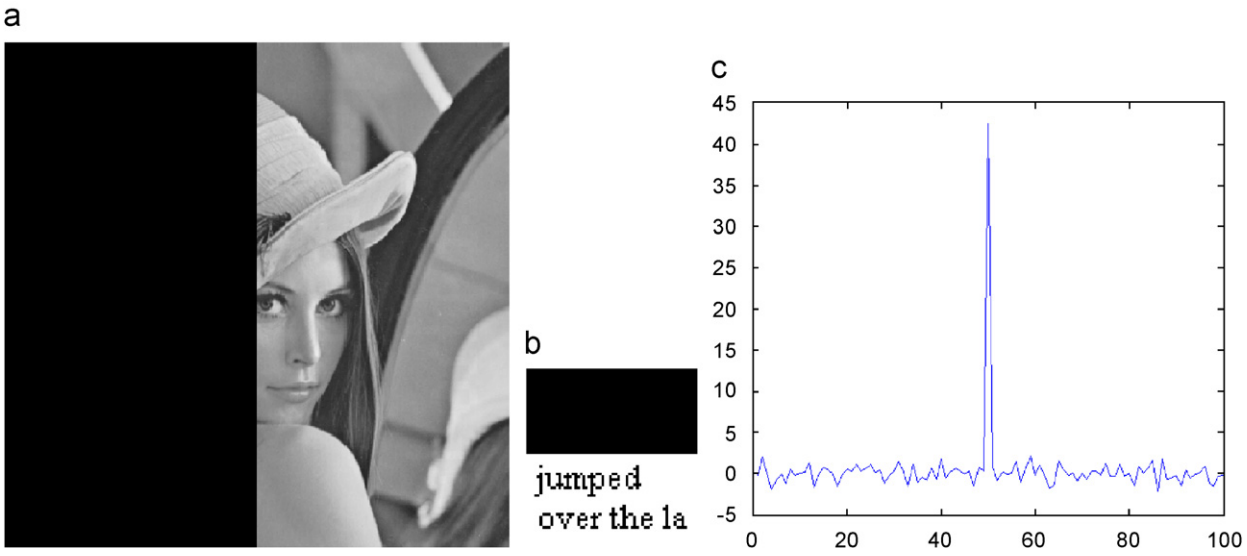


Fig. 23. Cropping for SVD method: (a) rotated watermarked image, (b) extracted watermark, and (c) correlation coefficient.

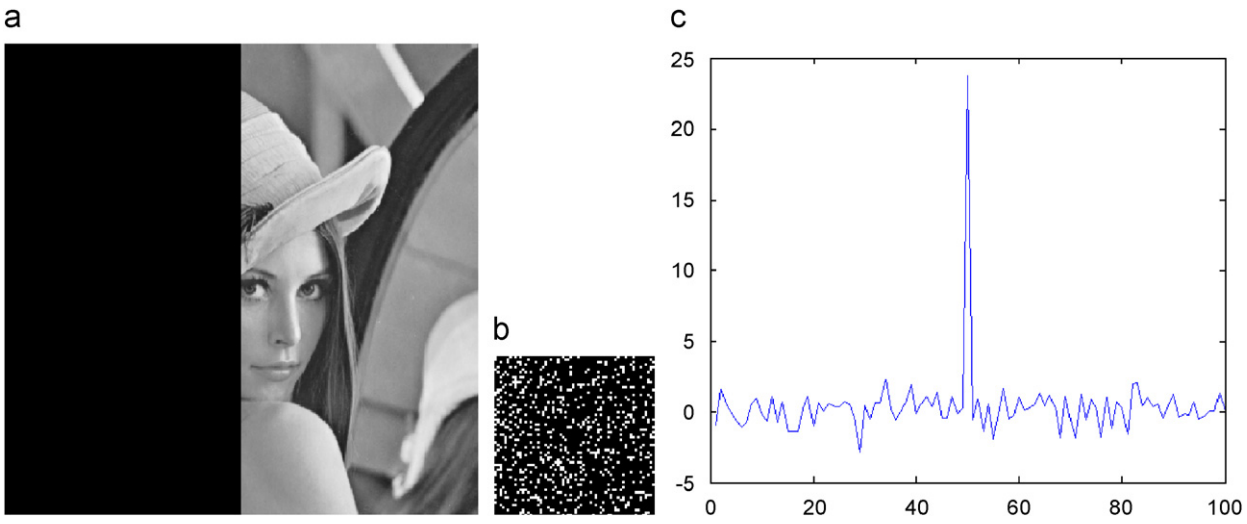


Fig. 24. Cropping for Cox method: (a) rotated watermarked image, (b) extracted watermark, and (c) correlation coefficient.

Figs. 9 and 10 compare the results of adding Gaussian noise attack. A Gaussian noise of zero mean and 15 dBW power (variance is ≈ 31) was added to the watermarked images. Each of Figs. 9 and 10 shows the attacked watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. Comparison between the extracted watermarks in Figs. 9 and 10 indicates that the performance of both techniques is acceptable. This is clear from the readability of the extracted watermarks and the high values of the correlation coefficients. It is clear that results obtained by the proposed SVD method are better than that obtained via the Cox method.

Figs. 11 and 12 compare the results of low pass filtering attack. The Gaussian low pass filter used was of size 16-by-16 and variance of 1. Each of Figs. 11 and 12 shows the results of low pass filtering as applied to the watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the proposed SVD and the Cox methods, respectively. Notice that, although the correlation coefficient is relatively high, the extracted watermark for the Cox method has no meaning. As mentioned earlier, the correlation coefficient may be deceiving. For this attack, it is clear that the proposed SVD method is more robust than the Cox method. One can see this by comparing the extracted images in Figs. 11 and 12.

Simulations have shown that if the original cover and watermarked images pass through the same filter, the extracted image will be almost perfect in the SVD case. This turned out to be true for all types of attacks except for

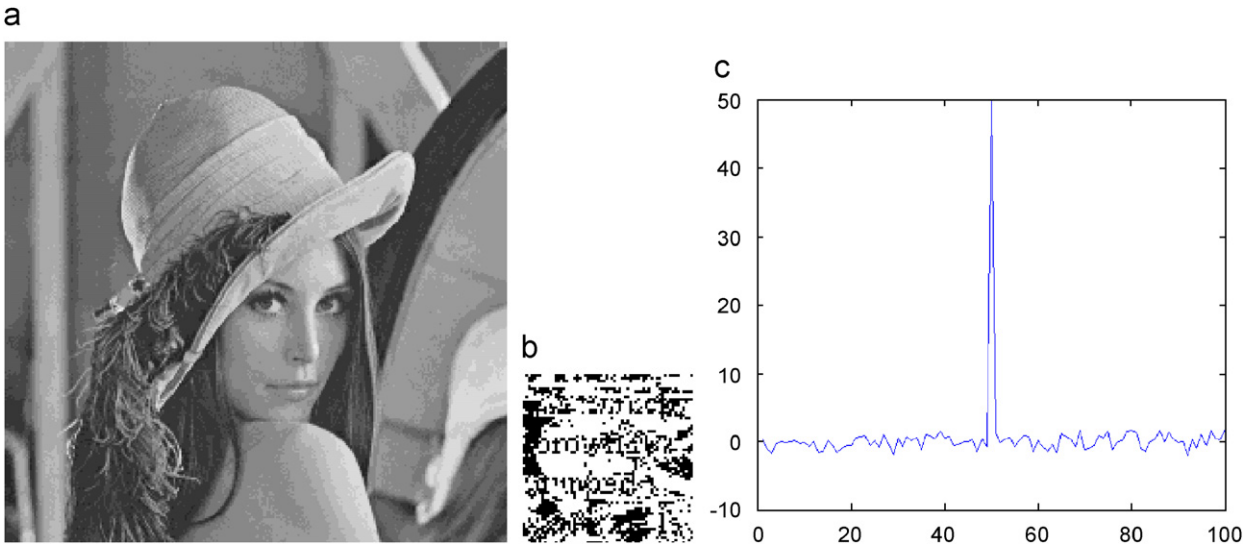


Fig. 25. Dithering the watermarked image for SVD method: (a) dithered watermarked image, (b) extracted watermark, and (c) correlation coefficient.

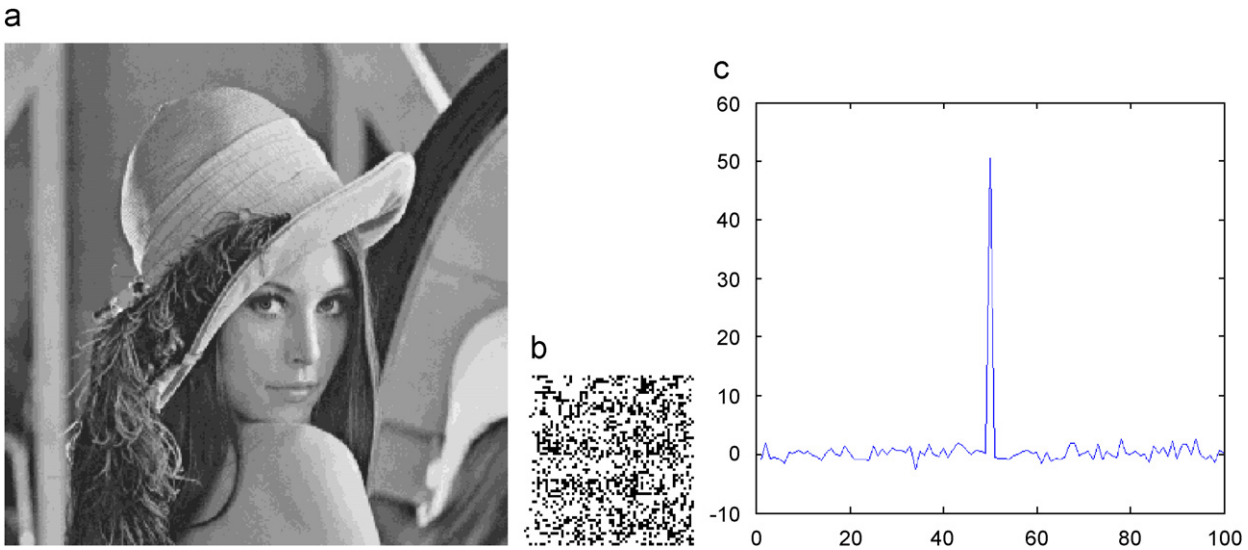


Fig. 26. Dithering watermarked image only for Cox method: (a) dithered watermarked image, (b) extracted watermarked, and (c) correlation coefficient.

the Gaussian noise attack. On the other hand, the application of the attack to both the cover image and the watermarked image does not improve the quality of the extracted image in the Cox case.

Figs. 13 and 14 show results of passing the original cover image and the watermarked image through the previous Gaussian low pass filter. Each of Figs. 13 and 14 shows the filtered image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. It is clear that the quality of the extracted watermark using SVD is much better than that obtained via the Cox technique. The extracted watermark via SVD is as clear as the original watermark. On the other hand, the extracted watermark via the Cox technique has no meaning.

Figs. 15 and 16 compare the results for 20% jpeg compression attack. Each of Figs. 15 and 16 gives the results for jpeg compression as applied to the watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. Although both methods give a relatively high correlation coefficient, the extracted watermark in both cases is very poor.

Figs. 17 and 18 show results of applying 20% jpeg compression to the original cover and watermarked images. Each of Figs. 17 and 18 shows the

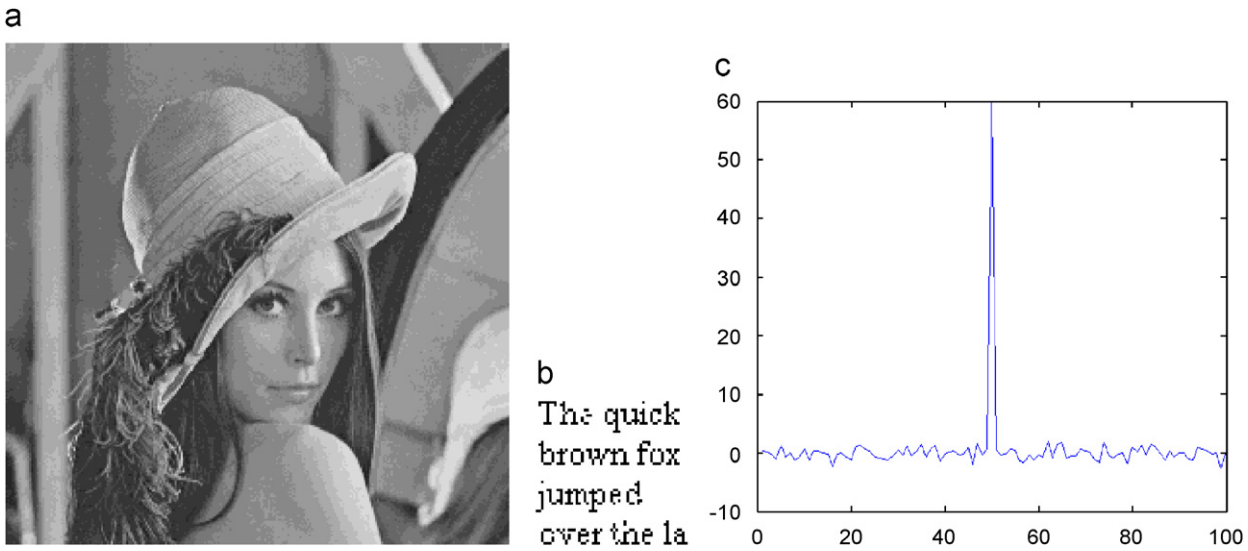


Fig. 27. Dithering both watermarked and original for SVD method: (a) rotated watermarked image, (b) extracted watermark, and (c) correlation coefficient.

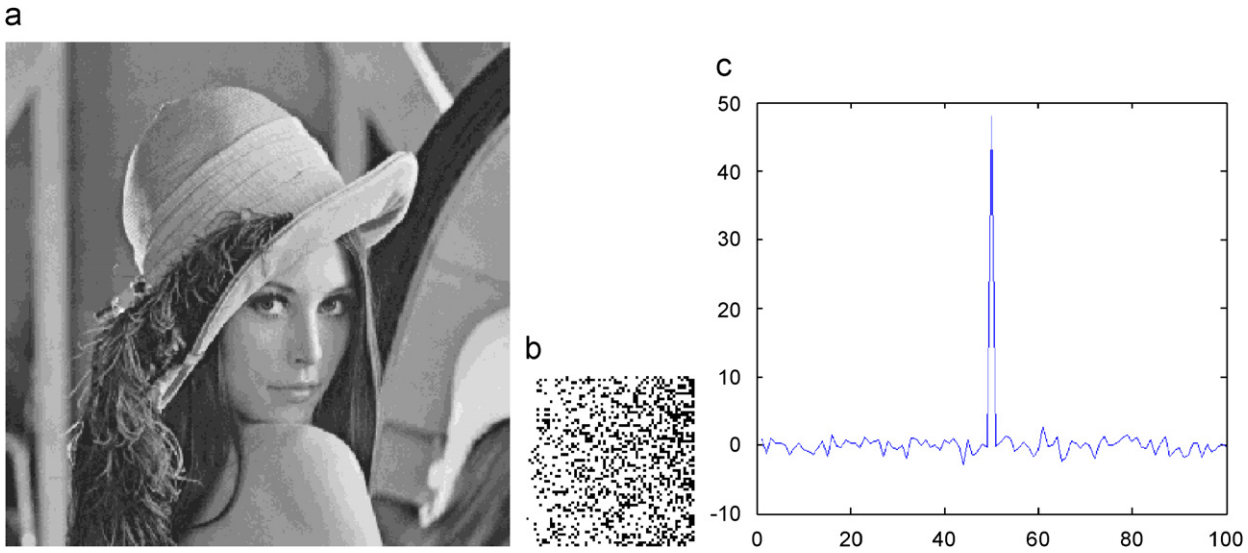


Fig. 28. Dithering both watermarked and original for Cox method: (a) dithered watermarked image, (b) extracted watermark, and (c) correlation coefficient.

jpeg-compressed watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. Notice the vast improvement in the extracted watermark image in the SVD case.

We applied the rotation attack in two different ways. In the first one, both the original and the watermarked images are rotated by 30°. In the second, only the watermarked image is rotated by 30° then by −30°. Figs. 19 and 20 show results for the first method. Each of Figs. 19 and 20 shows the rotated watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. By comparing the extracted images, it is clear that the SVD method is much more robust against rotation attacks.

Figs. 21 and 22 show results for rotation using the second method. Each of Figs. 21 and 22 shows the rotated watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. By comparing the two extracted messages, it is easy to see that the SVD method is superior to the Cox method. The Cox method is extremely fragile against image rotation. Actually, it does not withstand rotations as small as one degree. On the other hand, the proposed SVD technique is highly robust against rotations.

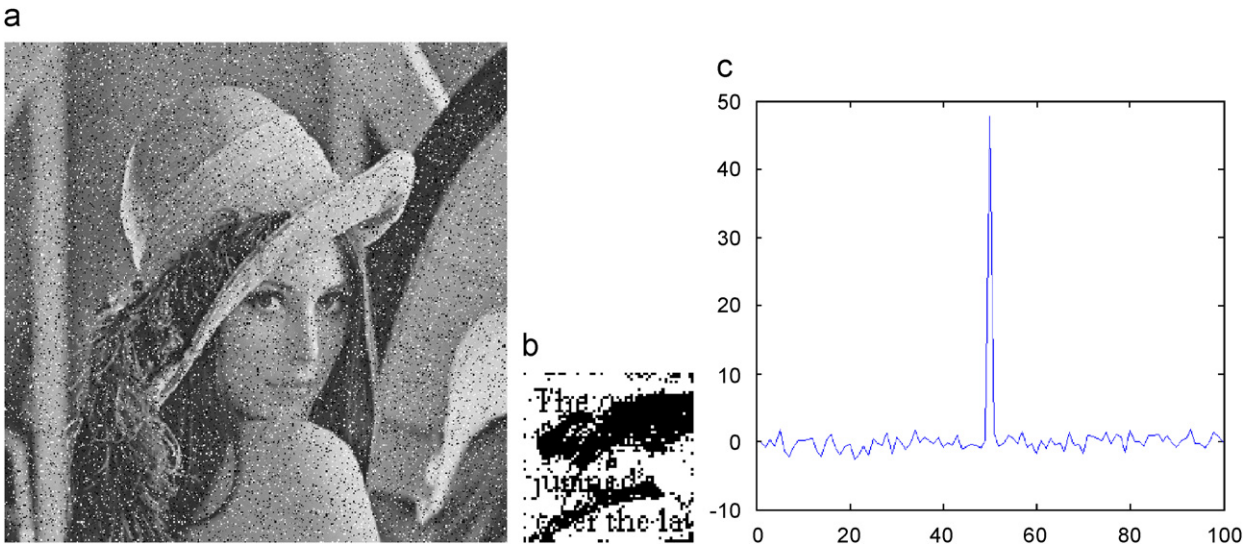


Fig. 29. Salt and pepper attack for the SVD method only watermarked image is corrupted with salt and pepper noise (.1 of 1) and passed through a median filter: (a) noisy watermarked image, (b) extracted watermark, and (c) correlation coefficient.

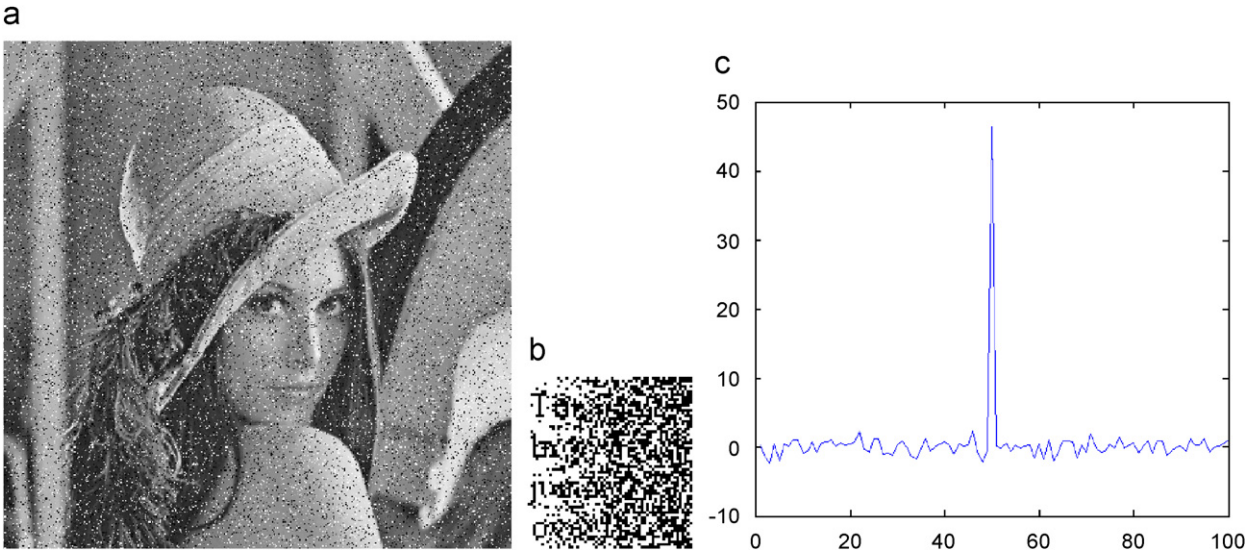


Fig. 30. Salt and pepper attack for the Cox method only watermarked image corrupted with salt and pepper noise (.1 of 1) and passed through a median filter: (a) noisy watermarked image, (b) extracted watermark, and (c) correlation coefficient.

Figs. 23 and 24 compare the results of cropping attack on the watermarked image. Each of Figs. 23 and 24 shows the cropped watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. Comparison between the extracted watermarks in Figs. 23 and 24 reveals the superiority of the SVD method.

We used the Matlab command 'dither (image, 4, 5)' to carry out the dithering attack. This resulted in a heavily dithered image. Figs. 25 and 26 compare the results of dithering attack on the watermarked image. Each of Figs. 25 and 26 shows the dithered watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. Again, comparison between the extracted watermarks in Figs. 25 and 26 reveals that the SVD technique is more robust against dithering attacks.

Figs. 27 and 28 compare the results of dithering attack on both the original and watermarked images. Each of Figs. 27 and 28 shows the dithered watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. Comparison between the extracted watermarks in Figs. 27 and 28 reveals that the SVD method is more resilient to dithering attacks.

Figs. 29 and 30 compare the results of salt and pepper attack. In this case, we added salt and pepper noise (.1 out of a scale of 1) to the watermarked image. Then, we used a

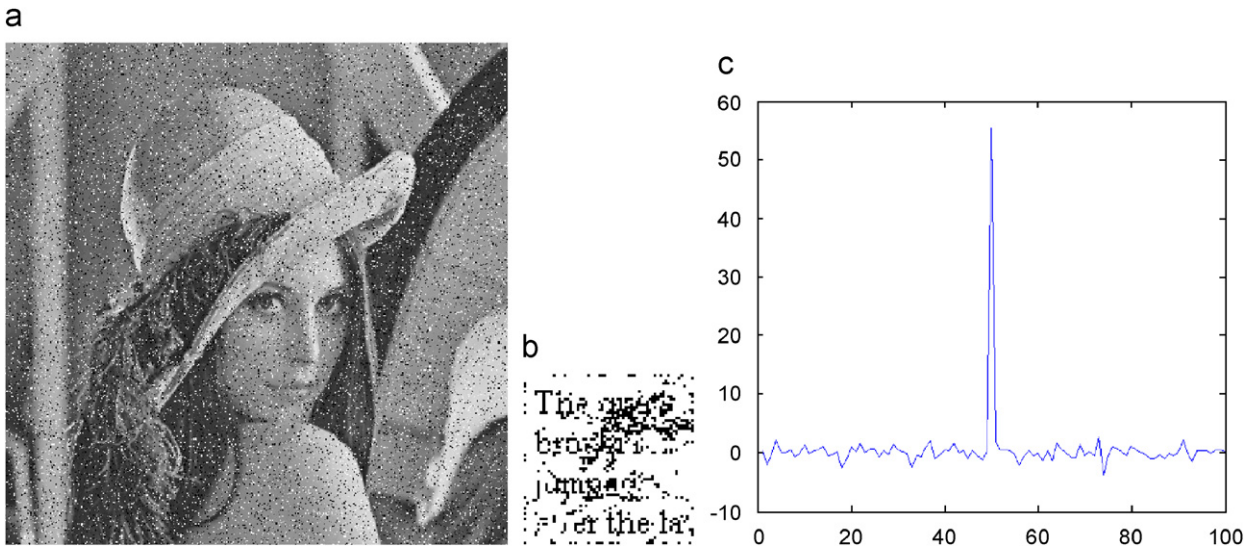


Fig. 31. Salt and pepper attack for the SVD method both the original and watermarked images are corrupted with salt and pepper noise (.1 of a scale of 1) and passed through a median filter: (a) noisy watermarked image, (b) extracted watermark, and (c) correlation coefficient.

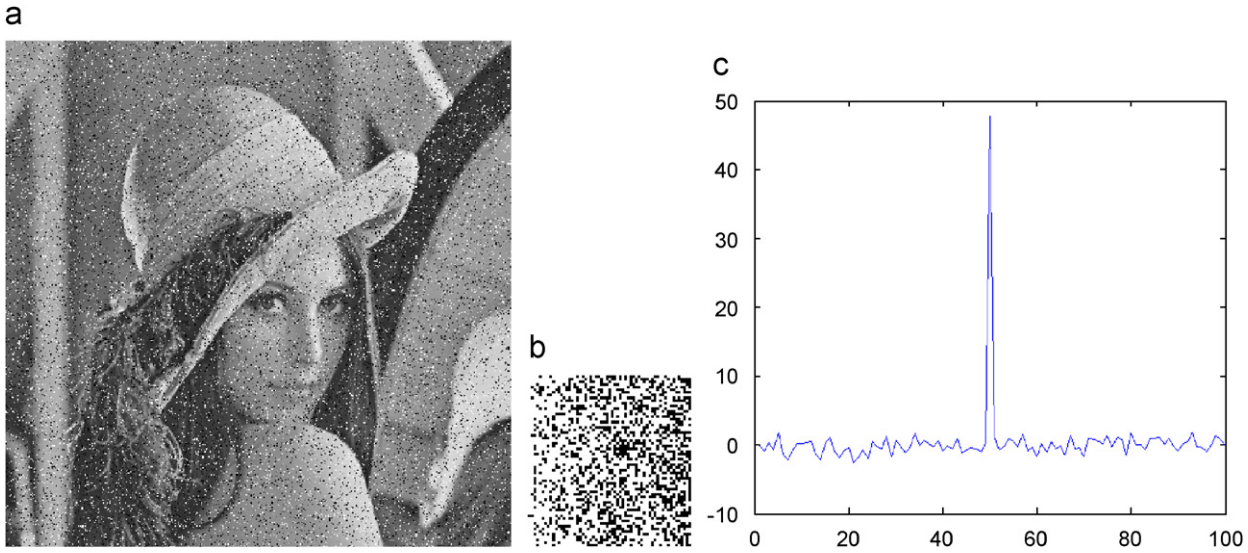


Fig. 32. Salt and pepper attack for the Cox method both the original and watermarked images are corrupted with salt and pepper noise (.1 of a scale of 1) and passed through a median filter: (a) noisy watermarked image, (b) extracted watermark, and (c) correlation coefficient.

median filter to smooth out the noise. Each of Figs. 29 and 30 shows the noisy watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. Comparison between the extracted images in Figs. 29 and 30 reveals that the SVD is more robust against salt and pepper attack.

Figs. 31 and 32 compare the results of salt and pepper attack as applied to both the cover and the watermarked images. In this case, we added salt and pepper noise of (.1 out of a scale of 1) to both the original and the watermarked images. The original and the watermarked images were then passed through a median filter to smooth out the noise. Each of Figs. 31 and 32 shows the noisy watermarked image (a), the extracted watermark (b), and the correlation coefficient (c) for the SVD and the Cox methods, respectively. Again, comparison between the extracted watermarks in Figs. 31 and 32 reveals that the SVD method proved is more robust against dithering attack.

Figs. 33 and 34 compare the results of resizing the watermarked image down to 25%. Each of Figs. 33 and 34 shows the extracted watermark (a) and the correlation coefficient (b) for the SVD and the Cox methods, respectively. Comparison between the extracted images in Figs. 33 and 34 shows that the SVD is more robust to resize attack.

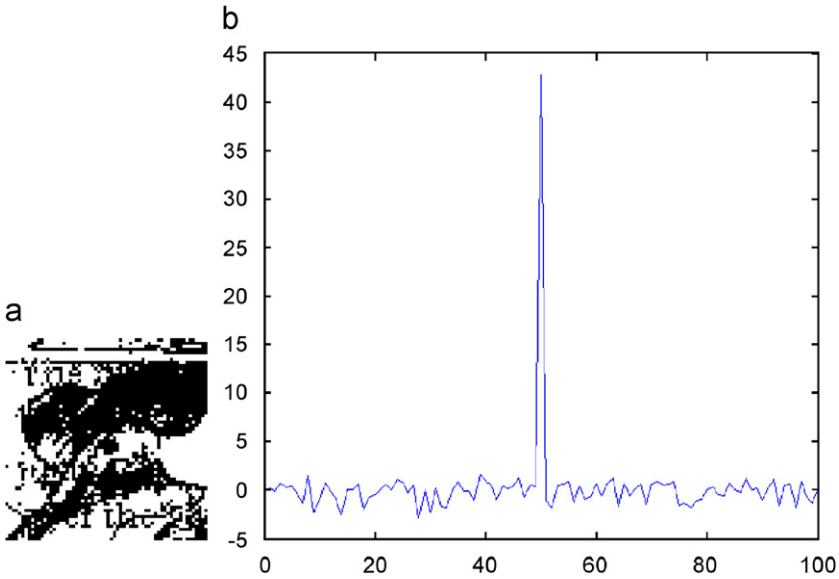


Fig. 33. Resize attack for SVD method only watermarked image is resized to 25%: (a) extracted watermark and (b) correlation coefficient.

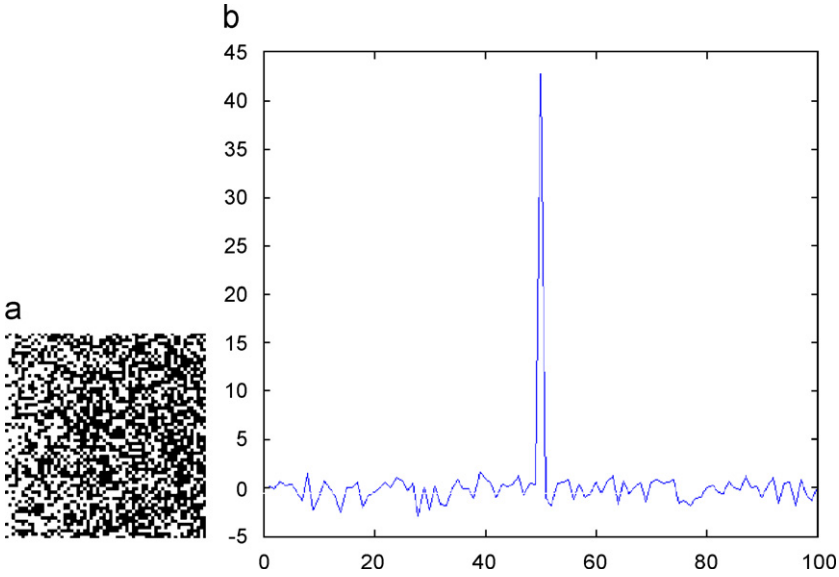


Fig. 34. Resize attack for Cox method only watermarked image is resized to 25%: (a) extracted watermark and (b) correlation coefficient.

Figs. 35 and 36 compare the results for resizing original and the watermarked images down to 25%. Each of Figs. 35 and 36 shows the extracted watermark (a) and the correlation coefficient (b) for the SVD and the Cox methods, respectively. It is clear that the SVD method is superior to the Cox method. It is also clear that the Cox method is not robust against resizing.

In summary, it is clear that the SVD method is superior to the Cox method in almost all attacks. This is especially true when attacking both the original and the watermarked images. The authors would like to emphasize that the main measure for robustness is the readability of the extracted message. In addition to the extracted message, we used the correlation coefficient and the PSNR as extra measures for similarity between the original and the extracted watermarks. In order to compare between the two measures, we utilized Eqs. (19) and (20) to calculate the two measures for all types of attacks. For each type of attack, Table 2 gives the PSNR, the correlation coefficient, and the extracted watermark for the proposed SVD-based

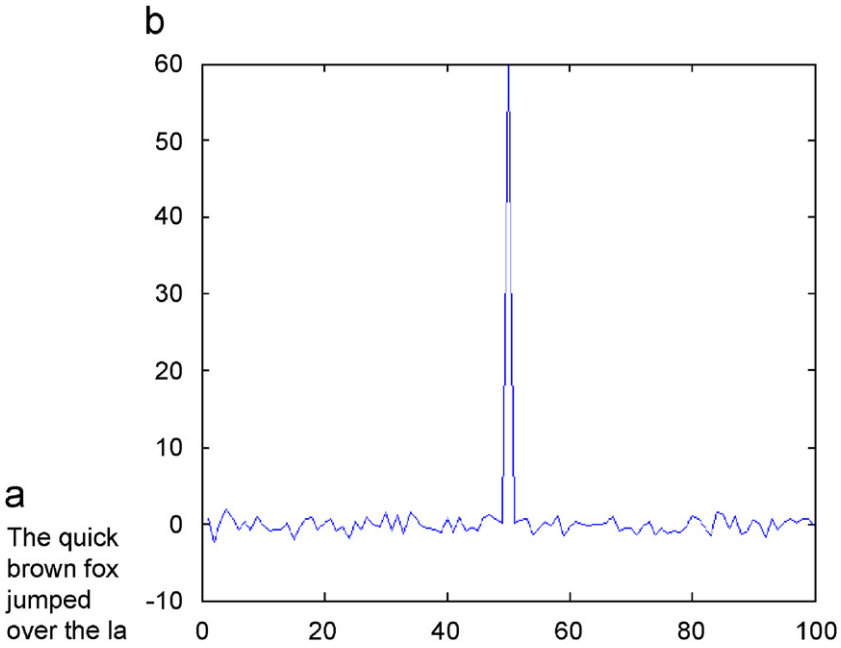


Fig. 35. Resize attack for SVD method original and watermarked images are resized to 25%: (a) extracted watermark, (b) correlation coefficient.

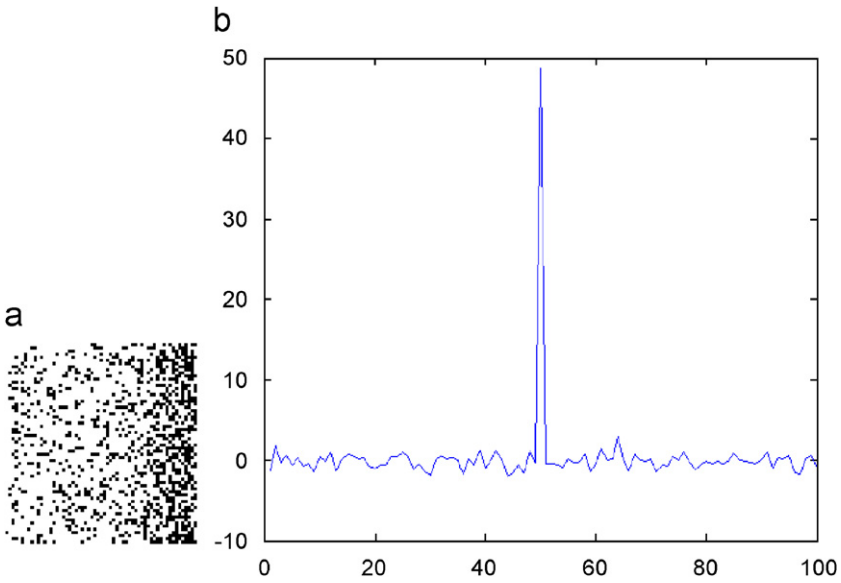


Fig. 36. Resize attack for Cox method original and watermarked images are resized to 25%: (a) extracted watermark and (b) correlation coefficient.

method and the Cox method. Results in Table 2 show that, a higher value of correlation coefficient corresponds to a higher value of PSNR. Thus, one can use either one.

5.2. Comparison with Bao and Ma's blind hybrid DWT–SVD algorithm

This section compares our algorithm with Bao and Ma's algorithm [55]. This algorithm is a blind hybrid DWT–SVD-based algorithm with the same capacity as our algorithm. As opposed to Liu and Tan's algorithm, this algorithm does not suffer the false-positive detection problem. Table 3 compares the performances of our algorithm with that of Bao and Ma. For each type of attack, Table 3 gives the PSNR, the correlation coefficient, and the extracted watermark for the proposed SVD-based method and that of Bao and Ma. As can be seen from the extracted messages, our algorithm proved to be much more robust than that of Bao and Ma. Actually, apart from the cropping attack, their algorithm could not resist any attack.

Table 2

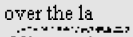
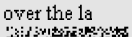
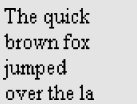
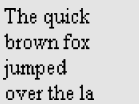
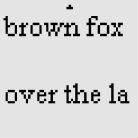
Attack type	PSNR for SVD	Correlation coefficient for SVD	Extracted image for SVD	PSNR for cox	Correlation coefficient for cox	Extracted image for cox
No attack	∞	59.97		∞	59.97	
JPEG compression	12.54	58.16		4.70	46.98	
Salt & pepper	9.00	55.55		4.53	46.48	
White noise	7.37	53.39		7.95	54.25	
Dithering	5.59	49.75		5.92	50.56	
Rotation (30 deg, both images rotated)	4.29	45.58		3.59	43.09	
Resize only watermarked image is resized	3.63	42.79		3.24	40.93	
Cropping	3.59	42.55		1.27	23.78	
Low pass filter (only watermarked image is filtered)	2.40	35.37		4.68	47.47	

Table 3

Attack type	PSNR for SVD	Correlation coefficient for SVD	Extracted image for SVD	PSNR for P. Bao & X. Ma	Correlation coefficient for P. Bao & X. Ma	Extracted image for P. Bao & X. Ma
No attack	∞	59.97		∞	59.97	
JPEG compression 50%	6.38	51.56		4.38	46.18	
Salt & pepper	8.76	55.28		3.50	42.33	
White noise	7.61	53.76		2.84	38.81	
Dithering	5.59	49.75		2.87	39.03	
Rotation (30 deg, both images rotated)	5.44	49.72		2.9	39.06	
Resize only watermarked image is resized	3.65	42.79		6.69	52.64	
Cropping	3.59	42.55		12.32	58.06	
Low pass filter (only watermarked image is filtered)	2.42	35.37		4.13	45.26	

6. Conclusion

This paper presented a new SVD-based watermarking algorithm for ownership protection. It was shown that the algorithm is non-invertible. Simulations show that the proposed algorithm is robust against most common attacks. In particular, the algorithm proved to be extremely robust against geometrical distortion attacks. Comparison with different algorithms reveals that the proposed algorithm is more robust. Moreover, the proposed algorithm solves the false-positive detection flaw in most SVD-based techniques such as Liu and Tan's algorithm.

References

[1] G. Langelaar, I. Setyawan, R. Lagendijk, Watermarking digital image and video data: a state-of-art overview, IEEE Signal Process. Mag. 17 (September 2000) 20–46.
[2] R. Liu, T. Tan, A SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 4 (1) (March 2002) 121–128.
[3] P. Moulin, M. Mihcak, A framework for evaluating the data-hiding capacity of image sources, IEEE Trans. Image Process. 11 (9) (September 2002) 1029–1042.
[4] M. Kutter, F. Petitcolas, A fair benchmark for image watermarking systems, in: Proceedings of the SPIE Conference on Security and Watermarking of Multimedia Contents, vol. 3657, USA, January 1999, pp. 226–239.
[5] C. Chang, P. Tsai, C. Lin, SVD-based digital image watermarking scheme, Pattern Recognition Lett. 26 (2005) 1577–1586.

[6] M. Swanson, M. Kobayashi, A. Tewfic, Multimedia data-embedding and watermarking technologies, Proc. IEEE 86 (6) (June 1998) 1064–1086.
[7] S. Craver, N. Memorn, B. Yeo, M. Yeung, Can invisible watermarks resolve rightful ownerships, IBM Research Report, RC 20509, July 1996, pp. 1–21.
[8] Y. Wu, On the security of SVD based ownership watermarking, IEEE Trans. Multimedia 7 (4) (August 2005) 624–627.
[9] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process. 6 (12) (1997) 1673–1687.
[10] L. Qiao, K. Nahrstedt, Watermarking schemes and protocols for protecting rightful ownership and customer's rights, J. Visual Commun. Image Represent 9 (3) (September 1998) 194–210.
[11] K. Nahrstedt, L. Qiao, Non-invertible watermarking methods for MPEG video and audio, in: Proceedings of the Security Workshop at ACM Multimedia, England, September 1998, pp. 93–98.
[12] Q. Li, E. Chang, On the possibility of non-invertible watermarking schemes, in: Proceedings of the Sixth International Workshop on Information Hiding, Canada, May 2004, pp. 13–24.
[13] A. Adelsbach, S. Katzenbeisser, H. Veith, Watermarking schemes provably secure against copy and ambiguity attacks, in: Proceedings of the 3rd ACM Workshop on Digital Rights Management, Washington, DC, USA, October 2003, pp. 117–133.
[14] F. Bao, Multimedia content protection by cryptography and watermarking in temper-resistant hardware, in: Proceedings of the ACM Workshop on Multimedia, USA, 2000, pp. 139–142.
[15] L. Coetzee, J. Eksteen, Copyright protection for cultureware preservation in digital repositories, in: Proceedings of the 10th Annual Internet Society Conference (INET2000), Japan, July 2000.
[16] K. Ratakonda, R. Dugad, N. Ahuja, Digital image watermarking: issues in resolving rightful ownership, in: Proceedings of the IEEE International Conference on Image Processing, USA, October 1998, pp. 414–418.
[17] S. Craver, N. Memorn, B. Yeo, M. Yeung, Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications, IEEE J. Sel. Areas Commun. 16 (4) (May 1998) 573–586.
[18] F. Hartung, M. Kutter, Multimedia watermarking techniques, Proc. IEEE 87 (7) (July 1999) 1079–1107.
[19] S. Craver, N. Memorn, B. Yeo, M. Yeung, On the invertibility of invisible watermarking techniques, in: Proceedings of the IEEE International Conference on Image Processing, October 1997, pp. 540–543.
[20] F. Cayre, C. Fontaine, T. Furon, Watermarking security: theory and practice, IEEE Trans. Multimedia 53 (10) (October 2005) 3976–3987.
[21] M. Ramkumar, A. Akansu, A robust protocol for proving ownership of multimedia content, IEEE Trans. Multimedia 6 (3) (June 2004) 469–478.
[22] M. Ramkumar, A. Akansu, Robust protocols for proving ownership of Images, in: Proceedings of the IEEE International Conference on Information Technology: Coding and Computing, USA, March 2000, pp. 22–27.
[23] A. Reddy, B. Chatterji, A new wavelet based logo-watermarking scheme, Pattern Recognition Lett. 26 (May 2005) 1019–1027.
[24] J. Hernandez, M. Amado, F. Perez-Gonzalez, DCT-domain watermarking techniques for still images: detector performance analysis and a new structure, IEEE Trans. Image Process. 9 (1) (January 2000) 55–67.
[25] C. Hsu, J. Wu, Hidden digital watermarks in images, IEEE Trans. Image Process. 8 (1) (January 1999) 58–68.
[26] C. Shieh, H. Huang, F. Wang, J. Pan, Genetic watermarking based on transform-domain techniques, Pattern Recognition 37 (March 2004) 555–565.
[27] F. Huang, Z. Guan, A hybrid SVD-DCT watermarking method based on LPSNR, Pattern Recognition Lett. 25 (15) (November 2004) 1769–1775.
[28] A. Sverdlov, S. Dexter, A. Eskicioglu, Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies, in: Proceedings of the 13th European Signal Processing Conference (EUSIPCO '05), Turkey, September 2005.
[29] W. Chu, DCT-based image watermarking using subsampling, IEEE Trans. Multimedia 5 (1) (March 2003) 34–38.
[30] P. Kumsawat, K. Attakitmongcol, A. Srikaew, Multiwavelet-based image watermarking using genetic algorithm, in: Proceedings of the IEEE TENCON Conference, November 2004, pp. 275–278.
[31] C. Wang, J. Doherty, R. Van Dyke, A wavelet-based watermarking algorithm for ownership verification of digital images, IEEE Trans. Image Process. 11 (2) (February 2002) 77–78.
[32] S. Wang, Y. Lin, Wavelet tree quantization for copyright protection watermarking, IEEE Trans. Image Process. 13 (2) (February 2004) 154–164.
[33] E. Ganic, A. Eskicioglu, Robust DWT-SVD domain image watermarking: embedding data in all frequencies, in: Proceedings of the ACM Workshop on Multimedia and Security, Germany, 2004, pp. 166–174.
[34] A. Reddy, B. Chatterji, A new wavelet based logo-watermarking scheme, Pattern Recognition Lett. 26 (May 2005) 1019–1027.
[35] P. Tao, A. Eskicioglu, A robust multiple watermarking scheme in the discrete wavelet transform domain, Proc. SPIE 5601 (October 2004) 133–144.
[36] C. Lin, M. Wu, J. Bloom, I. Cox, M. Miller, Y. Lui, Rotation, scale, and translation resilient watermarking for images, IEEE Trans. Image Process. 10 (5) (May 2001) 767–782.
[37] V. Solachidis, I. Pitas, Circularly symmetric watermark embedding in 2-D DFT domain, IEEE Trans. Image Process. 10 (11) (November 2001) 1741–1753.
[38] J. Ruanaidh, W. Dowling, F. Boland, Phase watermarking of digital images, in: Proceedings of the IEEE International Conference on Image Processing, Switzerland, September 1996, pp. 239–242.
[39] J. Ruanaidh, T. Pun, Rotation, scale and translation invariant digital image watermarking, in: Proceedings of the IEEE International Conference on Image Processing, October 1997, pp. 536–539.
[40] E. Ganic, N. Zubair, A. Eskicioglu, An optimal watermarking scheme based on singular value decomposition, in: Proceedings of the IASTED International Conference on Communication, Network, and Information Security, 2003, pp. 85–90.
[41] D. Chandra, Digital image watermarking using singular value decomposition, in: Proceedings of the IEEE 45th Midwest Symposium on Circuits and Systems, vol. 3, August 2002, pp. 264–267.
[42] R. Sun, H. Sun, T. Yao, A SVD and quantization based semi-fragile watermarking technique for image authentication, in: Proceedings of the 6th International Conference on Signal Processing (ICSP'02), August 2002, pp. 1592–1595.
[43] H. Ozer, B. Sankur, N. Memon, An SVD based audio watermarking technique, in: Proceedings of the 7th ACM Workshop on Multimedia and Security, August 2005, pp. 51–56.
[44] X. Zhang, K. Li, Comments on an SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 7 (3) (April 2005) 593–594.
[45] J. Liu, X. Niu, W. Kong, Image watermarking based on singular value decomposition, in: Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pasadena, CA, USA, December 2006, pp. 457–460.
[46] W. Kong, B. Bian, D. Wu, X. Niu, SVD based blind video watermarking algorithm, in: Proceedings of the International Conference on Innovative Computing, Information and Control, Beijing, China, August 2006, pp. 265–268.
[47] W. Kong, B. Bian, D. Wu, X. Niu, Additive vs. image dependent DWT-DCT based watermarking, in: Proceedings of International Workshop, MRCS, Istanbul, Turkey, September 2006, pp. 98–105.
[48] Y. Hu, Z. Chen, An SVD-based watermarking method for image authentication, in: Proceedings of 2007 International Conference on Machine Learning and Cybernetics, vol. 3, Hong Kong, China, August 2007, pp. 1723–1728.
[49] L. Lamarche, Y. Lui, J. Zhao, Flaw in SVD-based watermarking, in: Proceedings of Canadian Conference on Electrical and Computer Engineering, MRCS, Ottawa, Canada, May 2006, pp. 2082–2085.
[50] C. Chang, C. Lin, Y. Hu, An SVD oriented watermark embedding scheme with high qualities for the restored images, Int. J. Innovative Comput. Inf. Control 3 (3) (June 2007) 609–620.
[51] C. Chang, Y. Hu, C. Lin, Digital watermarking scheme based on singular value decomposition, in: Proceedings of the International Symposium on Combinatorics, Algorithms, Probabilistic and Experimental Methodologies, September 2007, pp. 82–93.
[52] J. Liu, C. Lin, L. Kuo, J. Chang, Robust multi-scale full-band Image watermarking for copyright protection, in: Proceedings of the 20th International Conference on Industrial, Engineering, and Other Applications of Applied Intelligent Systems, Kyoto, Japan, June 2007, pp. 176–184.
[53] J. Shieh, D. Lou, M. Chang, A semi-blind watermarking scheme based on singular value decomposition, Comput. Stand. Interface 28 (2006) 428–440.
[54] R. Ghazy, N. El-Fishawy, M. Hadhoud, M. Dessouky, F. El-Samie, An efficient block-by block SVD-based image watermarking scheme, in: Proceedings of the 24th National Radio Science Conference, Cairo, Egypt, March 2007, pp. 1–9.

[55] P. Bao, X. Ma, Image adaptive watermarking using wavelet domain singular value decomposition, IEEE Trans. Circuits Syst. Video Technol. 15 (1) (January 2005) 96–102.
[56] E. Yavus, Z. Telatar, Improved SVD-DWT based digital image watermarking against watermark ambiguity, in: Proceedings of the 2007 ACM Symposium on Applied Computing, Seoul, Korea, March 2007, pp. 1051–1055.
[57] C. Chan, L. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (March 2004) 469–474.
[58] D. Mukherjee, S. Maitra, S. Acton, Spatial domain digital watermarking of multimedia objects for buyer authentication, IEEE Trans. Multimedia 6 (1) (February 2004) 1–15.
[59] F. Sebe, J. Domingo-Ferrer, J. Herrera, Spatial domain image watermarking robust against compression, filtering, cropping, and scaling, in: Proceedings of the 3rd International Workshop on Information Security, Australia, December 2000, pp. 44–53.
[60] R. Wang, C. Lin, J. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (March 2001) 671–683.
[61] R. Schyndel, A. Tirkel, C. Osborne, A digital watermark, in: Proceedings of the International Conference on Image Processing, vol. II, USA, 1994, pp. 86–90.
[62] R. Schyndel, A. Tirkel, C. Osborne, Towards a robust digital watermark, in: Proceedings of the ACCV-95 Conference, Singapore, December 1995, pp. 504–508.
[63] W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3–4) (1996) 313–335.
[64] I. Cox, M. Miller, A review of watermarking and the importance of perceptual modeling, in: Proceedings of the SPIE Conference on Human Vision and Electronic Imaging II, vol. 3016, USA, February 1997, pp. 92–99.
[65] L. Knockaert, B. Backer, D. Zutter, SVD compression, unitary transforms, and computational complexity, IEEE Trans. Signal Process. 47 (10) (October 1999) 2724–2729.
[66] H. Andrews, C. Patterson, Singular value decompositions and digital image processing, IEEE Trans. Acoust. Speech Signal Process. 24 (1) (February 1976) 26–53.
[67] G.H. Golub, C.F. Van Loan, Matrix Computations, Johns Hopkins University Press, Baltimore, MD, 1989.