Algorithms **2009**, *2*, 46-75; doi:10.3390/a2010046

OPEN ACCESS

algorithms

ISSN 1999-4893

www.mdpi.com/journal/algorithms

Article

A Novel Block-based Watermarking Scheme Using the SVD Transform

Alessandro Basso*, Francesco Bergadano, Davide Cavagnino, Victor Pomponiu and Annamaria Vernone

Department of Computer Science, Università degli Studi di Torino, 10149, Torino, Italy

E-mails: {basso, bergadano, davide, pomponiu, vernone}@di.unito.it

* Author to whom correspondence should be addressed.

Received: 29 August 2008; in revised form: 11 December 2008 / Accepted: 14 January 2009 / Published: 22 January 2009

Abstract: In this paper, a block-based watermarking scheme based on the Singular Value Decomposition (SVD) is proposed. Our watermark, a pseudo-random Gaussian sequence, is embedded by modifying the angles formed by the right singular vectors of each block of the original image. The orthogonality property of the right singular vector matrix is preserved during the embedding process. Several experiments have been carried out to test the performance of the proposed scheme against different attack scenarios. We conclude that the proposed scheme is resistant against common signal processing operations and attacks, while it preserves the quality of the original image.

Keywords: digital image watermarking, Singular Value Decomposition, singular vectors, orthogonality, security.

1. Introduction

In recent years, the necessity to protect multimedia content from illegal copying has been made more critical by the advent of digital technology. A common and well-discussed solution to counter the unauthorized distribution of copyrighted contents is applied by means of digital watermarking. This term refers to specific information hiding techniques whose purpose is to embed secret information inside multimedia contents, such as images, video or audio streams. The watermark, i.e., the signal added to digital media, can be detected and retrieved when necessary. In the specific field of copyrighted content protection, the objective is to identify the media's owner by means of a specific user-related watermark.

The majority of watermarking techniques can be categorized as algorithms operating either in the *spatial domain* or in the *transform domain*. Examples of embedding schemes, which insert the mark in the *spatial domain* by modifying a subset of the image pixels, are analyzed in [1-5]. Watermarking schemes operating in the *transform domain* represent the original image in a transformed domain where the embedding is performed. They are generally more robust than those in the spatial domain, since most of the attacks can be characterized and modeled in the transform domain [6]. Common examples are methods based on the *frequency domain*, such as Discrete Cosine Transform (DCT) [7], Discrete Fourier Transform (DFT) [8] and Discrete Wavelet Transform (DWT) [9], or schemes based on the Singular Value Decomposition (SVD).

The general requirement in devising a new watermarking scheme for copyright protection is to achieve a compromise between the invisibility of the hidden watermark, while maintaining a high quality of the digital media, and its robustness against common signal processing operations and specific attacks aimed at removing the watermark or making it undetectable. In recent years, different human visual models (Watson model, masking functions, etc.) have been extensively exploited to achieve such an optimal compromise [10, 11].

A watermarking algorithm is generally classified as *robust* or *fragile*. The former is characterized by a high resistance to attacks and can be considered as one of the most interesting and widespread applications of digital watermarking. For information about the latter, the reader may refer to [12].

A further classification may be given according to evidence of ownership; indeed, watermarking schemes are generally considered *invertible* or *non-invertible*. In fact, suppose that the original image is I_o and W is the watermark to be inserted; then, the embedding process is carried out by means of a function E, defined as follows:

$$I_w=E\{I_o, W\}, \tag{1}$$

where I_w is the watermarked image. A scheme is said to be non-invertible if it is computationally unfeasible for an attacker to use the watermarked image I_w to construct a fake original image I_{oF} and a fake watermark W_F so that $E\{I_o, W\} = E\{I_{oF}, W_F\}$.

In addition, watermarking schemes can also be categorized in the following three classes: *non-blind methods*, which require at least the original media and, in some cases, the original watermark in the detection process; *semi-blind schemes*, which use only the original watermark or some other side information; and *blind algorithms*, which use neither the original data nor the watermark in the detection process [13]. According to the studies of Craver *et al.* [14], using invisible watermarks to establish rightful ownerships requires that the original media *isn't directly used* in the extraction process. Therefore, non-blind watermarking schemes are not suitable for proving the ownership of a digital media.

In this paper we introduce a novel block-based watermarking scheme, which uses the Singular Value Decomposition transform. The proposed scheme works by initially splitting the original image into non-overlapping blocks, applying the SVD transform to each of them and subsequently embedding a watermark into the singular vectors. Each watermark value is embedded by modifying a set of singular vector angles, i.e., angles formed by the right singular vectors of each block. The main contribution of this work can be identified in:

- the use of the angles formed by the singular vectors to embed the watermark while maintaining the property of orthonormality. To our knowledge, there are no watermarking schemes, based on singular vectors, that respect this property;
- an increased security of the watermarking process based on the SVD transform, due to the use of singular vectors for the watermark insertion rather than singular values. Indeed, many of the existing SVD-based algorithms embed the watermark into the singular values of the image, which implies a high robustness against common image processing operations and geometric attacks but, on the other hand, a complete vulnerability towards attacks based on singular value substitution, as explained for example in [15, 16].

The remainder of the paper is organized as follows: Section 2 presents detailed information on the SVD transform, while Section 3 introduces the most relevant works related to digital watermarking based on SVD. Section 4 is completely focused on the description of the novel scheme, detailing both the embedding and detection procedures, whose main properties are subsequently examined in Section 5. In Section 6, experimental results are shown to prove the effectiveness of the proposed solution. Finally, in Section 7 we conclude discussing open problems and possible improvements of our watermarking algorithm.

2. SVD Transform

In linear algebra, the Singular Value Decomposition (SVD) is a well-known technique for factorizing a rectangular matrix, real or complex, which has been widely employed in signal processing, like image compression [17, 18], noise reduction or image watermarking. Recently, the SVD transform was used to measure the image quality under different types of distortions [19].

Suppose to have an image represented as a matrix of size *m* rows by *n* columns, $A_{m\mathrm{x}n}$; applying the SVD on matrix *A* will result in the three decomposition matrices $U_{m\mathrm{x}m}$, $S_{m\mathrm{x}n}$ and $V_{n\mathrm{x}n}$, as shown in (2):

$$SVD(A_{m\times n}) = [U_{m\times m} S_{m\times n} V_{n\times n}] \tag{2}$$

By multiplying *U*, *S* and V^T (where V^T means the transpose of *V*) we obtain the matrix *A*:

$$A_{m\times n} = U_{m\times m} \cdot S_{m\times n} \cdot V_{n\times n}^T = \sum_{i=1}^{\min(m,n)} \sigma_i \cdot u_i \cdot v_i^T \ , \tag{3}$$

where $\sigma_i \in \Re_+$, $i = 1 \ldots \min(m,n)$ are the *singular values*, i.e., the available diagonal elements of the matrix *S* sorted in descending order, u_i are the *left singular vectors*, i.e., the columns of *U*, and v_i are the *right singular vectors*, i.e., the rows of V^T (or columns of *V*). *U* and *V* are unitary matrices, that means $U{\cdot}U^T{=}I_{m\mathrm{x}m}$, $V{\cdot}V^T{=}\ I_{n\mathrm{x}n}$, where $I_{m\mathrm{x}m}$ and $I_{n\mathrm{x}n}$ are the unit matrices.

To calculate the SVD we need to compute the eigenvalues and eigenvectors of $A{\cdot}A^T$ and $A^T{\cdot}A$. The eigenvectors of $A{\cdot}A^T$ form the columns of *U*, whilst the eigenvectors of $A^T{\cdot}A$ form the columns of *V*. Moreover, the singular values (SVs) in *S* are the square roots of the eigenvalues of $A^T{\cdot}A$ or $A{\cdot}A^T$.

Note that increasing the magnitude of the singular values of matrix *S* will increase the image luminance, while lowering the magnitude will decrease the image luminance. Therefore, it is correct to state that *S* is in close relation with the image luminance, while the intrinsic "geometry" of the image depends upon orthogonal matrices *U* and *V* which represent, respectively, the *horizontal* and *vertical details* (edges) of the image [20].

From (3) we can observe that each SV is multiplied by the corresponding left and right singular vectors. Hence, this creates different image layers, i.e., a sum of rank-one matrices, where the first image layer (generated multiplying the first SV by the left and right singular vectors) represents the image profile, which concentrates a large amount of the energy contained into the final image [15]. Left and right singular vectors which correspond to the largest SV represent the shape (i.e., strong edges) of the image, while the rest of singular vectors expresses edges and texture regions.

Another interesting feature of the SVD is the invariance of SVs to common image processing operations (except for noise addition) and geometric transforms, like rotation, translation and scaling [21]. Due to these properties, the SVD has been used (also combined with other techniques) for devising watermarking algorithms particularly resistant to geometric attacks.

3. Related Works

3.1 Overview of the SVD-based watermarking schemes

The applications of SVD in the robust digital watermarking context can be classified in:

- watermarking algorithms which embed the watermark or its singular values into the *singular values* of the host image;
- watermarking algorithms which insert the watermark by modifying the *right/left singular vectors* of the host image;
- watermarking techniques based on modification of *singular vectors* and *values*; the watermark inserted in *singular vectors* is used as a control parameter to avoid the false positive problem;
- watermarking methods that combine all features of the SVD transform (*singular vectors/values*) with others transforms (DFT, DCT, DWT, Zernike Moments Transform, Haar Transform, Hadamard Transform).

3.2 Watermarking algorithms based on Singular Values

In the literature, watermarking methods from the first category insert the mark in different ways. The simplest embedding scheme consists in adding the watermark by modifying the SVs of the whole host image (e.g., a gray-scale image), where the embedded watermark is a logo binary image or a pseudo-random generated sequence [22, 23]. Another variant is to apply the SVD transform also to the watermark, followed by insertion of the watermark singular values into the SVs of the image [24]. These methods are non-blind or blind [22], and are characterized by a simple implementation.

Instead of applying the SVD to the whole image, other schemes split the original image (and the watermark) into non-overlapping blocks, which are then transformed using the SVD. In the embedding process, SVs of the mark are added to SVs of the blocks of the image [25, 26]. The detection process can be blind [27, 28], semi-blind [26], or non-blind [29]. In [24] the authors proposed an algorithm which embeds the watermark (a gray-scale image) in the host image as follows: firstly, a block-based SVD transform (layer 1) is applied to the host image, while a whole SVD transform is performed on the watermark. Each SV of the watermark is then added to the largest SV of each block. Afterward, a global SVD (layer 2) is performed and the SVs of the watermark are added to those of the host image.

In several schemes, the embedding space is chosen basing the selection on feature extraction tools, like the Canny edge detector [29] and an entropy masking function [30].

Other techniques embed the watermark, which can be a pseudo-random sequence [21, 30], or a gray-scale image [20] or a binary image sequence (technique 2 in [31]), directly into the largest SV or by quantizing the largest SV of each block of the host image. The detection process is non-blind for [30] and [31], whereas it does not use the original image for schemes that quantize the largest SV (in [15, 21]).

The main drawbacks of the presented schemes can be summarized as follows:

- *False positive*. As stated in [16, 31-35], these schemes are subject to the *false positive problem*, which is an erroneous detection of a watermark in a content which does not actually contain one [36]. However, a false positive may occur also when a specific watermark is detected from a content in which a different watermark was embedded, causing an *ambiguous situation* [32]. This fact does not allow one to solve the *rightful ownership problem* [37]. In general, SVD-based watermarking methods which embed the Singular Values of the watermark into the Singular Values of the host image are considered invertible schemes [31]. Thus, they are vulnerable to the false positive problem, which appears in the detection phase, during the watermark reconstruction. Recently, Mohammad *et al*. [31] proposed a scheme which modifies the Tan's algorithm [23] in order to solve this problem. However, the algorithm cannot resist against common and geometric attacks even if the original image is used in the detection process.
- *Quality of the watermarked image*. In these schemes, modifying the largest SV may degrade the watermarked image, thus it is necessary to use an adequate strength factor in the embedding process, which attenuates the energy of the watermark and thus lowers the resistance against attacks.
- *Payload.* To increase the payload of these schemes the host image is split into small blocks; this fact lowers the robustness against common attacks (e.g., JPEG compression and noise addition) since the stability of the SVs decreases when reducing the size of the blocks.
- *Robustness*. Some of the presented algorithms aren't robust to common image manipulation and geometric attacks [20, 26, 27, 30, technique 1 in 31].
- *BER*. Exact extraction of the watermark cannot be achieved, i.e., the bit error rate (BER) between the original watermark and the recovered one is not zero [23, 35, 38]. This causes a decrease in robustness against signal processing operations and common attacks.
- *Security.* Most of the proposed schemes [23, 29, technique 1 in 31, 38] cannot be considered secure because they do not use any secret information in the watermarking process. To increase security and also to avoid the false positive problem, these algorithms must use secrets for choosing the embedding blocks [27, 28] or preprocess the watermark and the original image before embedding [24-26].

3.3 Watermarking algorithms based on singular vectors

In recent years, several watermarking schemes, which embed the watermark bits into the left or right singular vectors (matrices *U* and *V*), have appeared. The first algorithm based on singular vectors was proposed by Chang [39]. The host image is a grayscale image, whereas the watermark is a binary image. The embedding process can be briefly described as follows: the host image is divided into non-overlapping blocks of size 8×8, and blocks with higher ranks (i.e., complex blocks) are selected for embedding using a secret key. Each watermark bit is embedded by modifying the relation between the second and third coefficient of the first column of matrix *U*. The algorithm is robust to common attacks and the original image is not required in the detection process. However, using this algorithm an exact watermark extraction can't be achieved [29]. This is caused by the values of the *U* matrix which belong to the interval [-1..1]. Another defect of this technique is related to the selection of the higher rank blocks, since rank is not a reliable parameter [40, 41].

In [40], the authors propose a similar watermarking scheme except for the use of the *V* matrix in the embedding process. To improve the security, the components from the first column of the matrices *U* and *V* are randomly selected using a secret key. It is shown that the algorithm is robust against common attacks. Nonetheless, the bit error rate (BER) between the original watermark and the recovered one is different from zero.

3.4 Watermarking algorithms based on Singular values and vectors

In 2008, Chandra *et al.* [41] proposed a hybrid block-based watermarking scheme. The host image is divided into four blocks and the watermark (i.e., a binary image) is embedded twice: firstly in the largest SV of upper-left block (previously segmented into sub-blocks) by means of quantization, and secondly in the bottom-right block (segmented as well into sub-blocks), by using the method proposed by Chung *et al.* [42]. To enhance the security of the scheme the watermark is permuted before the embedding process. A quantization table formed with the largest SV of each block of the original image is used in extraction. The algorithm is robust against common and geometric attacks. However, by modifying only the upper-left and bottom-right blocks of the cover image, some images may show artifacts at the block's borders of the watermarked image (i.e., strong luminance differences between upper-left corner and upper-right or bottom-left corners).

It is important to mention that all the previously cited watermarking schemes based on singular vectors don't preserve the orthogonality property of the *U* and *V* matrices, since the transformation used to embed the watermark is nonlinear. It is very difficult to embed the watermark into the singular vectors of the host image while preserving the orthogonality, because it is necessary to devise an orthogonal transformation for watermark insertion and, at the same time, to preserve the quality of the watermarked image.

3.5 Combined watermarking algorithms

SVD has been used also in combination with other transforms, like DCT [35, 43-50]. The scheme proposed in [15] decomposes the original color image (in RGB format) into *YUV* components and splits the *Y* component into non-overlapping blocks. To embed the watermark bits, the largest SV of each block is quantized. The security is then improved by performing a torus permutation on the watermark image. The proposed scheme is robust to most attacks and does not need the original image in the detection process. A similar scheme is proposed in [35], where authors add the SVs of the watermark to the SVs of the approximation image, i.e., the image formed by the DC coefficients from each block. To avoid the false positive problem, the watermark matrix of the right singular vectors is embedded into the 2nd and 3rd AC coefficients of each block, as a control parameter. This information is later used in the extraction process, which requires the original image; however, the watermark cannot be extracted with zero bit error rate. In 2006, the paper [32] showed that the detection process of the scheme proposed in [43] is subject to the false positive problem. The same considerations can be applied to the algorithm proposed in [46].

The SVD transform was also used to devise semi-fragile watermarking schemes [15, 51, 52], which are used for data authentication.

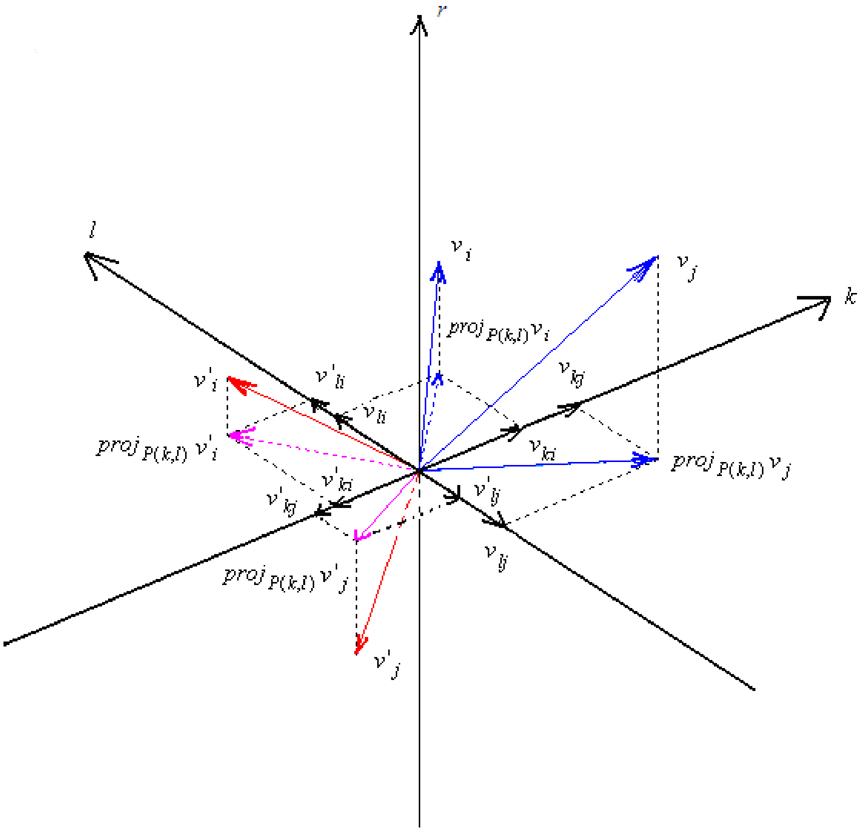
4. Proposed Watermarking Scheme

Generally, the SVD transform can be applied to an image with two different techniques: on the whole image and on blocks of the image. The former tends to spread the watermark all over the image, whereas the latter only affects local regions of the image. The watermarking scheme we propose in this paper is block-based, i.e., it splits the original image into a number of blocks and applies the SVD transform to each of them, producing a matrix of SVs (S) and two matrices of vectors (U, V) for each block.

The basic idea of the proposed algorithm is to act on some of these vectors, rotating them so to embed the watermark into angles related to such vectors and, at the same time, maintain the orthonormality of the matrices U and V. The angles considered here are the ones formed by the projection of the chosen vectors on selected planes with respect to the axes defining the planes. The watermarking algorithm is based on the idea of Zeng *et al.* [53], a feature-based watermarking scheme which embeds the watermark, i.e., an independent identical distributed pseudo-random sequence W, into a set of features F obtained from the original image I_o.

We consider that I_o is a gray-scale image of size $N\times N$ and the watermark W is a pseudo-random sequence, with zero mean and unitary variance, of size n^2, where $n=N/M$ and $M\times M$ is the size of a single block. Our feature set F is composed by angles identified by the components of the projection of a vector v_i on the hyper-plane P(k, l), i.e., $proj_{P(k,l)} v_i$; we refer to such components as v_{ki} and v_{li}. Each value of the watermark is considered as an angle, which is used to rotate the right singular vector v_i of each block of the original image, obtaining a new rotated vector, v'_i. A visual representation of the initial vector v_i, the rotated one v'_i, their projections and their components is given in Figure 1.

Figure 1. Three-dimensional visual representation of the vectors involved in the watermark embedding.



To perform the rotation, we use a unitary transformation matrix constructed as presented in [54]. The orthonormality property of the matrix V is maintained by rotating a second vector v_j together with vector v_i.

To improve the security of the algorithm, a secret key K is used to choose the right singular vectors, which will be rotated to embed the watermark, and the corresponding coefficients that determine the secret plane. The secret key, which allows the watermarking algorithm to be public, also contains a value which is used to initialize the pseudo-random generator to produce the watermark sequence W. For the specific purpose of content protection, note that such a value must be univocally associated with the copyright owner identity, e.g., applying a standard hash function to the string containing his name.

4.1 Watermark embedding

The steps of the embedding algorithm can be described as follows:

1) Split the host image I_o of size $N \times N$ into n^2 non-overlapping blocks, B_b, of size $M \times M$, where $M = N/n$ and $1 \leq b \leq n^2$.
2) Generate the watermark W, i.e., a pseudo-random Gaussian sequence of size n^2, by means of the secret key K.
3) Apply the SVD transform to each block:

$$SVD(B_b) = [U_b S_b V_b] \tag{4}$$

The computation of the SVD transform is based on the QR method [55], to which we add the sign flip correction function [56] (see Section 5 for details).

4) From the secret key K, extract the indices i and j that choose the v_i and v_j vectors belonging to the matrix V_b. From K, also extract the indices k and l which define the components on v_i and v_j, used to compute the secret plane P(k, l). For simplicity, we refer to such components as $x = v_{ki}$, $y = v_{li}$, $z = v_{kj}$ and $w = v_{lj}$.
5) Compute the angle θ_b, derived by the projection of vector v_i with the positive axis k, i.e., $\angle(k, proj_{P(k,l)}\, v_i)$ defined by the components x and y, using the four quadrant arctangent function (see Appendix A):

$$\theta_b = \frac{\arctan(y,x)}{\delta} \tag{5}$$

θ_b is then inserted in the feature set F.

The scaling factor δ is used to obtain a feature angle that is not close to the point of discontinuity in $-\pi$ and π. In this way, all angles are “compressed” around the origin, so the modification made by the watermark insertion should not allow the angle to bypass the discontinuity point. This can be obtained by carefully choosing the scaling factor and the watermark strength, taking also into account that the angle obtained after the watermark insertion should, in theory, span all the range *[-π..π]*. Nonetheless, it is possible (in a few cases, if the multiplicative constants are not carefully chosen) that for large values of the feature angle and of the watermark, the discontinuity will be traversed.
6) Compute the angle α_b, by adding the angle extracted from the watermark sequence W_b to the angle θ_b:

$$\alpha_b = \theta_b + \beta \cdot W_b \tag{6}$$

where β is the strength factor of the embedded watermark.
7) Determine the rotation angle φ_b, which is needed to rotate the v_i and v_j vectors in the plane P(v_i, v_j) so that $\alpha_b = \angle(k, proj_{\ P(k,l)}\, v_i^{'})$. To obtain this result, we apply the following relation (for its derivation see Appendix B):

$$\varphi_b = \begin{cases} \chi, & \text{if } \begin{cases} y \cdot \cos\varphi_b - w \cdot \sin\varphi_b < 0 \text{ and } \alpha_b > 0 \quad \text{or} \\ y \cdot \cos\varphi_b - w \cdot \sin\varphi_b > 0 \text{ and } \alpha_b < 0 \end{cases} \\ \tau, & \text{otherwise} \end{cases} \quad . \tag{7}$$

$$\chi = \arctan(x \cdot \sin\alpha_b - y \cdot \cos\alpha_b, z \cdot \sin\alpha_b - w \cdot \cos\alpha_b) + \pi$$
$$\tau = \arctan(x \cdot \sin\alpha_b - y \cdot \cos\alpha_b, z \cdot \sin\alpha_b - w \cdot \cos\alpha_b)$$

8) Construct the unitary transformation matrix G_b which rotates clockwise a single pair of right singular vectors, i.e., v_i and v_j, in the plane P(v_i, v_j), by an angle φ_b:

$$G_b = \begin{array}{c} \left[\begin{array}{cccccccc} 1 & \ldots & 0 & & \cdots & 0 & \cdots & 0 \\ 0 & \ddots & & & & & & \vdots \\ & & \cos\varphi_b & 0\cdots & \cdots 0 & -\sin\varphi_b & & 0 \\ \vdots & & & 1\ddots & & & & \vdots \\ & & & & \ddots 1 & & & 0 \\ 0 & \cdots & \sin\varphi_b & 0\cdots & \cdots 0 & \cos\varphi & & \\ & & & & & & 1\ddots & \\ 0 & & & 0 & & & & \ddots 1 \end{array}\right] \\ \begin{array}{cccccccc} & & i & & & j & & \end{array} \end{array} . \tag{8}$$

9) Apply the transformation matrix to V_b:

$$V_b' = V_b \cdot G_b^T \tag{9}$$

where V'_b is the modified matrix of the right singular vectors.

10) Reconstruct the modified watermarked image block using V'_b:

$$B'_b = U_b \cdot S_b \cdot V_b'^T . \tag{10}$$

To obtain the watermarked image I_w, we apply the above steps for all image blocks.

4.2 Watermark detection

The following steps describe the detection algorithm:

1) Apply the first three steps of the embedding on the possible watermarked and attacked image, I_{wa}, by means of the secret key K.
2) Construct the feature set F' with angles computed using the same procedure presented in step 5 of the embedding process. The angle θ'_b is determined using vectors v'_i and v'_j and their relative components $x' = v'_{ki}$, $y' = v'_{li}$, $z' = v'_{kj}$ and $w' = v'_{lj}$, according to the following relation:

$$\theta'_b = \frac{\arctan(y', x')}{\delta} . \tag{11}$$

3) To detect the watermark in the extracted feature set F' we construct the following hypothesis test [53]:

$$\begin{aligned} H_0 &: \quad F' = F + Z \\ H_1 &: \quad F' = F + \beta \cdot W + Z \end{aligned} \tag{12}$$

where F and F' are, respectively, the initial and the extracted feature sets, W is the watermark sequence and Z is the noise signal. Under the null hypothesis H_0 the original image is unmarked, whereas under the alternative hypothesis H_1 the watermark sequence W is embedded into the original image.

4) Compute the test statistic q with the following relation:

$$q = \frac{Mean_Y \cdot \sqrt{L}}{Var_Y} \tag{13}$$

where $Mean_Y$ and Var_Y are, respectively, the sample mean and the Root Mean Square Error (RMSE) of $Y = \sum_{i=1}^{n^2} F_i' \cdot W_i'$, whilst $L=n^2$ is the size of the feature set F'. According to [53], since the watermark strength factor β is a constant value, then it is possible to use $W_i' = W_i$, that is the sequence generated from the seed contained in the key. Intuitively, the value q measures the correlation between the watermark sequence and the extracted feature set.

5) The value of q computed above is compared with the acceptance threshold T which is calculated, under the hypothesis H_1 and for large L, with the relation:

$$T = \frac{m_{H_1}}{2} \cong \frac{1}{2} \cdot \frac{\beta \cdot \sum_{i=1}^{n^2} W_i \cdot W_i' + \sum_{i=1}^{n^2} Z_i \cdot W_i'}{Var_Y \cdot \sqrt{L}} . \tag{14}$$

where m_{H_1} is the mean of the distribution of the output statistic q under the hypothesis H_1.

As proposed by Zeng *et al.* [53], in the above relation we disregard the noise factor Z; then, if $q \geq T$, we consider that the watermark sequence W is present in the feature set F'.

5. Considerations on the Proposed Scheme

The proposed watermarking algorithm performs a block-wise SVD transform on the original image. Naturally, the first question that we encounter is: which is the optimal size of the blocks used throughout the watermarking process? We noticed that the embedding block size is an important parameter which affects the requirements, properties and behaviour of the watermarking scheme.

It is important to note that the application of a block-wise transform on the original image produces more robust features against signal processing operations and common attacks, than features provided by a whole transform. Moreover, the features obtained from the SVD transform (i.e., singular values and vectors) have a different behaviour: the *stability* (and, implicitly, the *robustness*) of the singular values and vectors is inversely proportional to the size of the segmentation block. Indeed, the SVD transform produces highly stable features when performed on large images (blocks). In general, the attacks which are very sensitive to the segmentation size are JPEG compression and noise addition (e.g., white Gaussian noise or salt and pepper noise) [20]. On the other hand, by splitting the cover image into small blocks, the watermark sequence can be embedded redundantly, i.e., each bit of the watermark is inserted in more image blocks. This ability confers to the watermarking scheme a high robustness against geometric attacks (e.g., translation, cropping and scaling).

Unfortunately, to achieve robustness against the geometric attacks it is required to embed the watermark redundantly which causes a sharp reduction of the watermark payload, i.e., number of bits which can be embedded into the cover image [36]. Thus it is necessary to realize a trade-off between the robustness against geometric attacks and the payload of the watermark sequence.

Besides these requirements of the watermarking scheme (robustness and payload) it is important to take into consideration the quality of the watermarked image [57] which is related to:

- *Imperceptibility*: A perfectly imperceptible bit sample of the watermark is present if the watermarked media and the original cannot be distinguished.
- *Undetectability*: The digital content due to the carried watermark information is not detectable if it is *consistent* with the original data. Non-detectability cannot be directly linked to non-perceptibility that is based on the concepts of human perceptions. Non-detectability is related to the data source and its components. It describes the consistency with the original data.

It is important to mention that segmenting the original image into small blocks satisfies the undetectability and imperceptibility features.

Another important property that we need to consider when devising watermarking schemes is *security*. All existing watermarking algorithms which are not *secure* cannot be used for copyright protection, for data authentication or to trace the illegal distribution of the digital content. Thus, a robust watermarking algorithm is *secure* if an attacker, exploiting the knowledge of the applied watermark procedure and without knowing the secret keys used to watermark the digital content, cannot damage or destroy the hidden information of the watermark [36]. Moreover, complexity of the watermarking procedure may be related to security, since an attacker will be discouraged to search the embedding locations in a large embedding space and for a long secret key. Therefore, to increase the security of the algorithm, we can enlarge the embedding space and increase the size of the secret key by splitting the cover image into small blocks.

In our scheme, the secret key K consists of two parts:

- The seed used to generate the watermark sequence W, i.e., the Gaussian distribution with zero mean and unitary variance.
- The singular vectors chosen in the watermarking process and their components from which we construct the feature set. For each block of the cover image, the secret key K produces the right singular vectors and the specific pair of their components. Note that more than one couple of vectors can be chosen to embed the watermark, with the purpose to improve the overall robustness of the watermarking process.

Thus, the secret key K can be represented mathematically as a structure with the following components:

$$K = \left\{\kappa^{seed}, \kappa^{c}{}_{1}, \kappa^{c}{}_{2}, \ldots, \kappa^{c}{}_{n^2}\right\} \tag{15}$$

where κ^{seed} is a random number used as the seed of the watermark sequence W; $\kappa^{c}{}_{b}$ is a vector with the following structure

$$\kappa^{c}{}_{b} = (i, j, k, l), \quad b \in [1..n^2], \quad i, j \in [3..M] \quad k, l \in [1..M], i \neq j \text{ and } k \neq l \tag{16}$$

where, for every block, i and j identify the singular vectors in the matrix V (v_i and v_j) and k and l define the components of v_i and v_j used to compute the secret hyper-plane P(k, l). Note that the first two singular vectors are excluded from rotation since the corresponding singular values, s_1 and s_2, concentrate a large amount of energy of the image. Their modification is therefore extremely difficult without excessively affecting the quality of the image.

By using such a key structure, the overall security of the scheme is considerably improved, because it is computational infeasible, for an attacker, to find the embedding space of the watermark, i.e., the right singular vectors and their corresponding components. For this reason, attacks such as singular vector substitution or re-watermarking are unlikely to succeed without severely damaging the attacked image.

It was recently discovered that singular vectors are affected by a form of ambiguity called *sign ambiguity* [56]. More precisely, the SVD arbitrarily assigns the sign of each singular vector. This has significant consequences in many applications which use SVD to process and analyze data. In our scheme, the sign ambiguity of the singular vectors changes the sign of their components which are used in the detection process to recover the embedded watermark angle; therefore it can modify the extracted feature set F' to such an extent that it becomes impossible to correctly detect the presence of the watermark. To solve this ambiguity we apply the algorithm proposed by Bro et al. [56], which suggests to determine the sign of a singular vector by computing the sign of the inner product of this vector and individual data vectors taken from the data set, that is, in our case, the original image.

With the proposed solution, good results are obtained when the inner products are not close to zero. Instead, to avoid an arbitrary sign assignment when the inner products are close to zero, the algorithm proposed in [56] considers the combined magnitudes of both left and right singular vectors. As far as we know, our method is the first SVD based watermarking scheme which takes into account the sign ambiguity of the singular vectors and attempts to solve it.

6. Experimental Results

In this section we show the robustness of the proposed scheme respect to signal processing operations and common attacks by applying the watermarking algorithm on different pictures taken from well-known data sets used for image processing [58, 59]. The experimental results were obtained using the reference gray-scale image "Lena" of size 512×512×8 bpp, which was partitioned into blocks of fixed size 16×16 ($512/n \times 512/n$, with the optimal value for $n = 32$). The size 16×16 was driven experimentally by the following considerations:

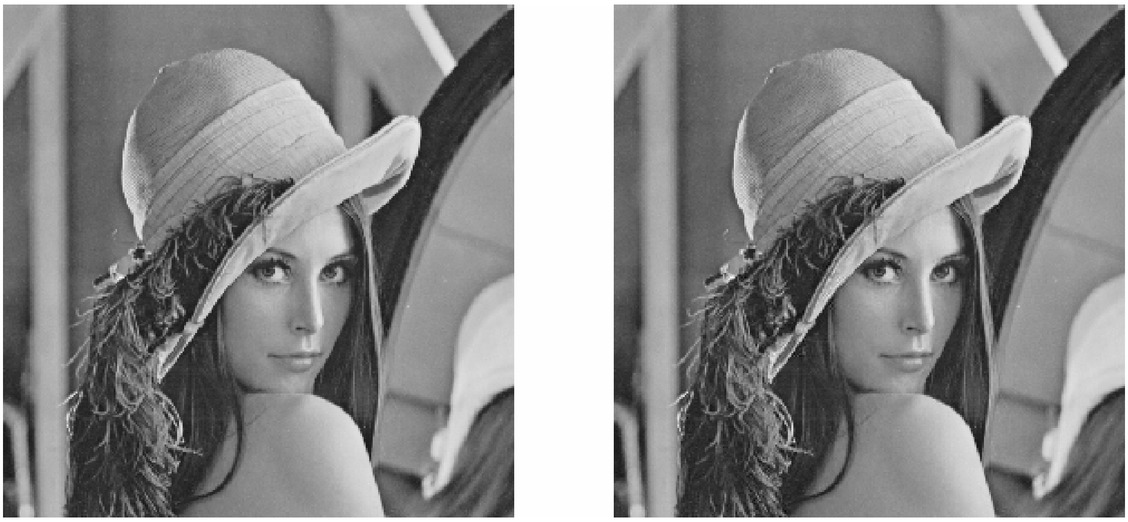
- to generate a sufficiently long sequence of features which allows to maintain the statistical properties required by the insertion/detection method;
- to have a high speed of computation of the SVD;
- to maintain a good visual quality of the watermarked image.

The latter point is subjective, whilst the previous ones are controlled by the computing power and by the statistical properties.

The watermark is a Gaussian pseudo-random sequence of size $n^2 = 1024$. The values of the watermark represent a sequence of angles, in radians, which are used to rotate a specified pair of right singular vectors of the matrix V in every block. The parameters used through the embedding process are experimentally set to the values $\beta = \pi/4$ and $\delta = 4$, which represent a compromise between the strength of the inserted mark and the quality of the watermarked image. Increasing the value of β implies larger angle fluctuations, decreasing the image quality. To avoid the discontinuity in $-\pi$ and π introduced by a large β, a corresponding larger δ is required (see step 5 in watermark embedding), and this fact implies large modifications to the original angle. By means of the secret key K, the 6th and 7th right singular vectors are selected from each block, together with the indices k and l which, for simplicity, are set to the same values. Choosing other pairs of vectors (e.g., the 2nd and 3rd) can increase the robustness of the scheme against attacks but it negatively affects the visual quality of the watermarked image.

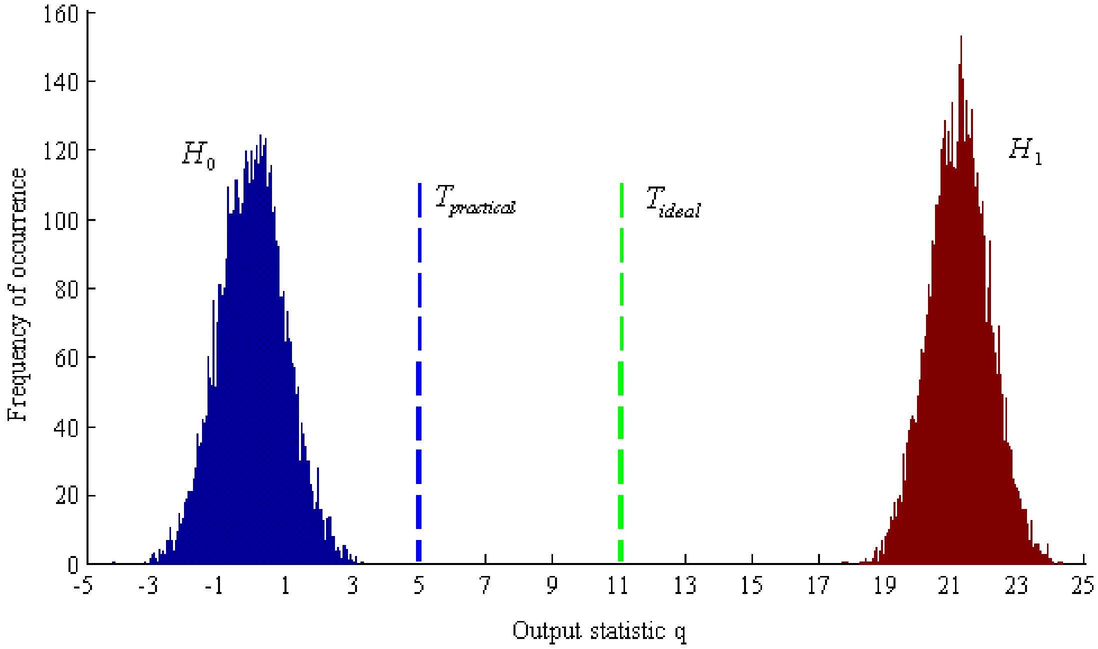
The quality measure used to compute the amount of distortion introduced by the embedding process is the Peak Signal-to-Noise Ratio (PSNR). Using 100 images we computed the average PSNR for the proposed scheme obtaining a value higher than 37 dB. A sample of the embedding process is presented in Figure 2; as the reader can note, no visual artifacts can be observed in the watermarked image.

Figure 2. Original "Lena" image on the left; watermarked image on the right (PSNR = 37.6752 dB).



The distribution of q under the hypothesis H_0 and H_1 was verified using the "Lena" image of size 512×512. Under the hypothesis H_0, we firstly generated 10,000 watermarks by setting 10,000 different seeds for the pseudo-random number generator; then, we checked the presence of these watermarks by correlating them with the original un-watermarked image. On the other hand, under the hypothesis H_1, we embedded 10,000 watermarks, generated using 10,000 different seeds, into the "Lena" image, and we subsequently applied the detection process. The distribution of q for the statistic hypothesis test is presented in Figure 3.

Figure 3. Distributions of the variable q under the hypothesis H_0 (left) and H_1 (right) for the reference image "Lena" with the ideal (dashed green line) and practical (dashed blue line) acceptance thresholds.



We can observe from Figure 3 that the output statistic q in both hypothesis tests follows a Gaussian distribution, with mean m and variance approximately one, i.e., $N(m, var)$. Moreover, under the null hypothesis, the mean of the distribution of q is m_{H_0} = 0.03 and var_{H_0} = 0.96, whereas under the alternative hypothesis the distribution of q is characterized by $m_{H_1} = 21.18$ and $var_{H_1} = 0.98$. Note that the distributions of the output statistic q in both null and alternative hypothesis are well separated. Thus, it is obvious that many thresholds between these distributions will yield both low false negative and false positive errors.

To check the presence of a watermark sequence, we compare the test statistic q with the acceptance threshold T, computed as a function of the mean m of the distribution of q under the hypothesis H_1. The ideal acceptance threshold for which the detection errors (i.e., the false negative error P_n and the false positive error P_f) are virtually zero is $T_{ideal} = \frac{m_{H_1}}{2}$. Nevertheless, as can be observed from Figure 3, we can choose an acceptance threshold much smaller (e.g., $T_{practical}$ = 5), maintaining at the same time *extremely low* values for the probability of false positive and false negative errors. The false positive detection error for different values of the acceptance threshold T is presented in Table 1.

Note that, for all values of T in Table 1, the probability of false negative error is virtually null, being $T \le m_{H_1}/2$. On the contrary, for $T > m_{H_1}/2$, P_n tends to increase, whilst P_f remains virtually zero. The robustness of the proposed scheme was tested by applying several signal processing operations and common attacks, which can also be found in the standard benchmarking tools (e.g., Stirmark, Checkmark, Optimark), to a suite of 100 watermarked images taken from common image databases [58, 59]. In Table 2, the average of the output statistic q, obtained detecting the watermark from each attacked image, is reported.

Table 1. The probability of false positive error P_f, associated to the acceptance threshold *T*.

Threshold *T*	**Probability of False positive error** P_f [$P_f\,(q \geq T)$]
3	3×10^{-4}
4	1.23×10^{-7}
5	2.54×10^{-12}
$\frac{m_{H_1}}{2}$	1.36×10^{-20}

We applied the sampling operation (i.e., up-sampling and down-sampling) on the watermarked images using different sampling factors (namely 0.8, 1.3 and 1.75). Nevertheless, the watermark can be detected with high confidence from the attacked images i.e., the averages of the output statistic *q* are 14.56, 20.16 and 18.78. Normally, the detector can easily distinguish the watermark from a down-sampled image. However, to obtain even better performance from the detector, one can firstly up-sample the attacked image by estimating the applied distortion, in case the original image is available.

Table 2. Robustness of the proposed scheme against common attacks (acceptance threshold *T* = 5).

Attack		**Factor**	**Average of the output statistic *q***
Sampling	Down	0.7	10.14
		0.8	14.56
	Up	1.3	20.16
		1.75	18.78
JPEG Compression		QF = 90	15.75
		QF = 80	11.17
		QF = 70	7.94
		QF = 60	5.83
Additive White Gaussian Noise		1%	17.69
		2%	12.87
		3%	10.59
Salt & Pepper Noise		Density = 0.001	12.81
		Density = 0.003	9.55
		Density = 0.005	7.11
Row-Column Copying		5-11	18.63
		35-78	19.08
		67-437	18.03
		3-16, 43-72	17.88
		139-126, 123-211	18.21
		333-164, 431-142	17.50
		14-26, 169-99, 119-192	17.27
		139-126, 123-211,43-72	16.80
		5-11, 35-78, 67-437	17.01

Table 2. *Cont.*

Row Column Blanking	5-11	19.65
	35-78	20.07
	67-437	20.54
	3-16, 43-72	19.12
	139-126, 123-211	20.81
	333-164, 431-142	19.75
	14-26, 169-99, 119-192	17.64
	139-126, 123-211,43-72	17.27
	5-9, 11-67, 437-500	17.60
Gamma Correction	$\gamma = 0.6$	10.31
	$\gamma = 0.8$	13.76
	$\gamma = 1.1$	14.04
	$\gamma = 1.2$	12.05
	$\gamma = 1.5$	10.58
Cropping	10%	17.12
	20%	15.26
	25%	14.41
	30%	10.34

Regarding the JPEG compression attack, the watermarked images were compressed with different quality factors QF, ranging between 100 (no compression – best quality) and 0 (maximum compression lowest quality).

As can be seen in Table 2, the average of the output statistic q decreases with the quality factor QF. The watermark can be still detected, with high confidence, if the watermarked images are compressed with a QF = 60 (the average of the value of q is 5.83).

Moreover, the average of the output response q for images with complex regions (edges, textures) is much higher, thus we can detect the watermark even if they are attacked with a higher compression factor. From our tests, we verified that the robustness against JPEG compression can be improved by:

- increasing the strength factor β;
- decreasing the multiplicative factor δ;
- increasing the size of the blocks of the original images used in the embedding process.

However, we believe that the previously suggested values for β, δ and the block size can already guarantee a good compromise between robustness and visual quality of the watermarked images.

Watermarked images were also attacked by adding white Gaussian noise (AWGN) of different intensities. The effect is a uniformly distributed noise across the image [19]. This noise is visible in all frequencies (i.e., high, middle and low frequencies) and textured regions. The average of the output statistic q is equal to 10.59 when 3% of additive white Gaussian noise is added to the watermarked images.

Another attack applied to watermarked images was the addition of salt and pepper noise with densities within the interval [0.001, 0.005]. The watermark sequence can still be detected even if the average of the output q is lower compared to other attacks. During the simulation tests, we observed that the SVD transform is less robust against aggressive noise-based attacks, such as additive white Gaussian noise or salt and pepper noise.

In the row-column copying attack random rows and/or columns are copied to random locations of the image. To better study the behavior of the proposed scheme, we divided this attack into the following sub-classes:

- 1-column copying (e.g., we copied the 5th column to the 11th column *or* the 35th column to the 78th column *or* the 67th column to the 437th column);
- 2-columns copying (e.g., we copied the 3rd column to the 16th column *and* the 43rd column to the 72nd column, etc.);
- 3-columns copying (e.g., we copied the 14th column to the 26th column *and* the 169th column to the 99th column *and* the 119th column to the 192nd column, etc.).

The same strategy was also adopted for the row-column blanking attack which selects random columns and rows and deletes them from each of the watermarked image (i.e., are replaced with zeros). Therefore, the sub-classes which correspond to this attack are:

- 1-row 1-column blanking (e.g., we deleted the 5th row and the 11th column, etc.);
- 2-rows 2-columns blanking (e.g., we deleted the 3rd and 43rd rows and the 16th and 72nd columns, etc.);
- 3-rows 3-columns blanking (e.g., we deleted the 14th, 169th and 119th rows and the 26th, 99th and 192nd columns, etc.).

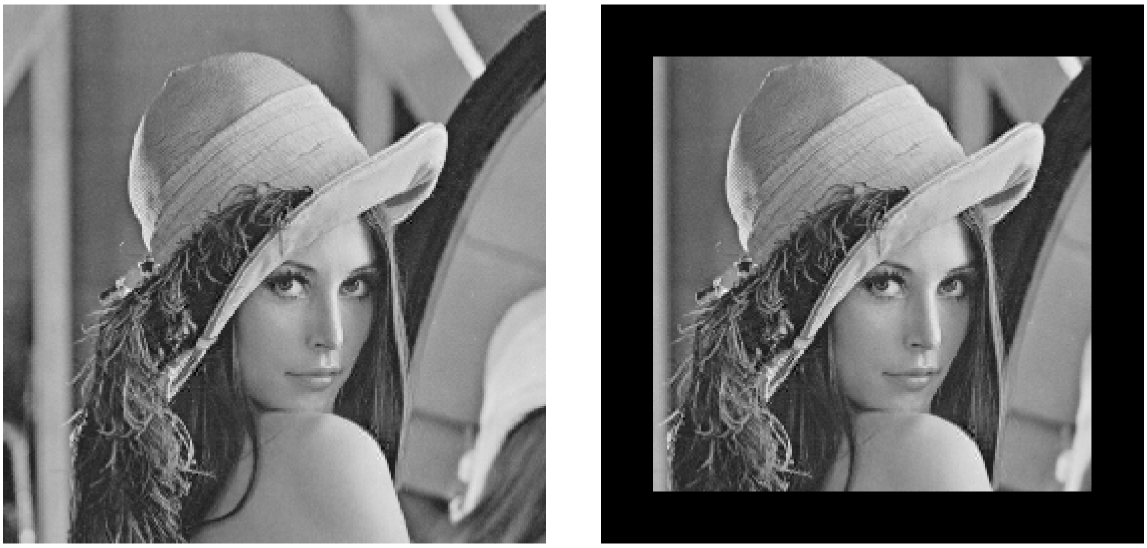
For these common attacks the presence of the watermark sequence can be easily detected from attacked images.

The gamma correction attack changes the brightness of pixels of the watermarked images by a specified factor $\gamma = \{0.8, 1.1, 1.2, 1.5\}$. In Table 2, the average of the values of q shows that the proposed scheme is robust against intensity modification of pixels.

The cropping attack consists of cutting a portion of the watermarked image from borders, preserving however its main features. We performed this attack by varying the size of the cropped portion of each watermarked image up to 30% and we could still detect the presence of the watermark sequence W with high confidence. A sample of the attack is shown in Figure 4. Notice that the robustness against cropping can be further increased by embedding redundantly the watermark into the cover image.

Regarding well known attacks such as rotation and translation, our algorithm cannot be considered sufficiently robust. Indeed, the values of q obtained during our tests for these attacks are smaller than the chosen threshold, besides being different from zero. As one of our aims was to minimize the false positive probability, we preferred not to lower the threshold, also considering the fact that the two previously cited attacks sensibly degrade the quality of the watermarked image. At this point a consideration deserves attention. It is not wrong to state that, in case of a dispute for determining image ownership, the "perfect looking" image has good chances to be considered as the "original" one [53]. This is unlikely to happen in case of rotated or excessively compressed images.

Figure 4. The cropping attack performed on the 512×512 “Lena” image: the watermarked image (left) and the same image with cropped border by 20% (right).



Besides signal processing operations and common attacks, we also executed comparative tests using a recently proposed watermarking scheme based on singular values [42] (Chung’s scheme). We focused on this scheme only because it is based on the modification of the singular vectors as our watermarking scheme. We did not consider suitable to include in the comparative analysis the following algorithms:

- the scheme proposed by Patra et al. [40] due to the lack of information regarding the quality of the watermarked image (i.e., PSNR) and the test performed to demonstrate the robustness of the scheme;
- the scheme proposed by Chang et al. [39], even if it is based on singular vectors, because of the detection problems analysed in various papers [29, 40, 41];
- the watermarking schemes based on singular values (SVs) since they are subject to the security and false positive problems, described in section 3. A discussion on the security of the watermarking schemes based on SVs is presented in Appendix C.

The implementation of Chung’s scheme is compliant with the idea presented in [42]. To correctly compare the methods we chose the parameters of the Chung’s scheme so that the quality of the watermarked images was approximately 38 dB. The chosen values were:

- the size of the test images equal to 512×512;
- a binary image of size 32×32 as watermark;
- the segmentation block size equal to 8×8;
- the threshold *th* set to 0.012;

The comparison test, presented in Table 3, was conducted by running both the embedding algorithms on 100 common images [58, 59] followed by the attacking and the extraction sessions. Given that both algorithms use different metrics for quantifying the detector response, we chose the percentage of the attacked images from which we were able to extract the watermark as a comparison factor. In Table 3, we refer to it as “Detection Ratio”.

The watermarking schemes were compared according to the essential requirements that must be satisfied by any marking system:

- **Quality of the watermarked image**. Our scheme produces a perceptually good watermarked image (PSNR≈38 dB) since it modifies the middle singular vectors in each block (i.e., the 6th and 7th right singular vectors). Differently from the Chung's scheme, which embeds the watermark into the first singular vector in each block, our method discards the first two couples of vectors to maintain the image quality as high as possible.
- **Robustness against attacks**. From Table 3, it can be observed that the Chung's method performs well against cropping and row and column blanking/copying. Instead, when other attacks are applied, the detection ratio considerably decreases as the scheme fails to extract the watermark from all attacked images. Moreover, the Chung's scheme has worse performance compared to ours when JPEG compression and noise addition are applied and doesn't resist to down-sampling and gamma correction attacks. In our opinion this behavior is due to the way the watermark is embedded into the cover image, i.e., the orthogonality property of the singular vectors is not maintained in the embedding process. On the contrary, preserving such a property allows our scheme to detect the watermark from all attacked images, except when JPEG compression with quality factor 60 is applied (but still having a detection ratio equal to 94%).

Table 3. Performance of our scheme compared to the Chung *et al*. [42] scheme.

Attack		**Factor**	**Detection Ratio**	
			Proposed	*Chung et al.*
Sampling	Down	0.7	100%	0%
		0.8	100%	0%
	Up	1.3	100%	100%
		1.75	100%	33%
JPEG Compression		QF = 90	100%	100%
		QF = 80	100%	86%
		QF = 70	100%	31%
		QF = 60	94%	11%
Additive White Gaussian Noise		1%	100%	93%
		2%	100%	21%
		3%	100%	5%
Salt & Pepper Noise		D = 0.001	100%	100%
		D = 0.003	100%	55%
		D = 0.005	100%	33%
Row-Column Copying		5-11	100%	97%
		35-78	100%	97%
		67-437	100%	96%
		3-16, 43-72	100%	91%
		139-126, 123-211	100%	91%
		333-164, 431-142	100%	92%
		14-26, 169-99, 119-192	100%	90%
		139-126, 123-211,43-72	100%	90%
		5-11, 35-78, 67-437	100%	92%

Table 3. *Cont.*

Row Column Blanking	5-11	100%	95%
	35-78	100%	95%
	67-437	100%	95%
	3-16, 43-72	100%	93%
	139-126, 123-211	100%	92%
	333-164, 431-142	100%	93%
	14-26, 169-99, 119-192	100%	90%
	139-126, 123-211,43-72	100%	94%
	5-9, 11-67, 437-500	100%	94%
Gamma Correction	γ = 0.6	100%	0%
	γ = 0.8	100%	0%
	γ = 1.1	100%	0%
	γ = 1.2	100%	0%
	γ = 1.5	100%	0%
Cropping	10%	100%	100%
	20%	100%	92%
	25%	100%	55%
	30%	100%	50%

- **Security**. The security property of our watermarking scheme is granted by the capability to choose one or more couples of vectors among a set of many possible candidates. In addition, a further improvement to security is assured by selecting any pair of components of the chosen singular vectors. Instead, we can not say that the algorithm proposed by Chung is secure because it always embeds the watermark by modifying the same components (2nd and 3rd) of the first singular vector.
- **Type of the watermark**. In our scheme, the watermark is a pseudo-random Gaussian sequence whereas in Chung's scheme it can be a significant watermark (i.e., binary or a gray-scale image). In general, it is better to use a significant mark in the watermarking process because of the possibility, in the detection step, to visually compare the original watermark with the inserted one [31].

Our method does not require the original image in the detection phase; however, we can improve the algorithm robustness by using the original image in the detection process. To test this approach, we modified the algorithm to perform a non-blind detection. Briefly, we used the original blocks to directly compute the angle difference in the singular vectors of the watermarked image, in order to extract the watermark and correlate it with the original one. In that case, we obtained a much higher detection rate, with an extremely small false positive probability. Therefore, even if the non-blind method cannot be used in some application contexts, such as copyright protection, we think that this variant of the algorithm could be used in other less demanding scenarios, e.g., image fingerprinting, due to its higher robustness.

7. Conclusions

The method presented in this paper was devised with the aim of creating a novel secure watermarking scheme for digital images based on the SVD transform. Our approach was influenced by the work by Craver et al. [14], which states that the original media is not required in the detection process for resolving legal ownerships. This disallows the usage of a non-blind watermarking method to attest the possession of the original digital image or, more generally, of a multimedia content.

The proposed scheme is based on singular vectors, therefore it does not suffer the majority of the problems related to SVD watermarking schemes which use the singular values in the embedding process. Moreover, our scheme preserves the orthogonality property of the singular vectors during the watermark embedding step, which permits a smooth detection of the watermark in case of no-attack.

Although our solution has been devised and tested using the right singular vectors, it can be applied to the left singular vectors as well (U matrix), or extended to use both right and left singular vectors. Indeed, enlarging the embedding space improves the security and provides the possibility to insert the watermark sequence redundantly. However, extra care must be taken in order not to degrade the quality of the watermarked image during the embedding process. This is one of our future research directions, with the aim of increasing the performance of the method with respect to robustness to attacks and further reduction of the false positive and false negative occurrence.

Given the interesting results presented, we are also going to test the application of the SVD (using singular vectors) to other type of media that in general require copyright protection.

Acknowledgements

The authors would like to thank Prof. Albert Werbrouck, Dr. Marco Milanesio and the anonymous reviewers for the precious comments and suggestions. During this research activity V. Pomponiu has been supported by the "*World Wide Style Mobility Project*" funded by the CRT Foundation.

Appendix A

The four quadrant arctangent function (i.e., arctan(y, x)) is a two-arguments function that computes the arctangent of y/x given y and x, but with a range of $(-\pi, \pi]$. Differently from the arctangent function with only one argument, the signs of both arguments allow to determine in which quadrant the point (x, y) lies and, consequently, the defined angle over the entire circle [61].

Appendix B

The objective is to make the projection of a vector v_i on a plane P(k, l) to form an angle α with the positive axis k. Moreover, the vector v_i forms, along with other vectors $v_1 \ldots v_{i-1}$ $v_{i+1} \ldots v_M$, an orthonormal base. The condition on v_i is obtained rotating it along with another vector v_j on the plane defined by them by an angle φ. Thus the target is to determine φ as a function of α.

Let's create the matrix A formed by the vectors v written in the rows.

$$A = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_M \end{bmatrix}. \tag{17}$$

For the orthonormality of the vectors, we have $A \cdot A^T = I,$ where I is the identity matrix.

Consider the matrix B

$$B = \begin{array}{c@{}l} \begin{bmatrix} 1 & \cdots & 0 & & \cdots & 0 & \cdots & 0 \\ 0 & \ddots & & & & & & \vdots \\ & & \cos\varphi & 0\cdots & \cdots 0 & -\sin\varphi & & 0 \\ \vdots & & & 1\ddots & & & & \vdots \\ & & & & \ddots 1 & & & 0 \\ 0 & \cdots & \sin\varphi & 0\cdots & \cdots 0 & \cos\varphi & & \\ & & & & & & 1\ddots & \\ 0 & & & 0 & & & & \ddots 1 \end{bmatrix} & \begin{matrix} \\ \\ \leftarrow i \\ \\ \\ \leftarrow j \\ \\ \\ \end{matrix} \\ \begin{matrix} \qquad\qquad i \qquad\qquad\qquad\qquad j \end{matrix} & \end{array} \tag{18}$$

which rotates the vectors v_i and v_j by an angle φ on their plane. The new vectors after the rotation are computed as:

$$C = BA = \begin{bmatrix} v_1 \\ \vdots \\ v_i \cos\varphi - v_j \sin\varphi \\ \vdots \\ v_i \sin\varphi + v_j \cos\varphi \\ \vdots \\ v_M \end{bmatrix}. \tag{19}$$

It is easy to see that $C \cdot C^T = I,$ i.e., the new vectors are still orthonormal.

Let's call v_{ki} and v_{li} the two components of vector v_i on the two axes k and l before the rotation. The angle formed by the projection of v_i with the positive axis k is:

$$\theta = \arctan(v_{li}, v_{ki}) \tag{20}$$

where arctan is the arctangent function over four quadrants.

After the rotation the two components of the vector v_i are:

- *l-th* component: $v_{li} \cos \varphi - v_{lj} \sin \varphi$
- *k-th* component: $v_{ki} \cos \varphi - v_{kj} \sin \varphi$

So:

$$\tan\alpha = \frac{\sin\alpha}{\cos\alpha} = \frac{v_{li}\cos\varphi - v_{lj}\sin\varphi}{v_{ki}\cos\varphi - v_{kj}\sin\varphi} \tag{21}$$

and some algebra leads to:

$$\tan\varphi = \frac{\sin\varphi}{\cos\varphi} = \frac{v_{ki}\sin\alpha - v_{li}\cos\alpha}{v_{kj}\sin\alpha - v_{lj}\cos\alpha} \ . \tag{22}$$

Appendix C

In this appendix we present the problem arising in SVD based watermarking schemes based on the watermarking of singular values only. Such schemes are vulnerable to the SVs substitution attack, i.e., the procedure of substituting SVs of an image with similar SVs derived from another image.

To better clarify this fact, let us consider two images represented by means of matrices *A* and *B*. Applying a *whole SVD transform* on both matrices by means of (2), we obtain:

$$\begin{aligned} SVD(A) &= \left[U_A S_A V_A\right] \\ SVD(B) &= \left[U_B S_B V_B\right] \end{aligned} \tag{23}$$

where U_A, U_B are the left singular vector matrices, V_A, V_B are the right singular vectors matrices and S_A, S_B are matrices containing on their diagonals the SVs of the *A* and *B* matrices. The S_A and S_B matrices have an interesting property: they are very similar, i.e., the SVs of matrix *A* are highly correlated with those of matrix *B*.

Then, exchanging S_A with S_B in (23), we obtain:

$$D = U_A \cdot S_B \cdot V_A^T \tag{24}$$

Finally, comparing matrix *A* with matrix *D*, we can notice that they are highly correlated and that the image *D* has a good visual quality. Analogously, we could repeat the reconstruction procedure in (24) with any image with similar SVs and we would obtain always the same result.

For example, let's take as the matrix *A* the well-known "Lena" image and as matrix *B* a randomly chosen image from a common image dataset [58]. They are both gray-scale images of size 512×512×8 bpp (Figure 5).

Next, we substitute the SVs of the *A* image with those of the *B* image. The resulting image *D* is presented in Figure 6. We can observe from this figure that the quality of the image *D* is high. Note that the same procedure may be applied to block based SVD producing the same results.

Given the above presented behavior of the SVD transform, we can identify two possible attack scenarios concerning SVs based watermarking schemes:

- when both images *A* and *B* are watermarked by different owners, the watermark in *A* may be completely substituted by the one in *B*, therefore changing the ownership of the image;
- when only image *A* is marked, the substitution of its SVs with those of an unmarked image *B* causes the watermark removal from *A*, and by consequence, a failure in proving the rightful ownership of *A*.

Many watermarking schemes which embed the watermark signal by modifying the SVs of the cover image have this problem, as has been demonstrated in various recent articles [15, 16, 31-35].

Figure 5. Sample images used in the test. On the left, the image *A* ("Lena"); on the right the image *B* (from dataset [58]).

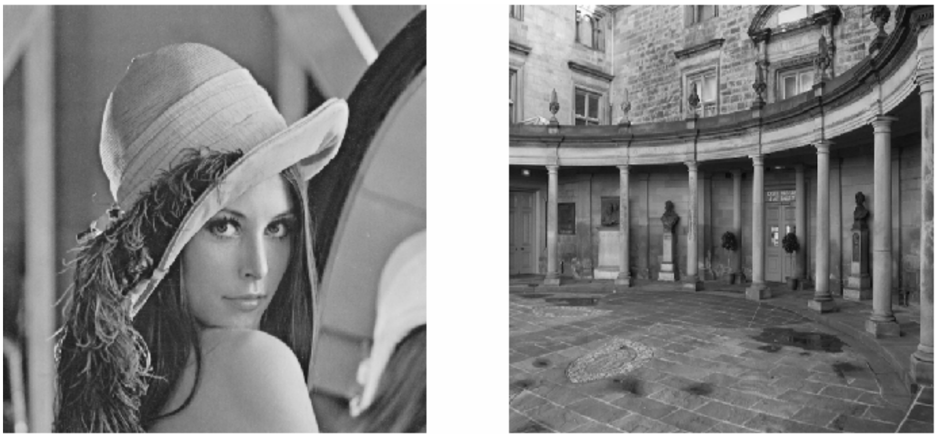
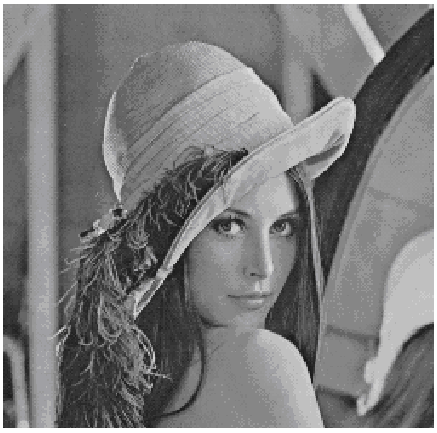


Figure 6. Resulting image by interchanging the SVs of the *A* image with those of the *B* image.



References

1. Seitz, J.; Jahnke, T. Digital Watermarking: An introduction. In *Digital Watermarking for Digital Media,* Information Science Publishing: Hershey, Pennsylvania, USA, 2005; pp. 19–20.
2. Johnson, N.F.; Katezenbeisser, S.C. A Survey of Steganographic Techniques. In *Information Techniques for Steganography and Digital Watermarking*, Katzenbeisser, S.C., Petitcolas, F.A.P. Eds., Artech House: Northwood, Massachusetts, USA, 1999; pp. 43–75.

3. Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F. A digital watermark. In *Proceedings of IEEE International Conference on Image Processing (ICIP'94)*, Austin Texas, USA, November 13-16, 1994; *2*, pp. 86–90.
4. Langelaar, G.; Setyawan, I.; Lagendijk, R.L. Watermarking Digital Image and Video Data. In *IEEE Signal Processing Magazine*, Piscataway, New Jersey, USA, September 2000; *17*, pp. 20-46.
5. Wollan, H. Digital Watermarking in Still Images. *Proceedings of the Computer Science Discipline Seminar Conference (CSCI 3901)*, University of Minnesota, Morris, Spring 2000, Available on http://cda.morris.umn.edu/~lopezdr/seminar/spring2000/wollan.pdf.
6. Podilchuk, C.; Zeng, W. Image-adaptive watermarking using visual models. *IEEE J. Sel. Are. Comm.* **1998**, *16*, pp. 525–539.
7. Cox, I.; Kilian, J.; Leighton, F. T.; Shamoon, T. Secure spread spectrum watermarking for multimedia, *In IEEE Transaction on Image Processing*, Piscataway, New Jersey, USA, December 1997; *6*, pp. 1673–1687.
8. Ruanaidh, J.J.K.; Dowling, W.J.; Boland, F.M. Phase watermarking of digital images. *Proceedings of the 1996 International Conference on Image Processing*, Lausanne, Switzerland, September 1996; *3*, pp. 239–242.
9. Dugad, R.; Ratakonda, K.; Ahuja, N. A new wavelet-based scheme for watermarking images. *International Conference on Image Processing Proceedings* (*ICIP 98)*, Chicago, USA, October 4-7, 1998; *2*, pp. 419–423.
10. Wolfgang, R. B.; Podilchuk, C. I.; Delp, E. J. Perceptual watermarks for digital images and video. *Proceedings of the IEEE*, Bellingham, USA, July 1999; *87*, pp. 1108–1126.
11. Bartolini, F.; Barni, M.; Cappellini, V.; Piva, A. Mask building for perceptually hiding frequency embedded watermarks. *Proceedings of the International Conference on Image Processing (ICIP 98)*, Chicago, Illinois, USA, 1998; *1*, pp. 450–454.
12. Lin, E.T.; Delp, E.J. A Review of Fragile Image Watermarks. *Proceedings of ACM Multimedia & Security Workshop*, Orlando, USA, October 1999; pp. 25–29.
13. Kutter M.; Hartung F. Introduction to watermarking techniques, *in Information Hiding Techniques for Steganography and Digital Watermarking,* Stefan Katzenbeisser, F.A.P. Petitcolas Eds.; Artech House: Nordwood, Massachusetts, USA, 2000; pp. 97–120.
14. Craver, S.; Memon, D. N.; Yeo, B.-L.; Minerva, M. M. Can invisible watermarks resolve rightful ownerships? *Proceedings of SPIE*, Bellingham, USA, 1997; *3022*, pp. 310–321.
15. Wu, H.-C.; Yeh, C.-P.; Tsai, C.-S. A Semi-fragile Watermarking Scheme Based on SVD and VQ Techniques. *Workshop on Applied Cryptography and Information Security (ACIS 2006), LNCS 3982*, Springer Berlin/Heidelberg, Germany, 2006; pp. 406–415.
16. Ling, H.-C.; Phan C.-W.; Heng, S.-H. Attacks on SVD-Based Watermarking Schemes. *Proceedings of ISI 2008 Workshop, Taipei, Taiwan, LNCS 5075*, Springer Berlin/Heidelberg, Germany, June 2008; pp. 83–91.
17. Yang, J.-F.; Lu, C.-L. Combined Techniques of Singular Value Decomposition and Vector Quantization for Image Coding. *IEEE Transaction on Image Processing*, Piscataway, New Jersey, USA, August 1995; *4*, pp. 1141–1146.
18. Andrews, H.C.; Patterson, C.L. Singular Value Decomposition (SVD) Image Coding. *IEEE Transactions on Communications*, Piscataway, New Jersey, USA, April 1976; pp. 425–432.

19. Shnayderman, A.; Gusev, A.; Eskicioglu, A. A Multidimensional Image Quality Measure Using Singular Value Decomposition. *Proceedings of the SPIE Image Quality and System Performance Conference*, San Jose, California, USA, January 19-20, 2004; *5294*, pp. 82–92.
20. Gorodetski, V.I.; Popyack, L.J.; Samoilov, V. SVD-Based Approach to Transparent Embedding Data into Digital Images. *Proceedings of International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS01)*, St. Petersburg, Russia, 2001; pp. 263–274.
21. Calagna, M.; Guo, H.; Mancini, L.V.; Jajodia, S. Robust Watermarking System based on SVD Compression. *Proceedings of the 2006 ACM Symposium on Applied Computing*, Dijon, France, April 23 -27, 2006; pp. 1341–1347.
22. Liu, J.; Niu, X.; Kong, W. Image watermarking scheme based on singular value decomposition. *International Conference on Intelligent Information Hiding and Multimedia*, Pasadena, California, USA, December 2006; pp. 457-460.
23. Liu, R.; Tan, T. A new SVD based Image Watermarking method. *IEEE Transactions on Multimedia*, Piscataway, New Jersey, USA, March 2002; *4*, pp. 121–128,
24. Ganic, E.; Zubair, N.; Eskicioglu, A. M. An Optimal Watermarking Scheme Based on Singular Value Decomposition. *Proceedings of the IASTED International Conference on Communication, Network, and Information Security (CNIS 2003)*, Uniondale, New York, USA, December 10-12, 2003, pp. 85-90.
25. Chandra, D. Digital image watermarking using singular value decomposition. *Proceedings of the IEEE 45th Midwest Symposium on Circuits and Systems*, Oklahoma State University, USA, August 4-7, 2002**;** *3*, pp. 264–267.
26. Shieh, J.-M.; Lou, D.-C.; Chang, M.-C. A semi-blind digital watermarking scheme based on singular value decomposition. *Computer Standards & Interfaces*, Elsevier, April 2006; *28*, pp. 428–440.
27. Chang, C.-C.; Hu, Y.-S.; Lin, C.-C. A Digital watermarking scheme based on singular value decomposition. *Proceedings of the International Symposium on Combinatory, Algorithms, Probabilistic and Experimental Methodologies Hangzhou, China*, *LNCS 4614*, Springer Berlin/Heidelberg, Germany, September 2007; pp. 82–93.
28. Chang, C.-C.; Lin, C.-C.; Hu, Y.-S. An SVD oriented watermark embedding scheme with high qualities for the restored images. *International Journal of Innovative Computing, Information and Control (IJICIC)*, Toroku, Kumamoto, Japan, June 2007; *3*, pp. 609–620.
29. Mohan, B.C.; Srinivaskumar, S.; Chatterji, B.N. A Robust Digital Image Watermarking Scheme using Singular Value Decomposition (SVD), Dither Quantization and Edge Detection. *ICGST-GVIP J.* **2008**, *8*, pp. 17–23.
30. Rezazadeh, S.; Yazdi, M. A Nonoblivious Image Watermarking System Based on Singular Value Decomposition and Texture Segmentation. *Proceedings of the World Academy of Science, Engineering and Technology*, Budapest, Hungary, May 26-28, 2006; *13*, pp. 255–259.
31. Mohammad, A.A.; Alhaj, A.; Shaltaf, S. An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Processing*, Elsevier North-Holland: Amsterdam, The Netherlands, September 2008; *88*, pp. 2158–2180.

32. Ting, G.C.-W. Ambiguity Attacks on the Ganic-Eskicioglu Robust DWT-SVD Image Watermarking Scheme. *Proceedings of Information Security and Cryptology (ICISC 2005), Seoul, Korea, LNCS 3935*, Springer Berlin/Heidelberg, Germany, 2006; pp. 378–389.
33. Wu, Y. On the Security of an SVD-Based Ownership Watermarking. *IEEE Transactions On Multimedia*, Piscataway, New Jersey, USA, August 2005; *7*, pp. 624–627.
34. Zhang, X.-P.; Li, K. Comments on An SVD-Based watermarking scheme for protecting rightful Ownership. *IEEE Trans. Multimed.* **2005**, *7*, 593–594.
35. Yavuz, E.; Telatar, Z. SVD Adapted DCT Domain DC Sub-band Image Watermarking Against Watermark Ambiguity. *Proceedings of International Workshop on Multimedia Content Representation, Classification and Security (IW-MRCS2006). LNCS 4105*, Istanbul, Turkey, 2006; pp. 66–73
36. Cox, I.J.; Miller, M.L.; Bloom, J.A. *Digital Watermarking.* Morgan Kaufmann Publishers Inc.: San Francisco, USA, 2001.
37. Craver, S.; Memon, D.N.; Yeo, B.-L.; Yeung, M.M. Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications. *IEEE Journal on Selected Areas in Communications*, California, USA, May 1998; *16*, pp. 573–586.
38. Ghazy, R.; El-Fishawy, N.; Hadhoud, M.; Dessouky M.; El-Samie, F. An efficient block-by block SVD-based image watermarking scheme. *Proceedings of the 24th National Radio Science Conference*, Cairo, Egypt, March 2007; pp. 1–9.
39. Chang, C.-C.; Tsai, P.; Lin, C.-C. SVD-based Digital Image Watermarking scheme. *Pattern Recognition Letters*, Elsevier, 2005; *26*, pp. 1577–1586.
40. Patra, J.C.; Soh, W.; Ang, E.L.; Meher, P.K. An Improved SVD-Based Watermarking Technique for Image and Document Authentication. *Circuits and Systems* (*APCCAS 2006)*, IEEE Asia Pacific, Singapore, December 4-7, 2006; pp. 1984–1987.
41. Mohan, B.C.; Kumar, S. A Robust Digital Image Watermarking Scheme using Singular Value Decomposition. *J. Multimed.* **2008**, *3*, 7–15.
42. Chung, K.-L.; Yang, W.-N.; Huang, Y.-H.; Wu, S.-T.; Hsu, Y.-C. On SVD-based watermarking algorithm. *Appl. Math. Comput.* **2007**, *8*, 54–57.
43. Sverdlov, A.; Dexter, S.; Eskicioglu, A. M. Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies. *Proceedings of 13th European Signal Processing Conference (EUSIPCO2005)*, Antalya, Turkey, September 2005; pp. 4–8.
44. Tsai, C.-F.; Yang, W.-Y. Real-Time Color Image Watermarking Based on D-SVD Scheme. *Advances in Image and Video Technology*, *LNCS 4872*, Springer Berlin/Heidelberg, Germany, December 2007; pp. 289–297.
45. Liu, F.; Liu, Y.A watermarking Algorithm for Digital Image based on DCT and SVD. *IEEE Congress on Image and Signal Processing*, Sanya, Hainan, China, May 27-30, 2008; *1*, pp. 380–383.
46. Ganic, E.; Eskicioglu, A.M. Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies. *Proceedings of the ACM Multimedia and Security workshop*, Magdeburg, Germany, September 20-21, 2004; pp. 167–174.

47. Lin, C.-H.; Liu, J.-C.; Han, P.-C. On the Security of the Full-Band Image Watermark for Copyright Protection. *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, Taiwan, June 11-13, 2008; pp. 74–80.
48. Li, H.; Wang, S.; Song, W.; Wen, Q. A Novel Watermarking Algorithm Based on SVD and Zernike Moments. *LNCS 3495*, Springer Berlin/Heidelberg, Germany, 2005; pp. 448–453.
49. Tang, X.; Yang, L.; Li, L.; Niu, Y. Study on a Multifunctional watermarking Algorithm. *In Proceedings of IEEE ICSP'2004*, Istanbul, Turkey, 2004; *1*, pp. 848–852.
50. Sugiyama, M.; Goto, M.; Kovács, S.; Matsumoto, T.; Naoi, T. A cropping-robust watermarking method based on singular value decomposition and Haar transformation. *Syst. Comp. Japan* **2003**, *34*, pp. 38–47.
51. Byun, S.-C.; Lee, S.-K.; Tewfik, A. H.; Ahn, B.-H. A SVD-Based Fragile Watermarking Scheme for Image Authentication, *Proceedings of First International Workshop (IWDW 2002), Seoul, Korea, LNCS 2613*, Springer Berlin/Heidelberg, Germany, 2003; pp. 375–391.
52. Sun, R.; Sun, H.; Yao, T. A SVD and quantization based semi-fragile watermarking technique for image authentication. *Proceedings of the 6th International Conference on Signal Processing (ICSP'02)*, Rochester, USA, 2002; *2*, pp. 1592–1595.
53. Zeng, W.; Liu, B. A statistical watermark detection technique without using original images for resolving rightful ownership of digital images. In *IEEE Transactions on Image Processing,* Piscataway, New Jersey, USA, November 1999; *8*, pp. 1534–1548.
54. Stathaki, T.; Dafas, P. Digital Image Watermarking Using Block-Based Karhunen-Loeve Transform. In *Proceedings of the 3rd International Symposium (ISPA)*, Rome, Italy, September 18-20, 2003; *2*, pp. 1072–1075.
55. Anderson, E.; Bai, Z.; Bischof, C.; Blackford, S.; Demmel, J.; Dongarra, J.; Croz, D.J.; Greenbaum, A.; Hammarling, S.; Mckenney, A.; Sorensen, D. *LAPACK User's Guide, third edition*. SIAM: Philadelphia*,* Philadelphia, USA, 1999.
56. Bro, R.; Acar, E.; Kolda, T.G. Resolving the sign ambiguity in the singular value decomposition. *J. Chemometr.* **2008**, *22*, pp. 135–140.
57. Lu, C.-S. *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*; Idea Group Publishing (an imprint of Idea Group Inc.): Hershey, Pennsylvania, USA, 2005; Chapter 2.
58. Li, L.-J.; Wang, G.; Li, F.-F. OPTIMOL: automatic Object Picture collecTion via Incremental MOdel Learning. In *IEEE Computer Vision and Pattern Recognition (CVPR)*, Minneapolis, USA, 2007; pp. 1–8.
59. Schaefer, G.; Stich, M. UCID - An Uncompressed Colour Image Database. In *Proceedings of SPIE*, *Storage and Retrieval Methods and Applications for Multimedia*, San Jose, USA, 2004; *5307*, pp. 472–480.
60. Schlauweg, M.; Pröfrock, D.; Zeibich, B.; Müller, E. Dual watermarking for protection of rightful ownership and secure image authentication. In *Proceedings of the 4th ACM international workshop on Contents protection and security*, Santa Barbara, California, USA, 2006; pp. 56–66.
61. *Wolfram Mathematica*. Wolfram Research Inc. Web Resource: http://reference.wolfram.com/mathematica/ref/ArcTan.html, 2008.