An enhanced semi-blind DWT–SVD-based watermarking technique for digital images

A Sleit*, S Abusharkh, R Etoom and Y Khero
Department of Computer Science, King Abdulla II School for Information Technology, University of Jordan, PO Box 13838, Amman 11942, Jordan

Abstract: This paper presents a semi-blind hybrid watermarking technique based on singular value decomposition (SVD) and discrete wavelet transformation (DWT). The proposed technique decomposes the host image using DWT and combines the singular values (SVs) of the watermark and the selected sub-bands. A binary watermark is used to be embedded in the grey-scale original image. This watermark image passes through multiple operations before embedding. The watermark is converted into a vector, which is permuted into scrambled data by using a key as the initial random seed of this process. Experimental results show that the proposed technique is able to resist a variety of attacks.

Keywords: digital watermarking, discrete wavelet transform, singular value decomposition, Haar wavelet, digital rights management system

1 INTRODUCTION

Digital watermarking is typically used by the digital rights management system, which is responsible for describing, identifying, trading, protecting, monitoring and tracking the intellectual property rights of digital multimedia content. Increasingly, digital contents are distributed over the internet causing digital watermarking to become more critical. Watermarking is a descendent of a technique known as steganography, where a secret message is hidden in another message and then sent to other party. However, digital watermarking is the process of embedding low-energy signal (called the watermark) in another signal (called the cover). The watermark usually contains some metadata about the main signal, like security or ownership information.

Digital watermarking schema consists of two main processes, namely, watermark embedding and extraction, where a public or secret key is used. A good image watermarking technique must observe the following two conflicting requirements.

- robustness: the watermark image must be robust against any alteration or modification
- transparency: the resulting watermarked image should be visually conventional and perceptually invisible.

Watermarking techniques are classified into various classes depending on various attributes. Based on the extraction process, watermarking techniques can be blind, semi-blind and non-blind. Non-blind techniques use the original image and secret key(s) to extract the watermark. Semi-blind techniques sometimes use part of the original image and demand the presence of both the watermark bit sequence and the secret key(s). Blind watermarking techniques, however, require only the secret key(s) for extraction.

Watermarking techniques can be applied on either the spatial or frequency domain of the cover. Spatial domain watermarking techniques embed the signal directly into the cover. In case of images, the pixel values or statistical traits are directly modified. Frequency domain-based techniques apply transforms such as the discrete cosine transform.
(DCT),\(^9,10\) discrete wavelet transform (DWT)\(^1,11,12\) or singular value decomposition (SVD)\(^13,14\) on the cover. Subsequently, the coefficient values of the selected transform are modified to store the watermark in the cover. Researchers have proposed watermarking techniques based on a combination of DWT and SVD.\(^15\)–\(^19\)

Barni et al.\(^9\) proposed a watermarking algorithm which operates in the wavelet domain. It depends on the characteristics of the human visual system, where masking is accomplished pixel by pixel by taking into account the texture and luminance contents of all the image sub-bands. The watermark consists of a pseudorandom sequence which is adaptively added to the largest detail bands of the hosting image. SVD method can be applied on the watermark only, the host image only, or on both. Liu and Tan\(^13\) proposed a scheme that inserts the watermark into the S matrix obtained from the SVD of the image alone to protect the ownership rights.

Ganic and Eskicioglu\(^15\) proposed a watermark scheme in which the wavelet transform of the host image is obtained, and then SVD is applied on all decomposed sub-bands. The watermark is embedded by summing up the singular values (SVs) of the watermark and host images. Bhatnagar and Raman\(^16\) introduced a semi-blind watermarking scheme, where embedding is performed by modifying the SVs of the cover image with the SVs of the watermark image. After decomposing the original image using DWT, a reference image is formed based on directive contrast. Monemizadeh and Seyedin\(^17\) proposed the Pareto-based multi-objective evolutionary algorithm in combination with traditional DWT–SVD watermarking.

Kim et al.\(^18\) presented a technique for embedding the watermark into selected sub-bands after applying DWT, which is accomplished by modifying the log-scale SV. The technique is considered blind image watermarking since only the key is used in the extraction phase. A single step of DWT is applied on the original image, and then the SVD of each sub-band is computed followed by calculating the log scale. Wang and Chen\(^19\) proposed a hybrid scheme depending on \(k\)-means clustering and visual cryptograph. \(k\)-means clustering is used to classify the extracted features of the host image after applying the DWT and the SVD. The resulting master share of clustering is combined with a secret image to construct an ownership share according to visual cryptograph.

This article proposes a semi-blind and invisible watermarking technique, which embeds a binary watermark in a grey-scale image. The proposed technique applies DWT and SVD on both the original and watermark images such that there is no need to save the original image. Instead, a predefined sub-band is used as input in the extraction process. This paper is organised as follows. Section 2 reviews the DWT and SVD. Next, Section 3 explains the proposed watermarking technique. Then, Section 4 discusses experimental results and demonstrates the merits of the proposed technique. Finally, Section 5 concludes the paper with a summary.

2 BACKGROUND

The DWT is computed by successive low- and high-pass filtering of the discrete time-domain signal. At each level, the high-pass filter produces detailed information, while the low-pass filter associated with scaling function produces coarse approximations. The half-band filters produce signals spanning only half the frequency band. Thus, while the half-band low-pass filtering removes half of the frequencies and halves the resolution, the decimation by 2 doubles the scale. The time resolution becomes arbitrarily good at high frequencies, while the frequency resolution becomes arbitrarily good at low frequencies. The filtering and decimation process is continued until the desired level is reached. The maximum number of levels depends on the length of the signal. The Haar wavelet is based on DWT and is used to decompose the input original image into four bands. It consists of two basic processes, horizontal and vertical.\(^20\)

The vertical process consists of two basic steps. First, it separates the original image into two equal blocks horizontally. Second, it adds and subtracts the corresponding pixels of the two sub-blocks, and replaces the pixels of the left sub-block with the result of the corresponding pixels summation and those of the right sub-block with the result of the pixels difference.

The horizontal process consists of two steps. First, it separates the vertically processed image along into two equal upper and lower sub-blocks. Second, it adds and subtracts the corresponding pixels of the two sub-blocks and replaces the pixels of the upper sub-block with the summations of the corresponding pixels and those of the lower sub-block with their
The SVD of a matrix is an orthogonal transform which decomposes the given matrix into three matrices of the same size. Let an image be represented as matrix $A$. The SVD of matrix $A$ is given by

$$ A = U S V^T $$

$U$ and $V$ are unitary matrices such that $UU^T = I$ and $VV^T = I$, where $I$ is the identity matrix. The $U$ matrix is called the left SVs and the $V$ matrix is called the right SVs. $S$ is the diagonal matrix which has in its main diagonal all positive SVs of $A$. These positive SVs can be used to embed the watermark. The entries of $S$ are called the SVs, and they are the largest values of all the elements compared to $U$ and $V$. $S$ can be written as

$$ S = (\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n) $$

where $\lambda_1 \geq \lambda_2 \geq \lambda_3 \ldots \geq \lambda_n$, and $n$ is the rank of the matrix. Then

$$ \text{SVD}(A) = \lambda_1 U_1 V_1^T + \lambda_2 U_2 V_2^T + \cdots + \lambda_n U_n V_n^T $$

Matrix $A$ can be reconstructed by using equation (1). SVs are used in the watermark embedding process due to two main properties. The SVs of an image are considered stable since minor modifications of the image slightly affect its SVs. Moreover, SVD is able to efficiently represent the essential algebraic properties of an image, where SVs correspond to the brightness of the image and singular vectors reflect the geometric characteristics of the image.\textsuperscript{21} Figure 3 illustrates a typical SVD-based watermarking technique.\textsuperscript{13}

3 PROPOSED WATERMARKING TECHNIQUE

In this section, we discuss in detail the design of our approach of image watermarking. During the embedding process, the proposed technique decomposes the host image using DWT that uses the Haar wavelet filter. Then, it combines the SVs of the watermark and selected sub-bands. The image can be reconstructed by applying the inverse discrete wavelet transform (IDWT).

3.1 Watermark embedding process

The original image is transformed into wavelet domain by applying a multi-DWT. Based on the size of the image and the watermark, the number of decomposition levels is determined. If $L$ is the number of levels, then $2L+2$ of sub-bands are generated. In our proposed embedding process, we use five-level DWT decomposition.

The challenge is to decide which sub-bands to use to embed the watermark. It is known that the human visual system is more sensitive to small perturbation in the lower-frequency bands than the higher ones. Therefore, keeping intact the low frequencies assures that the watermarked image will be as close as possible to the original one. Moreover, it is known that lossy compression schemes eliminate high-frequency components.

In order to meet the transparency and robustness requirements, the lower-frequency band is chosen for the one-level DWT. Therefore, successive wavelet decompositions use the higher-frequency bands. The SVs of the resulting four sub-bands of the last decomposition of HH4 are computed. Figure 4 shows the block diagram of the embedding process of our scheme.

The watermark image is a binary watermark sequence: $w(i) \in \{-1, +1\}$. These binary images do not require much storage. It is obvious from Fig. 3 that the watermark image passes through different operations as it may be resized depending on the decomposition level. The coefficients of wavelet transform are real numbers. Therefore, rotation is used to convert the watermark image into real-numbers. The resulting vector is permuted into scrambled data by using a key as the initial random seed of this process.
The scrambled real-numbers of the watermark vector is converted into an \( n \times n \) image. Then, the SVD operation is applied on the resulting processed watermark image to compute its SVs. Next, the combination of the SVs of both the watermark and the predefined four sub-bands is calculated. The watermarked image is reconstructed using the IDWT function. The watermark embedding algorithm is outlined as follows.

**Algorithm: Watermark-Embedding**

**Input:** Original Image, Watermark Image  
**Output:** Watermarked Image

1. Apply DWT on the original image to produce four sub-bands.
2. The low-pass band \{LL1\} can be further decomposed to obtain another level of decomposition.
3. Repeatedly, apply DWT of the HH sub-bands till fifth level.
4. Compute SVD of each sub-bands \{LL5, HL5, LH5, HH5\}
   \[
   \begin{bmatrix}
   U_{org}^k & v_{org}^k & V_{org}^{kT}
   \end{bmatrix} = \text{SVD}(I^k), \quad k = 1, 2, 3, 4
   \]
5. The watermark is permuted into scrambled real vector.
6. Apply SVD on the processed watermark image.
   \[
   \begin{bmatrix}
   U_w & S_w & V_w^T
   \end{bmatrix} = \text{SVD}(W), \quad k = 1, 2, 3, 4
   \]
7. Combine the SVs of watermark image and SVs of the four sub-bands

\[ S_{\text{wkd}}^k = S_{\text{org}}^k + \omega S_W, \quad k = 1, 2, 3, 4 \]

8. Obtain the modified coefficients of the sub-bands.

\[ I_m^k = \text{iSVD} \left( U_{\text{org}}^k S_{\text{wkd}}^k V_{\text{org}}^k \right), \quad k = 1, 2, 3, 4 \]

9. Compute the watermark image by applying the inverse DWT.

End Algorithm

3.2 Watermark extraction process

The extraction process is the reverse of embedding as demonstrated in Fig. 5. It can be observed from the watermark permutation process that it prevents tampering or unauthorised access by attackers since only the owner of the image has the value of the key which is a necessary operand in the extraction operation. The watermark extraction algorithm is outlined as follows.

**Algorithm: Watermark-Extraction**

**Input:** Watermarked image, selected sub-band, Watermark vector

**Output:** Extracted watermark

**Procedure:** Extracting

1. Decompose the watermarked (possibly distorted) image, using DWT for five levels.
2. Compute SVD of each sub-band of the last decomposition.
3. Calculate the possible SVs of watermark image.
4. Apply SVD on the 4 sub-bands.
5. Compute the new coefficients of the 5th level sub-band.
6. Obtain the modified coefficients of the sub-bands.
7. Combine the SVs of watermark image and SVs of the four sub-bands.
8. Compute the watermark image by applying the inverse DWT.

6. 128 x 128 watermark image
3. Apply DWT on the original selected sub-band \{HH4\}.
4. Apply SVD on each sub-band resulted from the previous step.
   \[ U_{\text{wkd}}^k V_{\text{wkd}}^k = \text{SVD}(i_m^k), k = 1, 2, 3, 4 \]
5. Compute the possible values of SVs of the watermark image.
   \[ S_W = \left( S_{\text{wkd}}^k - S_{\text{org}}^k \right) / \delta, k = 1, 2, 3, 4 \]
6. Find the average of the calculated SVs of the previous step.
7. Approximate the watermark image.
8. Descramble the extracted watermark vector.
9. Compute the extracted watermark.

**End Watermark-Extraction**

### 4 EXPERIMENTAL RESULTS

Our experiments were executed on IBM Core 2 Duo 2.00 GHz processors with 4 GB RAM using MATLAB 7.0 platform. We used a binary watermark image of size 128 × 128 as shown in Fig. 6, and 512 × 512 grey-scale images for Lena, Barbara and Baboon as shown in Fig. 7.

We used two evaluation criteria to judge the transparency and robustness of the proposed algorithm; namely, the peak signal-to-noise ratio (PSNR), and correlation. The quality of the resulting watermarked images is measured by PSNR using the mean square error (MSE) as follows

\[
\text{PSNR} = 10 \times \log_{10} \left( \frac{255^2}{\text{MSE}} \right) 
\]

\[
\text{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| W(i,j) - W'(i,j) \right|^2
\]

where \( W \) is the original watermark, \( W' \) is the extracted watermark, and \( N \) and \( M \) are the width and height of the watermark. The PSNR value is used as a measurement of the image degradation due to imbedding the watermark in the cover image. Figure 8 illustrates the watermarked images of Fig. 7 with their PSNR values. It is difficult to notice the difference between cover images and their corresponding watermarked images, which reveals

![Watermarked images](image.png)

7 512 × 512 test images: (a) Lena; (b) Barbara; (c) Baboon

8 Watermarked images: (a) Lena, PSNR=55.6; (b) Barbara, PSNR=47.9016; (c) Baboon, PSNR=45.1308
Table 1  Experimental results of the of common image processing attacks

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Rotation (50°)</th>
<th>Salt and Pepper noise</th>
<th>Gaussian noise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacked Image</td>
<td><img src="image1" alt="Image" /></td>
<td><img src="image2" alt="Image" /></td>
<td><img src="image3" alt="Image" /></td>
</tr>
<tr>
<td>Extracted watermark</td>
<td><img src="image4" alt="Image" /></td>
<td><img src="image5" alt="Image" /></td>
<td><img src="image6" alt="Image" /></td>
</tr>
<tr>
<td>PSNR</td>
<td>22.9829</td>
<td>20.79</td>
<td>14.8013</td>
</tr>
<tr>
<td>Correlation</td>
<td>0.8768</td>
<td>0.8309</td>
<td>0.8178</td>
</tr>
<tr>
<td>Attacks</td>
<td>JPEG compression (Q=10%)</td>
<td>JPEG compression (Q=20%)</td>
<td>JPEG compression (Q=50%)</td>
</tr>
<tr>
<td>Attacked image</td>
<td><img src="image7" alt="Image" /></td>
<td><img src="image8" alt="Image" /></td>
<td><img src="image9" alt="Image" /></td>
</tr>
<tr>
<td>Extracted watermark</td>
<td><img src="image10" alt="Image" /></td>
<td><img src="image11" alt="Image" /></td>
<td><img src="image12" alt="Image" /></td>
</tr>
<tr>
<td>PSNR</td>
<td>34.2789</td>
<td>37.5883</td>
<td>43.5585</td>
</tr>
<tr>
<td>Correlation</td>
<td>0.8243</td>
<td>0.8019</td>
<td>0.8626</td>
</tr>
<tr>
<td>Attacks</td>
<td>Smoothing/weighted filter</td>
<td>Median filter/5 x 5 mask</td>
<td>Sharpening/Laplacian filter</td>
</tr>
<tr>
<td>Attacked image</td>
<td><img src="image13" alt="Image" /></td>
<td><img src="image14" alt="Image" /></td>
<td><img src="image15" alt="Image" /></td>
</tr>
<tr>
<td>Extracted watermark</td>
<td><img src="image16" alt="Image" /></td>
<td><img src="image17" alt="Image" /></td>
<td><img src="image18" alt="Image" /></td>
</tr>
<tr>
<td>PSNR</td>
<td>41.0976</td>
<td>36.8340</td>
<td>26.8900</td>
</tr>
<tr>
<td>Correlation</td>
<td>0.8626</td>
<td>0.9123</td>
<td>0.7984</td>
</tr>
</tbody>
</table>
the good visual quality obtained by the proposed embedding algorithm.

Correlation is the second evaluation criterion used in the extraction process to verify the presence of the watermark in the cover image, and to evaluate the degree of similarity between the extracted and original watermarks. The correlation coefficient is defined as follows

\[
\text{Corr} = \frac{W W^*}{(W W^*)^{1/2}} = \frac{\sum_{i=2}^{M} \sum_{j=2}^{N} W_{ij} W_{ij}^*}{\left[ \sum_{i=2}^{M} \sum_{j=2}^{N} W_{ij}^2 \sum_{i=2}^{M} \sum_{j=2}^{N} (W_{ij}^*)^2 \right]^{1/2}}
\]

(4)

where \( W \) and \( W^* \) are the original and extracted watermarks of size \( N \times M \), respectively.

The robustness of the proposed DWT–SVD-based watermarking scheme was tested using different attacks, including Gaussian noise, JPEG compression, sharpening, rotation, blurring, median filter and rotation. Table 1 summarises the PSNR and correlation values under the various attacks on the Lena image mentioned below:

- image rotation by 50°
- JPEG compression using three different values of compression quality (\( Q = 10\%, 20\% \) and 50%)
- Salt and Pepper noise with default noise density equals to 0.05
- Gaussian noise with zero mean and 0.1 variance
- smoothing using the average filter
- smoothing using weighted filter
- Laplacian sharpening.

As shown in Table 1, the proposed scheme is robust to the abovementioned image processing attacks. The correlation values of the extracted watermarks after the attacks represent the quality factors. Note that the quality factor for images is an integer value ranging from 0 to 1, which denotes the predetermined image quality. The larger the quality factor is assigned, the better visual quality the attacked image retains. Table 1 also illustrates the watermarked images, together with their PNSR values. It reveals that good

### Table 2 PSNR values of proposed scheme under various attacks

<table>
<thead>
<tr>
<th>Attack</th>
<th>Our DWT–SVD Scheme</th>
<th>Barbara</th>
<th>Baboon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotation (50°)</td>
<td>22.9829</td>
<td>18.8387</td>
<td>16.4006</td>
</tr>
<tr>
<td>Compression (10%)</td>
<td>34.2789</td>
<td>26.9227</td>
<td>37.4593</td>
</tr>
<tr>
<td>Compression (20%)</td>
<td>37.2789</td>
<td>29.7664</td>
<td>27.5536</td>
</tr>
<tr>
<td>Compression (50%)</td>
<td>43.5585</td>
<td>37.4593</td>
<td>37.0205</td>
</tr>
<tr>
<td>Salt and Pepper noise</td>
<td>20.79</td>
<td>20.7430</td>
<td>20.7099</td>
</tr>
<tr>
<td>Gaussian noise</td>
<td>14.8013</td>
<td>14.7782</td>
<td>14.7871</td>
</tr>
<tr>
<td>3 × 3 median filter</td>
<td>42.1034</td>
<td>24.2228</td>
<td>24.5107</td>
</tr>
<tr>
<td>5 × 5 median filter</td>
<td>36.8340</td>
<td>22.303</td>
<td>22.1605</td>
</tr>
<tr>
<td>Average filter</td>
<td>38.9281</td>
<td>24.4969</td>
<td>23.8768</td>
</tr>
<tr>
<td>Weighted filter</td>
<td>41.0976</td>
<td>26.5318</td>
<td>25.9688</td>
</tr>
<tr>
<td>Laplacian filter</td>
<td>26.8900</td>
<td>19.1202</td>
<td>18.946</td>
</tr>
</tbody>
</table>

### Table 3 Correlation results of three watermarking schemes under various attacks

<table>
<thead>
<tr>
<th>Attack</th>
<th>Our DWT–SVD scheme</th>
<th>SVD scheme (^\text{13})</th>
<th>DWT–SVD scheme (^\text{15})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>Lena</td>
<td>Barbara</td>
<td>Baboon</td>
</tr>
<tr>
<td>Rotation (50°)</td>
<td>0.8768</td>
<td>0.8037</td>
<td>0.7981</td>
</tr>
<tr>
<td>Compression (10%)</td>
<td>0.8243</td>
<td>0.8768</td>
<td>0.8697</td>
</tr>
<tr>
<td>Compression (50%)</td>
<td>0.8626</td>
<td>0.8487</td>
<td>0.8697</td>
</tr>
<tr>
<td>Salt and Pepper noise</td>
<td>0.8309</td>
<td>0.8268</td>
<td>0.8065</td>
</tr>
<tr>
<td>Gaussian noise</td>
<td>0.8178</td>
<td>0.8132</td>
<td>0.8041</td>
</tr>
<tr>
<td>3 × 3 Median filter</td>
<td>0.8626</td>
<td>0.8556</td>
<td>0.8375</td>
</tr>
<tr>
<td>5 × 5 median filter</td>
<td>0.9123</td>
<td>0.6848</td>
<td>0.8200</td>
</tr>
<tr>
<td>Average filter</td>
<td>0.8839</td>
<td>0.8717</td>
<td>0.8786</td>
</tr>
<tr>
<td>Weighted filter</td>
<td>0.8626</td>
<td>0.851</td>
<td>0.7357</td>
</tr>
<tr>
<td>Laplacian filter</td>
<td>0.7984</td>
<td>0.7921</td>
<td>0.8442</td>
</tr>
</tbody>
</table>
visual quality of watermarked images can be obtained by the proposed scheme. Moreover, Table 1 shows the watermarks retrieved from the marked images after the attacks. The extracted watermarks can be easily recognised by the human eyes. Table 2 shows the PSNR values obtained for the above attacks on the three images of Fig. 7. These experimental results illustrate that the robustness and transparency objectives are achieved by the proposed scheme.

For performance comparison, we implemented another two existing digital watermarking schemes proposed by Liu and Tan\cite{13} and Ganic and Eskicioglu\cite{15}. The three host images presented in Fig. 7 were used in the experiments. The correlation values for the abovementioned attacks on the three images for our proposed scheme along with those proposed by Liu and Tan\cite{13} and Ganic and Eskicioglu\cite{15} are listed in Table 3. The closer the correlation value to 1, the better visual quality the attacked image retains. The superiority of the proposed scheme in this article over the other two schemes is established.

5 CONCLUSIONS

An enhanced semi-blind SVD–DCT-based image watermarking technique has been introduced in this paper. During the embedding process, the lower-frequency band is chosen for the one-level DWT and successive wavelet decompositions use the higher-frequency bands. The SVs of the resulting four sub-bands of the last decomposition of HH4 are computed. Rotation is used to convert the watermark image into real-numbers, where the resulting vector is permuted into scrambled data by using a key. The scrambled real-numbers of the watermark vector is converted into an $N \times N$ image and SVD is performed on the resulting processed watermark image to compute the SVs where the combination of the SVs of both the watermark and the predefined four sub-bands is conducted. The watermarked image is reconstructed using IDWT. The extraction process is secure because it requires the key used in the embedding process.

With the proposed scheme, the embedded watermark can successfully survive after attacked by image processing operations, especially for rotation, blurring, sharpening, median filtering, noise addition and compression. Experimental results also showed that the proposed scheme outperformed two existing digital watermarking schemes proposed by Liu and Tan\cite{13} and Ganic and Eskicioglu\cite{15} in terms of robustness with respect to various attacks.

REFERENCES


