Jane, O.; Elbasi, E; Ilk, H. G.
Hybrid Non-Blind Watermarking Based on DWT and SVD
Centro de Ciencias Aplicadas y Desarrollo Tecnológico
Distrito Federal, México

Available in: http://www.redalyc.org/articulo.oa?id=47431860012
Hybrid Non-Blind Watermarking Based on DWT and SVD

O. Jane¹, E. Elbaşi² and H. G. İlk³

¹The Scientific and Technological Research Council of Turkey (TÜBİTAK)
Ankara, Turkey
*onur.jane@tubitak.gov.tr
²İpek University
Department of Animation
Ankara, Turkey
³Ankara University
Department of Electrical and Electronics Engineering
Ankara, Turkey

ABSTRACT

Watermarking is identified as a major technology to achieve copyright protection and multimedia security. Therefore, recent studies in literature include some evident approaches for embedding data into a multimedia element. Because of its useful frequency component separation, the Discrete Wavelet Transform (DWT) is commonly used in watermarking schemes. In a DWT-based scheme, the DWT coefficients are modified with the data that represents the watermark. In this paper, we present a hybrid non-blind scheme based on DWT and Singular Value Decomposition (SVD). After decomposing the cover image into four sub bands (LL, HL, LH and HH), we apply the SVD to LL band and modify diagonal singular value coefficients with the watermark itself by using a scaling factor. Finally, LL band coefficients are reconstructed with modified singular values and inverse DWT is applied to obtain watermarked image. Experimental results show that the proposed algorithm is considerably robust and reliable. In comparison to the previous literature, peak signal-to-noise ratio (PSNR) values of watermarked images are increased by approximately 20%. In terms of PSNR values before and after attacks and of normalized similarity ratio (NSR); although watermark is embedded into LL sub band; our proposed method gives much more satisfactory results on filtering, scaling, Gaussian, JPEG compression, rotation and cropping than that of previous literature.

Keywords: Digital image watermarking, discrete wavelet transform, singular value decomposition, peak signal-to-noise ratio, normalized similarity ratio, non-blind watermarking, multimedia security.

1. Introduction

Digital watermarking is the process that embeds data called watermark into a multimedia object (such as text, audio, image and video) such that watermark can be detected or extracted later to make an assertion about the object [1]. Digital watermarking has received increasing attention especially in recent years. Apart from copy control and copyright protection; broadcast monitoring, fingerprinting, indexing, medical applications and content authentication are other application areas of digital watermarking. For the purpose of designing and developing a new watermarking algorithm in those application areas, the most important properties are robustness and invisibility [2] which are the focal point of this study.

There are basically two approaches to embed a watermark: spatial domain and transform domain watermarking. In the spatial domain, the watermark is embedded by modifying the pixel values in the original image. Transform domain watermarking is similar to spatial domain watermarking; in this case, the coefficients of transforms such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) or Discrete Wavelet Transform (DWT) are modified [3].

Watermark detection is classified into three categories: Non-blind, Blind and Semi-blind Watermarking. Non-blind watermarking requires the original image to detect the watermark. A blind technique does not require the original image to detect watermark. Semi-blind watermarking technique requires the key and the watermarked document for detection.

In this study, visual, invisible and non-blind binary watermark will be embedded into cover image in
transform domain. The rest of this paper includes the following sections. Section 2 reviews related studies on spatial and transform domain watermarking in the literature. Section 3 describes quality measures used as an objective metrics in order to evaluate experimental results. Watermark embedding and extracting algorithms are explained in detail in Section 4 and Section 5 respectively. Section 6 illustrates the experimental results and finally Section 7 concludes this work.

2. Literature review

There are basically two ways to embed a watermark in: spatial domain and transform domain.

Starting point of spatial domain watermarking is to modify the host image pixel values.

Least Significant Bit embedding [4] is the simplest technique. Since the last binary bits are the least significant bits, their modification will not be recognized by human eyes. Spatial domain embedding techniques are very simple and effective, but they are not robust against all kinds of attacks, especially the cropping attack [5, 6].

The principle of transform domain watermarking techniques is to modify transform coefficients. One major drawback of transform domain techniques is the higher computational requirement. In this study, a new watermarking algorithm in combination of DWT and SVD will be implemented. Therefore, previous studies in the literature are discussed in the following.

a. Discrete Wavelet Transform: Due to its great frequency component separation properties, the DWT, in contrast to DCT, is very useful to identify the coefficients to be watermarked [7]. The DWT separates image into a lower resolution image (LL), and horizontal (HL), vertical (LH) and diagonal (HH) detail components. The DWT is also computationally efficient and implemented by using simple filter convolution. The magnitudes of DWT coefficients are larger in the lowest bands (LL) at each level of decomposition. Embedding the watermark in the higher level sub bands increases the robustness of the watermark. However, the image visual fidelity may be lost, which can be measured by PSNR. With the DWT, the edges and texture can be easily identified in the high frequency bands like HH, LH and HL. The large coefficients in these bands normally indicate edges in the image. Therefore, DWT understands the human visual system more closely in comparison to the DCT.

Dugad et al. [7] proposed wavelet based scheme for watermarking images by embedding the watermark into LL band coefficients in the same way Cox et al. proposed before [8]. Hsieh and Tseng proposed DWT-based algorithm in the following steps: An original image is decomposed into wavelet coefficients. Then, multi-energy watermarking scheme based on the qualified significant wavelet tree is used to achieve a robust algorithm [9]. Elbasi and Eskicioglu embedded a pseudo-random sequence as a watermark in two bands (LL and HH) by using DWT [10].

b. Singular Value Decomposition: Any m by n matrix A can be factored into $A = U \times S \times V^T$ (orthogonal) (diagonal) (orthogonal). The columns of U (m by m) (left singular vectors) are eigenvectors of $A \times A^T$ and the columns of V (n by n) (right singular vectors) are eigenvectors of $A^T \times A$ [11]. The U and V matrices are orthogonal matrices so that $U^T \times U = I$ and $V^T \times V = I$, where I is the unit matrix. Columns of U and V matrices are called left and right singular vectors which represent horizontal and vertical details of an image respectively [12]. Their singular values on the diagonal of S (m by n) are the square roots of the nonzero eigenvalues of both $A \times A^T$ and $A^T \times A$. If A is an image in this case; S, the diagonal matrix with rank R, have the luminance (gray scale) values of the image layers produced by U and V.

Gorodetski et al. proposed an approach on embedding a bit of data through slight modifications of singular values of a small block of the segmented covers [13]. Chandra divided the image into sub blocks, applied the SVD to those blocks and modified the largest singular value of them by a watermark and a scaling factor [14]. Liu and Tan used a pseudo Gaussian random number as a watermark and added it to the singular values of the original image [15]. Calagna et al. divided the cover image into blocks and applied the SVD to each block. In order to balance embedding capacity with distortion, the watermark was embedded in all the non-zero singular values according to the local features of the cover image [16]. Bao and Ma proposed an image-adaptive watermarking scheme for image authentication by
applying a simple quantization-index-modulation process on wavelet domain SVD [17]. Ghazy et al. designed a new watermarking algorithm in the following order: The original image is divided into blocks and then the watermark is embedded in the singular values of each block separately. Watermark detection is implemented by extracting the watermark from the singular values of the watermarked blocks [18].

In general, most of the image energy is concentrated at the lower frequency coefficient sets LLs and therefore embedding watermarks in these coefficient sets may degrade the image significantly. However, embedding watermark in the LL bands increase robustness effectively [19]. The fact that makes our study novel is that we will increase robustness of the watermarked image under certain attacks without degrading the image by embedding binary watermark on LL band. In comparison to [18], in our study, watermark is embedded into SVD coefficients of LL sub-band. Although LL sub band embedding is not generally robust to geometric attacks, experimental results in Section 6 will show that the algorithm is not only robust to compression attacks but also to geometric attacks. This also explains why LL sub band is chosen for watermark embedding.

3. Quality measures

Measurement of image and video quality is a challenging problem in wide range of application [6, 20]. The quality measures can be classified into two groups: Subjective and objective. There are a number of objective measures. We mention some of these measures below:

Mean Square Error (MSE): MSE is an old, proven measure of control and quality. The MSE is defined as follows in Eq. 1:

\[
MSE = \frac{1}{M \times N} \sum_{i,j} [I(i,j) - I'(i,j)]^2
\]

where \( I(i,j) \) is the original image that contains \( M \times N \) pixels, and \( I'(i,j) \) is the watermarked image.

Peak Signal-to Noise Ratio (PSNR): PSNR is most commonly used as a measure of quality of reconstruction in image watermarking. It is a ratio between the maximum value of a signal and the magnitude of background noise. It is most easily defined via MSE for an 8-bit gray scale image as shown in Eq. 2.

\[
PSNR = 20 \times \log \left( \frac{255}{\sqrt{MSE}} \right)
\]

Similarity Ratio (SR): SR is defined as in Eq. 3

\[
SR = \frac{s}{s+d}
\]

where \( S \) and \( D \) represents the number of matching pixel values in compared images and the number of different pixel values in compared images respectively. SR is used in evaluation of non-blind watermark extraction. When different pixel values converge to 0, SR will be close to 1 which is the optimum and desired condition. In this study, binary image in Figure 1.c. is used as a watermark. Even the letters ‘B’ and ‘C’ is assigned as 0 under attack, SR is computed as 0.8002 which can be seen as a successful result at first glance; however, when SR is equal to 0.8002, all of pixels in extracted watermark is 0. Thus, it is convenient to map minimum SR 0.8002 to 0 and to use and calculate “Normalized SR (NSR)” in Eq. 4.

\[
NSR = \frac{SR - \min(SR)}{1 - \min(SR)}
\]

4. Watermark embedding algorithm

In our proposed study, watermark embedding procedure is as follows:

Input: Cover Work (I) and Binary Image Watermark (W)

Output: Watermarked Image (IW)

Step 1. Using DWT, decompose the cover work, I, into four sub bands: LL, LH, HL and HH.

Step 2. Apply SVD to the sub band LL:

\[ LL = U_{LL} \times S_{LL} \times V_{LL}^T \]

Step 3. Modify \( S_{LL} \), the singular values of the sub band LL, by adding binary watermark image, W, with the scaling factor \( \alpha \):

\[ S_{LLo} = S_{LL} + \alpha \times W \]
Step 4. Since the watermark image is directly added to the singular values of the sub band LL with the scaling factor, it is wise to reconstruct it by applying SVD again to $S_{LLD}$:

$$S_{LLD} = U_{SSL} \times S_{SSL} \times V_{SSL}^T$$

Step 5. Replace $S_{SSL}$ with SLL in Step 2:

$$LL_{svd} = U_{LL} \times SS_{LL} \times V_{LL}^T$$

Step 6. Compute the inverse DWT to obtain the watermarked cover image.

5. Watermark extracting algorithm

According to watermark embedding algorithm in the previous section, watermark extracting procedure is as follows:

Input: Attacked Watermarked Image (IW*)

Output: Extracted Watermark (W*)

Step 1. Using DWT, decompose watermarked and possibly attacked image, IW*, into four sub bands: $LL_W$, $LH_W$, $HL_W$, and $HH_W$.

Step 2. Apply SVD to the sub band $LL_W$:

$$LL_W = U_W \times S_W \times V_{W}^T$$

Step 3. Using left and right singular vectors ($U_{SSL}$ and $V_{SSL}^T$) of $S_{SSL}$ in Step 4 in watermark embedding algorithm, construct $S_{SSL}^*$ by multiplying them with $S_W$ in Step 2 in the following order:

$$S_{SSL}^* = U_{SSL} \times S_S \times V_{SSL}^T$$

Step 4. Extract the watermark W*:

$$W^* = S_{SSL}^* \times S_{LL} \times \alpha$$

Step 5. If the value of a pixel in W* is greater than or equal to pre-defined threshold value, TH, assign that pixel value to binary 1, otherwise to binary 0.

6. Experimental results

Test images used in this proposed watermarking algorithm are shown in Figure 1.

Goldhill in Figure 1.a and Peppers Figure 1.b and are 8 bit 512x512 gray scale images respectively. Figure 1.c used as the watermark is a binary image in size 256x256.

In order to obtain good visual quality of watermarked images, choosing scaling factor value, $\alpha$, plays an important role in watermark embedding procedures [21]. If the value of $\alpha$ is chosen close to zero, the watermarked image is less distorted and maximum PSNR can be obtained. However, for lower $\alpha$ values, watermarked images are less robust to several attacks. Therefore, to choose optimum value of $\alpha$, it is useful in practice to investigate PSNR values of watermarked images after several attacks and to make a trade-off analysis on them.

Guiding to choose optimum scaling factor in watermark embedding algorithm, Table 1 shows the change of PSNR values for $\alpha$ in certain intervals for the cover work in Figure 1.a.
After investigating Table 1 in detail, maximum PSNR values for several attacks can be obtained by choosing the scaling factor, $\alpha$, as 23 for the cover work in Figure 1.a., Goldhill.

In the same manner, Table 2 shows the change of PSNR values for scaling factors in certain intervals for the cover work in Figure 1.b.

Table 1. Variation of PSNR values on different scaling factors and attacks for Goldhill.

<table>
<thead>
<tr>
<th>Goldhill Attacks/Scaling Factors</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
<th>30</th>
<th>35</th>
<th>40</th>
<th>45</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian</td>
<td>30.000</td>
<td>29.993</td>
<td>29.941</td>
<td>29.960</td>
<td>29.889</td>
<td>29.846</td>
<td>29.719</td>
<td>29.618</td>
<td>29.533</td>
<td>29.414</td>
</tr>
<tr>
<td>Histogram Eq.</td>
<td>17.545</td>
<td>17.555</td>
<td>17.570</td>
<td>17.553</td>
<td>17.547</td>
<td>17.551</td>
<td>17.532</td>
<td>17.538</td>
<td>17.516</td>
<td>17.543</td>
</tr>
<tr>
<td>Gamma Correct.</td>
<td>17.696</td>
<td>17.698</td>
<td>17.703</td>
<td>17.707</td>
<td>17.714</td>
<td>17.719</td>
<td>17.720</td>
<td>17.726</td>
<td>17.734</td>
<td>17.747</td>
</tr>
</tbody>
</table>

After investigating Table 2 in detail, maximum PSNR values for several attacks can be obtained by choosing the scaling factor, $\alpha$, as 20 for the cover work in Figure 1.b., Peppers.

Figure 2 shows watermarked images after using related scaling factors and applying watermark embedding algorithm in Section 4.

Table 2. Variation of PSNR values on different scaling factors and attacks for Peppers.

<table>
<thead>
<tr>
<th>Peppers Attacks/Scaling Factors</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
<th>30</th>
<th>35</th>
<th>40</th>
<th>45</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian</td>
<td>30.100</td>
<td>30.080</td>
<td>30.050</td>
<td>30.059</td>
<td>30.004</td>
<td>30.007</td>
<td>29.948</td>
<td>29.894</td>
<td>29.800</td>
<td>29.741</td>
</tr>
</tbody>
</table>
Thinking that PSNR values between 30 and 40 dB is considered as satisfactory, results in Figure 2 show that watermark embedding algorithm is successful enough to use it in several applications. Nevertheless, watermark embedding and extracting algorithms are complements of each other. Thus, it is worthwhile to investigate extracted watermarks after pre-defined attacks in both Table 1 and Table 2.

Figure 3 shows watermarked Goldhill images after attacks and their PSNR values.

In a similar way, Figure 4 shows watermarked Peppers images after attacks and their PSNR values.

Even though PSNR values after attacks are too low to extract the watermark on them, our proposed algorithm provides high NSR enough close to 1.0. However, before calculating and
comparing NSR values for each attacked images, we had better find optimum threshold values as we did in choosing optimum scaling factor. Figure 5 shows the change of NSR for threshold values in certain intervals between 0 and 1 for the cover work in Figure 1.a., Goldhill.

Figure 4. a. Filter (31.7115 dB), b. Scaling 512x512→256x256 (30.4856 dB), c. Gaussian (30.0589 dB), d. Histogram (18.6076 dB), e. Gamma Correction (18.3488 dB), f. JPEG Compression (Q=25) (8.0828 dB) g. Rotation (20 degree) (10.0352 dB), h. Intensity Adjustment (18.7548 dB), i. Cropping (12.8781 dB), j. Salt & Pepper (12.0598 dB).
In the same way, Figure 6 shows the change of NSR for threshold values in certain intervals between 0 and 1 for the cover work in Figure 1.b., Peppers.

After analyzing Figure 5 and 6, NSR values for several attacks can be obtained maximum by choosing threshold value, TH, as 0.5 for both cover works in Figure 1.a and Figure 1.b. Figure 7 shows extracted watermark images from attacked Goldhill and calculated NSR values for TH=0.5 after applying watermark extracting algorithm in Section 5.

---

**Figure 5.** Variation of NSR values of Goldhill cover work for several attacks on different threshold between 0 and 1.

**Figure 6.** Variation of NSR values of Peppers cover work for several attacks on different threshold between 0 and 1.
Figure 7. Extracted watermarks from attacked Goldhill image and their NSR values. a. Filter (0.9946), b. Scaling 512x512 → 256x256 (0.9925), c. Gaussian (0.9883), d. Histogram (0.9880), e. Gamma Correction (0.9995), f. JPEG Compression (Q=25) (0.9929) g. Rotation (20 degree) (0.9883), h. Intensity Adjustment (0.9903), i. Cropping (0.9947), j. Salt & Pepper (0.9076).

Figure 8. Extracted watermarks from attacked Peppers image and their NSR values. a. Filter (0.9946), b. Scaling 512x512 → 256x256 (0.9936), c. Gaussian (0.9939), d. Histogram (0.9878), e. Gamma Correction (0.9969), f. JPEG Compression (Q=25) (0.9880) g. Rotation (20 degree) (0.9957), h. Intensity Adjustment (0.9891), i. Cropping (0.9947), j. Salt & Pepper (0.9047).
7. Conclusion

This paper presented a non-blind watermarking scheme based on hybrid DWT and SVD. After decomposing the cover image into four sub bands (LL, HL, LH and HH), we apply SVD to LL band and modify diagonal singular value coefficients with the watermark itself by using a scaling factor. Then, LL band coefficients are reconstructed with modified singular values and finally inverse DWT is applied to obtain watermarked image.

The novelty of this study from the reference method proposed by Ghazy et al. in [18] is to decompose the cover work, I, into four sub bands; LL, LH, HL and HH by using DWT and to modify singular values of sub band LL with a pre-defined scaling factor.

The other novel side of this study is to make an optimization analysis and decide on scaling factor used in embedding and on threshold value used in extracting.

PSNR values before and after attacks for both referenced method in [18] and proposed method are compared in Table 3.

In the same way, NSR values for both referenced method in [18] and proposed method are comparatively shown in Table 4.

In our study, frequently-preferred transform domain technique DWT and decomposition method SVD is combined so that watermarked images are much more robust against attacks. Thus, on the contrary to traditional DWT watermarking techniques, this proposed algorithm can be considered as robust against not only compression-based attacks such as filtering, Gaussian and JPEG compression; but also geometric and pixel-based attacks such as scaling, histogram equalization, gamma correction, rotation, intensity adjustment, and salt and pepper. This is because the change of diagonal coefficients in singular value matrix of LL sub band has small effect on perceptual of the watermark.

As shown visually in Figure 7, Figure 8 and compared SNR values objectively in Table 4, NSR values are close to 1 despite strong attacks causing lower PSNR values in Table 3.

In comparison to [18], PSNR values of watermarked images are increased approximately by 20%. Furthermore; in the light of PSNR values before and after attacks and NSR values, our proposed method gives much more satisfactory results on filtering, scaling, Gaussian, JPEG compression, rotation and cropping than that of previous studies.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Goldhill (α=23)</th>
<th>Peppers (α=20)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>24.0069</td>
<td>29.863</td>
</tr>
<tr>
<td>Scaling</td>
<td>24.3656</td>
<td>29.7727</td>
</tr>
<tr>
<td>Gaussian</td>
<td>29.6162</td>
<td>29.9154</td>
</tr>
<tr>
<td>Histogram Eq.</td>
<td>17.5812</td>
<td>17.5452</td>
</tr>
<tr>
<td>Gamma Correct.</td>
<td>17.8411</td>
<td>17.7106</td>
</tr>
<tr>
<td>JPEG (Q=25)</td>
<td>8.1869</td>
<td>8.3348</td>
</tr>
<tr>
<td>Rotation (20°)</td>
<td>11.2472</td>
<td>11.4089</td>
</tr>
<tr>
<td>Intensity Adj.</td>
<td>19.012</td>
<td>19.0637</td>
</tr>
<tr>
<td>Cropping</td>
<td>9.9401</td>
<td>13.0455</td>
</tr>
<tr>
<td>Salt &amp; Pepper</td>
<td>12.2597</td>
<td>12.3335</td>
</tr>
</tbody>
</table>

Table 3. Comparative study on PSNR values before and after attacks for both referenced and proposed method.
### References


### Table 4

<table>
<thead>
<tr>
<th>Attacks</th>
<th></th>
<th>NSR Goldhill ($\alpha=23$)</th>
<th>Peppers ($\alpha=20$)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Referenced Method</td>
<td>Proposed Method</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Ghazy et al., 2007)</td>
<td>(Ghazy et al., 2007)</td>
</tr>
<tr>
<td>Filter</td>
<td></td>
<td>0.9702</td>
<td>0.9946</td>
</tr>
<tr>
<td>Scaling</td>
<td></td>
<td>0.9359</td>
<td>0.9925</td>
</tr>
<tr>
<td>Gaussian</td>
<td></td>
<td>0.9886</td>
<td>0.9883</td>
</tr>
<tr>
<td>Histogram Eq.</td>
<td></td>
<td>0.9877</td>
<td>0.9878</td>
</tr>
<tr>
<td>Gamma Correct.</td>
<td></td>
<td>0.9995</td>
<td>0.9995</td>
</tr>
<tr>
<td>JPEG (Q=25)</td>
<td></td>
<td>0.9921</td>
<td>0.9929</td>
</tr>
<tr>
<td>Rotation (20°)</td>
<td></td>
<td>0.9512</td>
<td>0.9883</td>
</tr>
<tr>
<td>Intensity Adj.</td>
<td></td>
<td>0.9907</td>
<td>0.9930</td>
</tr>
<tr>
<td>Cropping</td>
<td></td>
<td>0.9845</td>
<td>0.9947</td>
</tr>
<tr>
<td>Salt &amp; Pepper</td>
<td></td>
<td>0.9288</td>
<td>0.9076</td>
</tr>
</tbody>
</table>

Table 4. Comparative study on NSR values for both referenced and proposed method.


