Robust Watermarking for Color Images using SVD with Column/Row Wavelet Transforms in Low and Mid-Frequency Spectrum of Host

H. B. Kekre¹, Tanuja Sarode² and Shachi Natu³
¹MPSTME, NMIMS University Mumbai, India
²TSEC, Mumbai University, Mumbai,
³NMIMS University, Mumbai;
¹hbekre@yahoo.com, ²tanuja_0123@yahoo.com, ³shachi_natu@yahoo.com

ABSTRACT

This paper proposes a joint SVD and wavelet transform based watermarking technique. Host and watermark images are column/row transformed using wavelet transforms like DCT wavelet, Walsh wavelet, Haar wavelet and DKT wavelet. These wavelet transforms are generated from orthogonal transforms DCT, Walsh, Haar and DKT. Generally middle frequency region of transformed host is used to hide the watermark. However, in proposed technique, stability of SVD is exploited to hide the watermark in low frequency region of host. Singular values of low as well as middle frequency region of transformed host are altered with suitable scaling factors to hide the watermark. Performance of the technique is tested under compression, cropping, noise addition and resizing attack. Use of low frequency region in proposed method shows strong robustness for all attacks except cropping and is immediately followed by use of mid-frequency region. To sustain against cropping attack, mid-frequency region is found to be more suitable.

Keywords: Watermarking, Singular Value Decomposition, column wavelet transform, row wavelet transform, Discrete Kekre Transform (DKT), Binary distributed run length noise, Gaussian Distributed run length noise, JPEG compression.

1 Introduction

Watermarking is the process of hiding some information in multimedia contents such as image, audio or video file to protect it from copyright abuse [1]. Two major constraints that need to be followed while watermarking the digital contents are robustness and visual imperceptibility of hidden information. In recent years, use of transforms is gaining popularity in the process of watermarking as it is more robust than spatial domain watermarking techniques. DCT, DFT, wavelet transform prove to be more robust in digital watermarking process. Combining two or more transforms together has also become quite popular to increase the robustness. Singular Value decomposition (SVD) and Discrete Wavelet Transform (DWT) [2, 3, 4, 5], DCT-DWT [6, 7, 8], DCT_DWT_SVD [9, 10] are the commonly used combinations of transforms in watermarking. In this paper a hybrid watermarking technique using SVD and column/row wavelet transform generated from orthogonal transforms DCT, Walsh, Haar and Discrete Kekre Transform is proposed. Middle frequency band and low frequency band of column/row wavelet transformed image is used to embed the singular values of watermark. Proposed method is evaluated against compression, cropping, noise addition, and image resizing. Remaining paper is organized as follows: section 2
discusses existing work in digital image watermarking field. Section 3 explains singular value decomposition and wavelet transforms. Section 4 explains proposed method. Section 5 evaluates the performance of proposed technique against various attacks. Section 6 ends the paper with conclusion.

2 Related Work

Qiang Li, Chun Yuan, Yu-Zhuo Zhong proposed a hybrid DWT-SVD based watermarking considering human visual properties [2]. Host image is divided into four sub bands and each band is subjected to SVD. Singular values of watermark are embedded in these singular values of host. The embedding strength is determined by a human visual model proposed in A.S. Lewis and G. Knowles, (1992) and improved in M. Bertran et al., (2001). The scheme is claimed to be robust for its embedding data into all frequencies and large capacity for using SVD. In addition, the use of human visual model guarantees the imperceptibility of the watermark.

In [11] a robust hybrid image watermarking scheme based on SVD and DCT is proposed. After applying SVD to the cover image blocks, DCT on the macro block comprised of the first singular values of each image block is applied. Watermark is embedded in the high-frequency band of the SVD-DCT block by imposing a particular relationship between some pseudo-randomly selected pairs of the DCT coefficients. In [12] a method of non-blind transform domain watermarking based on DWT-DCT-SVD is proposed. The DCT coefficients of the DWT coefficients are used to embed the watermarking information. This method of watermarking is found to be robust and the visual watermark is recoverable without any perceivable amount of distortion even in the case of attacks.

In [13] authors proposed implementation and performance analysis of two different watermarking schemes based on DCT-DWT-SVD. One is based on SVD of DC coefficients using second level DWT decomposition and other is considering SVD of all DCT values of second level DWT composition of cover image. Effectiveness of proposed schemes is measured using PSNR and Normalized Cross Correlation (NCC).

A new SVD based and DCT-DWT oriented watermarking scheme is proposed in [9]. To achieve robustness with high perceptual transparency and low insertion ratio, the middle band DCT coefficients are chosen to achieve high robustness against JPEG compression. Robustness against other attacks is achieved by taking DWT of the DCT coefficients and the lowest frequency LL band of DWT is chosen for insertion. Insertion method in proposed technique uses SVD because slight variation of singular values does not change the visual perception of the image. To attain robustness and imperceptibility, a hybrid image-watermarking scheme based on Discrete Wavelet Transform (DWT) and Singular value decomposition (SVD) is proposed in [14]. The LH Band of the third level of image in DWT domain is modified with SVD to embed the singular value of watermark. The proposed embedding and extracting methodology was employed to accelerate the hybrid DWT-SVD watermarking and to avoid the leak of watermark. This hybrid technique results to optimize both (robustness and imperceptibility) the fundamentally conflicting requirements. Lagzian, Soryani and Fathy [15] proposed a watermarking scheme based on redundant discrete wavelet transform (RDWT) and Singular Value Decomposition (SVD). After applying RDWT to cover image, SVD is applied to each sub band. Then singular values of the cover image are modified using singular values of the visual watermark. The advantage of the proposed technique is its robustness against most common attacks in comparison to the DWT-SVD method.
In [16] a novel approach of watermarking for copyright protection applications using the singular value decomposition (SVD) in the dual tree complex wavelet transform (DT-CWT) domain is introduced. After applying the 2-level DT-CWT to the cover grayscale image, SVD of each high-pass sub band is obtained. These singular values are then modified by the singular values of the DT-CWT-transformed visual watermark. Modification in all sub bands allows the development of a watermarking scheme that is robust to a wide range of attacks. Wang et. al in [17] proposed a novel watermarking scheme for image authentication based on discrete wavelet transform (DWT) and singular value decomposition (SVD). Different from the developed SVD-based watermarking schemes where the singular values are slightly modified, this scheme constructs the watermarks from the singular vectors which specify intrinsic geometry properties of images. Within the framework of zero watermarking, the watermarks are registered in a third-party intellectual property rights (IPR) database for copyright protection. Experimental results show that this scheme is robust not only to common image processing operations, but also robust to local geometric distortions. A blind watermarking scheme based on the discrete wavelet transform (DWT) and singular value decomposition is proposed in [18]. Singular values of high frequency (HH) band are used to optimize perceptual transparency and robustness constraints. A joint DWT and DCT based watermarking technique with low frequency watermarking with weighted correction is proposed in [19]. DWT has excellent spatial localization, frequency spread and multi-resolution characteristics, which are similar to the theoretical models of the human visual system (HVS). DCT based watermarking techniques offer compression while DWT based watermarking techniques offer scalability. These desirable properties are used in this combined watermarking technique.

### 3 Wavelet Transforms and Singular Value Decomposition

Wavelets are mathematical functions that cut up data into different frequency components, and then study each component with a resolution matched to its scale [23]. Principal advantage of wavelet is that they provide time-frequency localization. Temporal analysis is performed with a contracted, high-frequency version of the prototype wavelet, while frequency analysis is performed with a dilated, low-frequency version of the same wavelet [23]. Wavelet transform used in the proposed method is generated using wavelet generation algorithm given in [23].

Using singular value decomposition, any real matrix A can be decomposed into a product of three matrices U, S and V as A=USVT, where U and V are orthogonal matrices and S is diagonal matrix. If A is mxn matrix, U is mxm orthonormal matrix whose columns are called as left singular vectors of A and V is nxn orthonormal matrix whose columns are called right singular vectors of A. For m>n, S takes the following form [20]:

\[
S = \begin{bmatrix}
s_1 & 0 & \cdots & 0 \\
0 & s_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & s_n
\end{bmatrix}
\]

The diagonal elements are listed in descending order, \(s_1 \geq s_2 \geq \cdots \geq s_n \geq 0\).

Some properties of SVD which make it useful in image processing are:

- The singular values are unique for a given matrix.
- The rank of matrix A is equal to its nonzero singular values. In many applications, the singular values of a matrix decrease quickly with increasing rank. This property allows us to reduce the noise or compress the matrix data by eliminating the small singular values or the higher ranks [21].
The singular values of an image have very good stability i.e. when a small perturbation is added to an image; its singular values don’t change significantly [22].

4 Proposed Method

In the proposed method, DCT wavelet, Walsh wavelet, Haar wavelet and DKT wavelet transforms are used generated from orthogonal transforms DCT, Walsh, Haar and DKT respectively by using the algorithm in [23]. Since, different size combinations are possible to generate desired size wavelet transform matrix, all such possible size combinations are tried and the best size combination is selected for experimental work. For watermark image, (32, and 4) and for host image (16, 16) pair of component orthogonal transforms is observed to give best robustness and hence it is selected. A test set of five color bitmap host images (256x256) and a watermark (128x128) is used.

Embedding and extraction procedures explained below are followed on each plane of host and watermark image separately.

4.1 Steps for embedding

Step 1. Apply column/row wavelet transform to host and watermark image.

Step 2. Perform Singular value decomposition on column/row transformed watermark image. Since watermark is of size 128x128, it gives 128 singular values.

Step 3. Due to high energy compaction property of SVD, only few of these singular values hold maximum energy of image and are sufficient for embedding in host. In proposed experimental work it has been observed that only first 30 singular values pack almost 99% of image energy and hence are selected for embedding.

Step 4. To embed 30 singular values in host, frequency band of 30 rows/columns is selected from column/rows transformed host image. After testing various middle frequency rows/columns for robustness it is observed that frequency band ranging from row/column 101 to 130 is better than other rows/columns. Also a low frequency band of rows/columns 1 to 30 is selected for embedding the watermark.

Step 5. Singular value decomposition of selected low / mid frequency band of host is obtained. These singular values of host are now replaced by singular values of column/row transformed watermark. Each singular value of watermark is adaptively scaled down to match with the singular value of host frequency band in order to minimize the distortion in watermarked image. These scaling factors are preserved for use in extraction process.

Step 6. Inverse SVD followed by inverse column/row transform is obtained to get watermarked image. Imperceptibility of proposed technique is measured by calculating average of absolute pixel difference (Mean Absolute Error) between host and watermarked image.
Watermarked image obtained through embedding process is tested under various image processing attacks and from these attacked watermarked images; watermark is extracted using extraction procedure as described below.

4.2 Extraction procedure

Extraction procedure is performed on watermarked image in the following manner:

**Step 1.** Take column/row wavelet transform of watermarked/attacked watermarked image. Select the frequency band (low / middle) in which embedding is done.

**Step 2.** Perform SVD on this frequency band and scale up the obtained singular values using adaptive scaling factors preserved in embedding process.

**Step 3.** Perform inverse singular value decomposition using these singular values to get the extracted watermark.

**Step 4.** Robustness of proposed technique is measured using Average absolute pixel difference (MAE) between embedded and extracted watermark.

5 Performance Analysis of Proposed Technique against Various Attacks

Watermarked images are subjected to attacks like compression, cropping, noise addition, resizing. Performance of each of these attacks when watermark is embedded in low frequency band and middle frequency band is evaluated.

5.1 Compression attack

Watermarked images are subjected to compression using different techniques namely compression using transforms, compression using Vector Quantization and JPEG compression.

DCT, DST, Walsh, Haar and DCT wavelet are the transforms used for transform based compression. In VQ based compression KFCG [24] algorithm is used and a codebook of size 256 is generated to compress the image. In JPEG compression, 100% quality factor is used to compress the image.

Watermarked images after performing compression attack using Haar and watermark extracted from it are shown in Figure 2. These images are for embedding done in low and middle frequency bands. For each of these images, MAE is given below it.

<table>
<thead>
<tr>
<th></th>
<th>(a) DCT column wavelet transform rows 1-30</th>
<th>(b) DCT column wavelet transform rows 101-130</th>
<th>(c) DCT row wavelet transform columns 1-30</th>
<th>(d) DCT row wavelet transform columns 101-130</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAE</td>
<td>0.810</td>
<td>8.018</td>
<td>0.733</td>
<td>0.733</td>
</tr>
</tbody>
</table>

Figure 2 watermarked images after performing compression attack using Haar and watermark extracted from them (a) when watermark is embedded in low frequency band of DCT column wavelet transform (b) when watermark is embedded in middle frequency band of DCT column wavelet transform (c) when watermark is embedded in low frequency band of DCT row wavelet transform (d) when watermark is embedded in middle frequency band of DCT row wavelet transform.

Summary of different types of compression attacks is given in Figure 3 to Figure 6. Figure 3 shows performance of various column wavelet transforms against compression using DCT, DST, Walsh and Haar when watermark is embedded in low frequency region (rows/columns 1 to 30) and middle frequency region (rows/columns 101 to 130).
From Figure 3, it is observed that all column transforms used for watermark embedding give excellent robustness against compression attack using DCT and DST when watermark is embedded in low or middle frequency band. Column DCT wavelet and column Haar wavelet show little increase in MAE when compression is performed using Walsh and embedding is done in middle frequency region. However this increase is not spoiling the quality of recovered watermark and still can be considered as very good performance against compression attack. Thus proposed method is highly robust for almost all transform based compression attacks.

Figure 4 compares performance of each column wavelet transforms against compression using DCT wavelet, JPEG compression and VQ based compression when watermark is inserted in low and middle frequency elements.

In low frequency region, all column wavelet transforms exhibit very good robustness against compression using DCT wavelet, JPEG compression and VQ based compression. When embedding is done in middle frequency region, column Walsh wavelet and column Haar wavelet performance against DCT wavelet based compression is slightly degraded. For JPEG and VQ based compression all column wavelet transforms exhibit high sustainability.
Figure 5 shows performance comparison against compression using different transforms when embedding in low and middle frequency is done using row wavelet transforms.

Similar to column wavelet transform behavior, row DCT wavelet shows excellent robustness against compression when low frequency region is used for embedding. For middle frequency region embedding, DCT wavelet shows very good robustness for DCT and DST and Walsh compression. For Haar based compression, row DCT wavelet performance is poorer as compared to Walsh wavelet, Haar wavelet and DKT wavelet. Row Walsh wavelet transform also shows good sustenance for all transform based attacks when watermark is embedded in middle frequency as well as low frequency singular values. Row DKT wavelet is also observed to be robust for all transform based compression attacks when watermark is embedded in low and middle frequency band singular values. Row Walsh wavelet transform shows excellent robustness for DCT, DST and Haar based compression irrespective of frequency band used for embedding. For Walsh based compression it shows higher MAE when embedding is done in middle frequency region. In all Row wavelet transforms also show very good robustness against compression using DCT, DST, Walsh and Haar when watermark is embedded in singular values of low frequency region.

Figure 6 compares performance of embedding in low and middle frequency regions using different row wavelet transforms against compression using DCT wavelet, JPEG compression and VQ based compression.
From Figure 6, we can see that for compression using DCT wavelet, embedding watermark in low frequency region, all row wavelet transform used for embedding, shows excellent sustenance. Row DCT wavelet and row DKT wavelet also sustain this attack when watermark is embedded in middle frequency region. However, row Walsh wavelet and row Haar wavelet show poor resistance against DCT wavelet based compression when embedding is performed in middle frequency region. For JPEG and VQ based compression though use of low frequency band shows better sustenance than middle frequency region, both regions can be concluded to show excellent robustness.

5.2 Cropping of watermarked images

Different amount of information is cropped from watermarked images by cutting the 16x16 size square portion at corners, 32x32 size square portions at corners and 32x32 size square portions at the center of watermarked image. Figure 7 shows result images for cropping 32x32 at center and using DCT column wavelet for embedding watermark. Sustenance of proposed method against such cropping when singular values of low and middle frequency region of host are chosen for watermark embedding using different column and row wavelet transforms is compared in Figure 8 and Figure 9.

Figure 7 watermarked images after performing cropping attack and watermark extracted from them (a) when watermark is embedded in low frequency band of DCT column wavelet transform (b) when watermark is embedded in middle frequency band of DCT column wavelet transform (c) when watermark is embedded in low frequency band of DCT row wavelet transform (d) when watermark is embedded in middle frequency band of DCT row wavelet transform.

From Figure 7, it can be seen that embedding watermark in low frequency region is less robust against cropping attack than embedding in middle frequency singular values. Further, for middle frequency embedding, row DCT wavelet is more robust than column wavelet.

Figure 8 shows the comparison of performance against cropping attack when column wavelet transforms are used.

Figure 8 Comparison of MAE between embedded and extracted watermark against cropping when watermark is embedded in low and middle frequency elements using different column wavelet transforms.
From Figure 8 it is observed that, all column wavelet transforms explored in proposed technique give outstanding robustness against cropping attack when watermark is embedded in middle frequency region. Comparatively, when watermark is embedded in low frequency region, robustness is less. For 32x32 cropping done at corners of an image, embedding watermark in low frequency region does not give acceptable robustness. However if we compare 16x16 cropping at corners and 32x32 cropping at center where area cropped from watermarked image is same, proposed technique shows marginally better robustness for cropping done at corners for all wavelet transforms.

Figure 9 shows comparison against cropping attack when row wavelet transforms are used to embed the watermark in low and middle frequency regions.

From Figure 9, it is observed that proposed watermarking technique is not giving good robustness for 32x32 cropping done at corners of an image using low as well as middle frequency band for embedding watermark when row DCT wavelet and row Haar wavelet is used. Row Walsh wavelet and row DKT wavelet give very good robustness against 32x32 cropping at corners and when middle frequency region is used to embed the watermark. For 16x16 cropping at corners and 32x32 cropping at center where same amount of information is cropped from image, all row wavelet transforms show excellent robustness irrespective of frequency band used for embedding. Among them row DCT wavelet and Row Haar wavelet perform marginally better for cropping at center and row Walsh and row DKT show marginally better robustness for 16x16 cropping at corners.

5.3 Noise addition to watermarked images

Binary distributed run length noise with different run length and Gaussian distributed run length noise are added to watermarked images.
Figure 11 shows the comparison of MAE between embedded and extracted watermark from different types of noise added watermarked images and when low and middle frequency singular values of host are selected for watermark embedding using column wavelet transforms.

From Figure 11 we can observe that irrespective of the frequency band selected for embedding watermark (low/middle) and column transform used for embedding process, proposed technique shows excellent robustness against noise addition attack as the MAE values between embedded and extracted watermark are very small.

Figure 12 shows comparison of low frequency and middle frequency embedding using row wavelet transforms against noise addition attacks.

From Figure 12 we can conclude that for binary distributed run length noise with run length 1 to 10 and for Gaussian distributed run length noise, better robustness is observed for low frequency singular values selected for watermark embedding. For increased run length of binary distributed run length noise, selection of middle frequency region to embed the watermark is more robust. Highest robustness is observed for binary distributed run length noise with run length 10 to 100 by
column DCT wavelet and column Haar wavelet when watermark is embedded in middle frequency region. For Gaussian distributed run length noise attack though for middle frequency region MAE value is higher than low frequency region, since these values itself are very small, performance of proposed technique can be considered excellent using row wavelet transforms as well.

5.4 Resizing attack

In resizing attack, watermarked image is increased in size two times and then reduced to its original size. For this bicubic interpolation, transform based image zooming [25] and grid based interpolation [26] mechanism are used. For bicubic interpolation, resizing is performed by increasing the image size to four times and two times separately and then reducing it back to original size. Figure 13 shows resized-reduced (twice large and reduced) watermarked imaged using bicubic interpolation

![Figure 13 Watermarked images resized and reduced back to original size using bicubic interpolation and watermark extracted from them when (a) watermark is embedded in low frequency band using column DCT wavelet transform (b) watermark is embedded in middle frequency region using column DCT wavelet (c) watermark is embedded in low frequency region using row DCT wavelet transform (d) watermark is embedded in middle frequency region using row DCT wavelet.](image)

As can be seen from Figure 13, embedding watermark in low frequency region of host is more robust against resizing attack. Average performance of various column wavelet transforms against noise addition attack when low and middle frequency regions are used to embed watermark is compared in Figure 14

![Figure 14 Comparison of MAE between embedded and extracted watermark against resizing attack when watermark is embedded in low and middle frequency elements using different column wavelet transforms](image)
Figure 15 Comparison of MAE between embedded and extracted watermark against resizing attack when watermark is embedded in low and middle frequency elements using different row wavelet transforms

As can be seen from Figure 14 and Figure 15, different column and row wavelet transforms perform very well against bicubic interpolation based resizing attack when singular values of low frequency region of host are selected for embedding watermark. Except column DCT wavelet, other wavelet transforms also show very good robustness against bicubic interpolation attack when singular values of middle frequency region are used to embed the watermark. Also against transform based resizing and grid based resizing attack, irrespective of low or middle frequency region and transform used for embedding watermark, zero MAE is obtained between embedded and extracted watermark thus leading to excellent robustness.

Performance of proposed method against various attacks is summarized in the Figure 16. Yellow color of a node in the hierarchy indicates excellent performance, Pink indicates very good robustness and orange color indicates good robustness.

Figure 16 Summarized performance of proposed watermarking technique against various attacks (Yellow=Excellent, Pink=Very Good, Orange=Good)

6 Conclusion

Proposed method of watermarking embeds singular values of watermark in singular values of column wavelet or row wavelet transform of host. Watermarked image is subjected to different attacks and watermark is extracted from it. Selection of low frequency band proves to be robust for attacks except cropping attack. Proposed method allows embedding watermark in low frequency
Advances in Image and Video Processing Volume 2, Issue 6, December 2014

region which otherwise leads to heavy distortion in watermarked image. Robustness of technique where watermark is embedded in middle frequency band is also acceptable but it is not as good as lower frequency bands.

REFERENCES


