ROBUST DCT-SVD DOMAIN IMAGE WATERMARKING FOR COPYRIGHT PROTECTION: EMBEDDING DATA IN ALL FREQUENCIES

Alexander Sverdlov
The Graduate Center
The City University of New York
365 Fifth Avenue, NY, NY 10016
Tel: 212-817-8190
sverdlov@sci.brooklyn.cuny.edu

Scott Dexter
Department of CIS, Brooklyn College
2900 Bedford Avenue
Brooklyn, NY 11210
Tel: 718-951-3125
sdexter@sci.brooklyn.cuny.edu

Ahmet M. Eskicioglu
Department of CIS, Brooklyn College
2900 Bedford Avenue
Brooklyn, NY 11210
Tel: 718-758-8481
eskicioglu@sci.brooklyn.cuny.edu

ABSTRACT

Both Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) have been used as mathematical tools for embedding data into an image. In this paper, we present a new robust hybrid watermarking scheme based on DCT and SVD. After applying the DCT to the cover image, we map the DCT coefficients in a zig-zag order into four quadrants, and apply the SVD to each quadrant. These four quadrants represent frequency bands from the lowest to the highest. The singular values in each quadrant are then modified by the singular values of the DCT-transformed visual watermark. We assume that the size of the visual watermark is one quarter of the size of the cover image. We show that embedding data in lowest frequencies is resilient to one set of attacks while embedding data in highest frequencies is resilient to another set of attacks. We compare our hybrid algorithm with a pure SVD-based scheme.

1. INTRODUCTION

Watermarking (data hiding) [1] is the process of embedding data into a multimedia element such as an image, audio or video file. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or a detection, algorithm. Watermarks can be embedded in the pixel domain or a transform domain. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. The approaches used in watermarking still images include least-significant bit encoding, basic M-sequence, transform techniques, and image-adaptive techniques.

In the classification of watermarking schemes, an important criterion is the type of information needed by the detector:

- Non-blind schemes require both the original image and the secret key(s) for watermark embedding.
- Semi-blind schemes require the secret key(s) and the watermark bit sequence.
- Blind schemes require only the secret key(s).

The most important uses of watermarks include copyright protection (identification of the origin of content, tracing illegally distributed copies) and disabling unauthorized access to content. The requirements for digital watermarks in these scenarios are different, in general. Identification of the origin of content requires the embedding of a single watermark into the content at the source of distribution. To trace illegal copies, a unique watermark is needed based on the location or identity of the recipient in the multimedia network. In both of these applications, non-blind schemes are appropriate as watermark extraction or detection needs to take place in a special laboratory environment only when there is a dispute regarding the ownership of content. For access control, the watermark should be checked in every authorized consumer device, thus requiring semi-blind or blind schemes. Note that the cost of a watermarking system will depend on the intended use, and may vary considerably.

Two widely used image compression standards are JPEG and JPEG 2000. The former is based on the Discrete Cosine Transform (DCT), and the latter the Discrete Wavelet Transform (DWT). In recent years, many watermarking schemes have been developed using these popular transforms.

In all frequency domain watermarking schemes, there is a conflict between robustness and transparency. If the watermark is embedded in perceptually most significant components, the scheme would be robust to attacks but the watermark may be difficult to hide. On the other hand, if the watermark is embedded in perceptually insignificant components, it would be easier to hide the watermark but the scheme may be less resilient to attacks.

In image watermarking, two distinct approaches have been used to represent the watermark. In the first approach, the watermark is generally represented as a sequence of randomly generated real numbers having a normal distribution with zero mean and unity variance. This type of watermark allows the detector to statistically check the presence or absence of the embedded watermark. In the second approach, a picture representing a company logo or other copyright information is embedded in the cover image. The detector actually reconstructs the watermark, and computes its visual quality using an appropriate measure.

A few years ago, a third transform called the Singular Value Decomposition (SVD) was explored for watermarking [2]. The SVD for square matrices was discovered independently by Beltrami in 1873 and Jordan in 1874, and extended to rectangular matrices by Eckart and Young in the 1930s. It was not used as a computational tool until the 1960s because of the need for sophisticated numerical techniques. In later years, Gene Golub demonstrated its usefulness and feasibility as a tool in a variety of applications [3]. SVD is one of the most useful tools of linear algebra with several applications in image compression, and other signal processing fields.

A recent paper [4] on DWT-based multiple watermarking argues that embedding a visual watermark in both low and high valued coefficients results in a robust scheme for a wide range of attacks. Embedding in low valued coefficients increases the robustness with respect to attacks that have low pass characteristics like filtering, lossy compression and geometric distortions while making the scheme more sensitive to modifications of the image histogram, such as contrast/brightness adjustment, gamma correction, and histogram equalization. Watermarks embedded in middle and high valued coefficients are typically less robust to low-pass filtering, lossy compression, and small geometric deformations of the image but are highly resilient with respect to noise addition, and nonlinear deformations of the gray scale. Arguing that advantages and disadvantages of using both bands are complementary, the authors propose a new scheme where two different visual watermarks are embedded in one image. Both watermarks are 32x32 binary images; one contains the letters CO, and the other EP against a white background. The cover image is 128x128 hetu.tif. Two levels of decomposition are performed on the cover image. The watermark CO is embedded in the second level LL, and the watermark EP is embedded in the second level HH. The experiments show that embedding in the LL subband is robust against JPEG compression, wiener filtering, Gaussian noise, scaling, and cropping while embedding in the HH subband is robust against histogram equalization, intensity adjustment, and gamma correction. In their implementation, the authors have used a scaling factor of 0.1 without considering the difference between the magnitudes of coefficients in the two bands. This results in visible degradation in all parts of the cover image, reducing the commercial value of the image.

In this paper, we generalize the above scheme to four subbands using DCT-SVD watermarking. An earlier work used the same idea in the DWT-SVD domain [5].

2. DCT-SVD DOMAIN WATERMARKING

The process of separating the image into bands using the DWT is well-defined. In two-dimensional DWT, each level of decomposition produces four bands of data denoted by LL, HL, LH, and HH. The LL subband can further be decomposed to obtain another level of decomposition.

In two-dimensional DCT, we apply the transformation to the whole image but need to map the frequency coefficients from the lowest to the highest in a zig-zag order to 4 quadrants in order to apply SVD to each block. All the quadrants will have the same number of DCT coefficients. For example, if the cover image is 512x512, the number of DCT coefficients in each block will be 65,536. To differentiate these blocks from the DWT bands, we will label them B1, B2, B3, B4. This process is depicted in Figure 1.

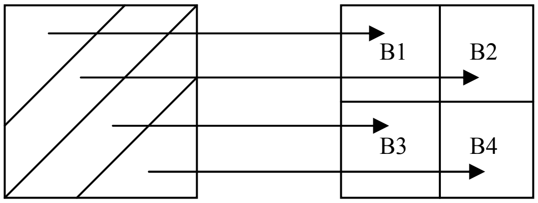


Figure 1. Mapping of DCT coefficients into 4 blocks

In pure DCT-based watermarking, the DCT coefficients are modified to embed the watermark data. Because of the conflict between robustness and transparency, the modification is usually made in middle frequencies, avoiding the lowest and highest bands.

Every real matrix A can be decomposed into a product of 3 matrices $A = U\Sigma V^T$, where U and V are orthogonal matrices, $U^TU = I$, $V^TV = I$, and Σ = diag (λ_1, λ_2, ...). The diagonal entries of Σ are called the singular values of A, the columns of U are called the left singular vectors of A, and the columns of V are called the right singular vectors of A. This decomposition is known as the *Singular Value Decomposition (SVD)* of A, and can be written as

$$A = \lambda_1 U_1 V_1^T + \lambda_2 U_2 V_2^T + \ldots + \lambda_r U_r V_r^T,$$

where r is the rank of matrix A. It is important to note that each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image.

In SVD-based watermarking, several approaches are possible. A common approach is to apply SVD to the whole cover image, and modify all the singular values to embed the watermark data. An important property of SVD-based watermarking is that the largest of the modified singular values change very little for most types of attacks.

We will combine DCT and SVD to develop a new hybrid non-blind image watermarking scheme that is resistant to a variety of attacks. The proposed scheme is given by the following algorithm. Assume the size of visual watermark is nxn, and the size of the cover image is $2n$x$2n$.

Watermark embedding:

1. Apply the DCT to the whole cover image A.
2. Using the zig-zag sequence, map the DCT coefficients into 4 quadrants: B1, B2, B3, and B4.
3. Apply SVD to each quadrant: $A^k = U_A^k \Sigma_A^k V_A^{kT}$, k = 1,2,3,4, where k denotes B1, B2, B3, and B4 quadrants.
4. Apply DCT to the whole visual watermark W.
5. Apply SVD to the DCT-transformed visual watermark W: $W = U_W \Sigma_W V_W^T$.
6. Modify the singular values in each quadrant Bk, k = 1,2,3,4, with the singular values of the DCT-transformed visual watermark: $\lambda_i^{*k} = \lambda_i^k + \alpha_k \lambda_{wi}, i$ = 1,…,n, where λ_i^k, i=1,…,n are the singular values of Σ_A^k, and λ_{wi}, i = 1,…,n are the singular values of Σ_W .
7. Obtain the 4 sets of modified DCT coefficients: $A^{*k} = U_A^k \Sigma_A^{*k} V_A^{kT}$, k = 1,2,3,4.
8. Map the modified DCT coefficients back to their original positions.
9. Apply the inverse DCT to produce the watermarked cover image.

Watermark extraction:

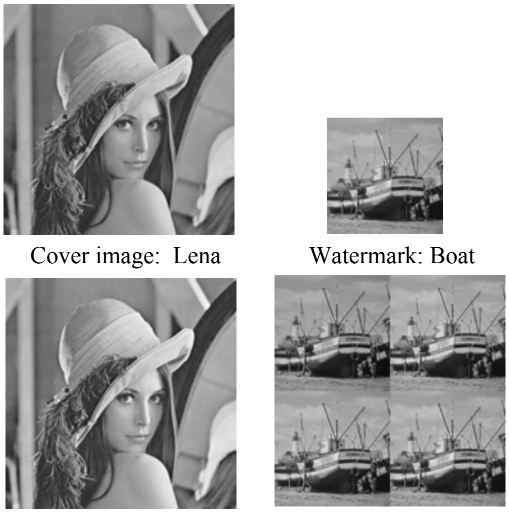
1. Apply the DCT to the whole watermarked (and possibly attacked) cover image A^*.
2. Using the zig-zag sequence, map the DCT coefficients into 4 quadrants: B1, B2, B3, and B4.
3. Apply SVD to each quadrant: $A^{*k} = U_A^k \Sigma_A^{*k} V_A^{kT}$, k = 1,2,3,4, where k denotes the attacked quadrants.
4. Extract the singular values from each quadrant Bk, k = 1,2,3,4: $\lambda_{wi}^k = (\lambda_i^{*k} - \lambda_i^k) / \alpha_k$, , $i = 1,\ldots,n$.
5. Construct the DCT coefficients of the four visual watermarks using the singular vectors:
   $W^k = U_W^k \Sigma_W^k V_W^{kT}$, k = 1,2,3,4.
6. Apply the inverse DCT to each set to construct the four visual watermarks.

The DCT coefficients with the highest magnitudes are found in quadrant B1, and those with the lowest magnitudes are found in quadrant B4. Correspondingly, the singular values with the highest values are in quadrant B1, and the singular values with the lowest values are in quadrant B4.

The largest singular values in quadrants B2, B3, and B4 have the same order of magnitude. So, instead of assigning a different scaling factor for each quadrant, we used only two values: One value for B1, and a smaller value for the other three quadrants.

3. EXPERIMENTS

Figure 2 shows the 512x512 gray scale cover image Lena, the 256X256 gray scale visual watermark Boat, the watermarked cover image, and the visual watermarks constructed from the four quadrants. In the experiments, we used the scaling factor 0.25 for B1, and 0.01 for the other three quadrants.



Cover image: Lena

Watermark: Boat

Watermarked Lena

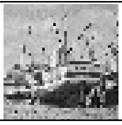
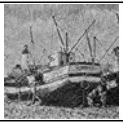
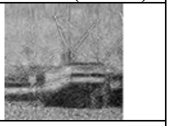
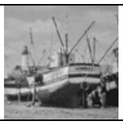
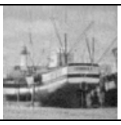
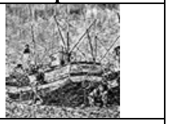
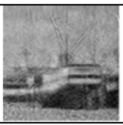
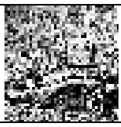
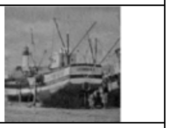
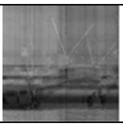
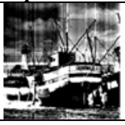
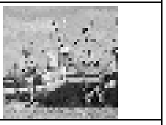
Extracted Watermarks

Figure 2. Watermark embedding/extraction

The DCT-SVD based watermarking scheme was tested using twelve attacks with Matlab: Gaussian blur, Gaussian noise, pixelation, JPEG compression, JPEG 2000 compression, sharpening, rescaling, rotation, cropping, contrast adjustment, histogram equalization, and gamma correction. Table 1 shows the best quality watermarks extracted from the 4 bands together with the Matlab parameters. The numbers below the images indicate the Pearson product moment correlation between the original vector of singular values and extracted vector of singular values for each quadrant. The Pearson product moment correlation coefficient is a dimensionless index that ranges from -1.0 to 1.0, and reflects the extent of a linear relationship between two data sets. The observer is also able to evaluate the quality of constructed watermarks subjectively through a visual comparison with the reference watermark.

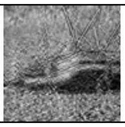
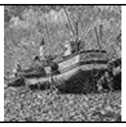
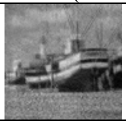
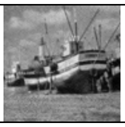
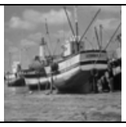
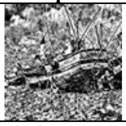
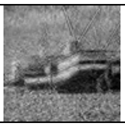
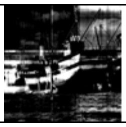
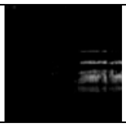
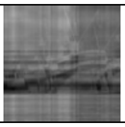
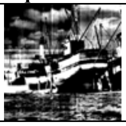
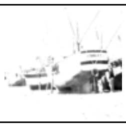
In watermark extraction, the singular values of the original image are subtracted from the singular values of the watermarked image. If the difference is negative for the largest singular values, the constructed visual watermark looks like a negative film (i.e., lighter parts of the image become darker, and darker parts become lighter). This is actually indicated consistently by the Pearson correlation coefficients in all 12 experiments as the computed value ranges from 1 to -1.

Table 1. Constructed watermarks with best quality

Gaussian Blur 5x5	**Gaussian Noise 0.3**	**Pixelate 2 (mosaic)**
		
0.9894 (B1)	0.9942 (B1)	0.9939 (B1)
JPEG 30:1	**JPEG 2000 50:1**	**Sharpen 80**
		
0.9998 (B1)	0.9994 (B1)	0.9275 (B1)
Rescale 512→256→512	**Rotate 20^0**	**Crop on both sides**
		
0.9957 (B1)	0.7617 (B2)	0.9990 (B4)
Contrast -20	**Histogram Equalization**	**Gamma Correction 0.60**
		
0.9941 (B4)	0.9148 (B4)	0.9993 (B4)

We now compare our results with those obtained from a pure SVD-based watermarking scheme. In this comparison, the 256x256 grayscale Lena is the cover image. We modified the 256 singular values of Lena with the 256 singular values of Boat, using the same scheme used in each quadrant above. The value of the scaling factor was 0.1. The constructed watermarks after the twelve attacks are given in Table 2. A comparison of Tables 1 and 2 indicates that the proposed watermarking scheme is superior. Note that the visual quality of all images in Table 2 is relatively worse both subjectively and objectively. In particular, the watermarks constructed after some attacks (e.g., rotation, cropping, and histogram equalization) have an extremely poor visual quality, making the pure SVD-based approach very unreliable.

Table 2. Constructed watermarks using pure SVD-based scheme

Gaussian Blur 5x5	**Gaussian Noise 0.3**	**Pixelate 2 (mosaic)**
		
0.9308	0.9120	0.9900
JPEG 30:1	**JPEG 2000 50:1**	**Sharpen 80**
		
0.9921	0.9991	0.6716
Rescale 256→128→256	**Rotate 20^0**	**Crop on both sides**
		
0.9711	0.1885	-0.9278
Contrast -20	**Histogram Equalization**	**Gamma Correction 0.60**
		
0.9335	0.4785	0.9983

4. CONCLUSIONS

Our observations regarding the proposed watermarking scheme can be summarized as follows:

- The scaling factor can be chosen from a fairly wide range of values for B1, and also for the other three quadrants. As quadrant B1 contains the largest DCT coefficients, the scaling factor is chosen accordingly. When the scaling factor for B1 is raised to an unreasonable value, the image brightness becomes higher while an increase in the scaling factor for the other quadrants results in diagonal artifacts that are visible especially in low frequency areas.
- In most DCT-based watermarking schemes, the lowest frequency coefficients are not modified as it is argued that watermark transparency would be lost. In the DCT-SVD based approach, we experienced no problem in modifying the coefficients in quadrant B1.
- Watermarks inserted in the lowest frequencies (B1) are resistant to one group of attacks, and watermarks embedded in highest frequencies (B4) are resistant to another group of attacks. The only exception is the rotation attack for which the data embedded in middle frequencies survives better. With different angles, the results may be different. If the same watermark is embedded in 4 quadrants, it would be extremely difficult to remove or destroy the watermark from all frequencies.
- A comparison of the hybrid DCT-SVD watermarking scheme with a pure SVD based algorithm shows that the proposed scheme performs much better, providing more robustness and reliability.
- One advantage of SVD-based watermarking is that there is no need to embed all the singular values of a visual watermark. Depending on the magnitudes of the largest singular values, it would be sufficient to embed only a small set. This SVD property has in fact been exploited to develop algorithms for lossy image compression.
- Observers can evaluate the quality of constructed watermarks either subjectively or objectively. In subjective evaluation, the reference watermark is compared with the watermark constructed after an attack. In objective evaluation, statistical measures like Pearson's correlation coefficient can be used, not requiring the singular vectors of the watermark image. For automatic watermark detection, the highest value of the correlation coefficient can be used to identify the quadrant with the highest resistance.
- Different measures can be used to show the similarity between the reference and the extracted singular values. An example of such a measure is $\Sigma W(i)W'(i)$/sqrt($\Sigma W'^2(i)$), where W is the vector of singular values of the reference watermark, and W' is the vector of extracted singular values.
- Experimentation with multiple images will enable a better understanding of the proposed watermarking scheme. As different images may have singular values with different magnitudes, what would be a general formula for determining the values of the scaling factor for each quadrant?
- In SVD watermarking, we embed singular values into singular values. Variations of this approach can be considered. For example, instead of embedding singular values, any other vector that represents some information may be used.
- In DWT-SVD domain watermarking [5], we obtained very similar results. Watermark embedding in the LL band (B1) is resistant to attacks including Gaussian blur, Gaussian noise, pixelation, JPEG compression, JPEG2000 compression, and rescaling. Watermark embedding in the HH band (B4) is resistant to attacks including sharpening, cropping, contrast adjustment, histogram equalization, and gamma correction. Watermark embedding in the LH band (B2) is resistant to the rotation attack. As in DCT-SVD domain watermarking, this is the only exception.

REFERENCES

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2002.

[2] R. Liu and T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership," *IEEE Transactions on Multimedia*, 4(1), March 2002, pp.121-128.

[3] D. Kahaner, C. Moler and S. Nash, *Numerical Methods and Software* (New Jersey: Prentice-Hall, Inc, 1989).

[4] R. Mehul and R. Priti, "Discrete Wavelet Transform Based Multiple Watermarking Scheme," *Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific*, Bangalore, India, October 14-17, 2003.

[5] E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," *ACM Multimedia and Security Workshop 2004, Magdeburg*, Germany, September 20-21, 2004.