Secure DCT-SVD Domain Image Watermarking: 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 the DCT-domain, the DCT coefficients are modified by the elements of a pseudo-random sequence of real values. In the SVD domain, a common approach is to modify the singular values by the singular values of a visual watermark. In this paper, we present a new robust hybrid watermarking schemes 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. Modification in all frequencies enables a watermarking scheme that is robust to normal A/V processes or intentional attacks that destroy the watermark in either lower or higher frequencies. We show that embedding data in lowest frequencies is resistant to one set of attacks while embedding data in highest frequencies is resistant to another set of attacks. The only exception is the rotation attack for which the data embedded in middle frequencies survive better.

Categories and Subject Descriptors

K.4.4 [Computers and Society]: Electronic Commerce - c*ybercash, digital cash, distributed commercial transactions, electronic data interchange (EDI), intellectual property, payment schemes, security.*

General Terms

Security

Keywords

copyright protection, discrete cosine transform, image watermarking, multimedia, singular value decomposition.

1. INTRODUCTION

Watermarking (data hiding) [1,2,3] is the process of embedding data into a multimedia element such as image, audio or video. 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 [4]. Invisibility refers to the degree of distortion introduced by the watermark and its affect on the viewers or listeners. Robustness is the resistance of an embedded watermark against intentional attacks, and normal A/V processes such as noise, filtering (blurring, sharpening, etc.), resampling, scaling, rotation, cropping, and lossy compression. Capacity is the amount of data that can be represented by an embedded watermark. The approaches used in watermarking still images include least-significant bit encoding, basic M-sequence, transform techniques, and image-adaptive techniques [5].

Typical uses of watermarks include copyright protection (identification of the origin of content, tracing illegally distributed copies) and disabling unauthorized access to content. Requirements and characteristics for the 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, watermark extraction or detection needs to take place only when there is a dispute regarding the ownership of content. For access control, the watermark should be checked in every authorized consumer device used to receive the content. 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 JPEG2000. 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 resistant 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 [6,7,8,9,10]. In the second approach, a picture representing a company logo or other copyright information is embedded in the cover image [11,12,13,14,15,16].

A few years ago, a third transform called Singular Value Decomposition (SVD) was explored for watermarking. 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 [17]. SVD is one of the most useful tools of linear algebra with several applications in image compression [18,19,20,21,22,23], watermarking [14,15,16], and other signal processing fields [24,25,26,27].

A recent paper [28] on DWT-based multiple watermarking argues that embedding a visual watermark in both low and high frequencies results in a robust scheme that can resist to different kinds of attacks. Embedding in low frequencies 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 frequencies are typically less robust to low-pass filtering, lossy compression, and small geometric deformations of the image but are highly robust with respect to noise adding, and nonlinear deformations of the gray scale. Arguing that advantages and disadvantages of low and middle-to-high frequency watermarks are complementary, the authors propose a new scheme where two different visual watermarks are embedded in one image. Both watermarks are binary images, one contains the letters CO, and the other EP against a white background. The cover image is the picture of a young girl. 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. Extracted watermarks appear to have similar quality after the Gaussian noise attack only. We noticed that the embedded watermark is highly visible in all parts of the cover image. The degradation is pronounced especially in low frequency areas (e.g., the wall behind the young girl), resulting in a loss in the commercial value of the image.

In this paper, we generalize the above scheme to four subbands using DCT-SVD watermarking.

2. DCT-SVD DOMAIN WATERMARKING

The process of separating the frequency 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.

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.

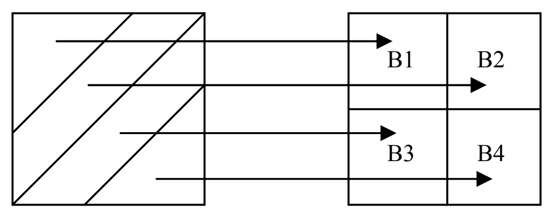


Figure 1. Mapping of DCT coefficients into 4 blocks

Every real matrix A can be decomposed into a product of 3 matrices $A = U\Sigma VT$, where U and V are orthogonal matrices, $UTU = I$, $VTV = I$, and $\Sigma = \text{diag}(\lambda_1, \lambda_2, ...)$. 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

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

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.

In this paper, we will combine DCT and SVD to develop a new hybrid 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:

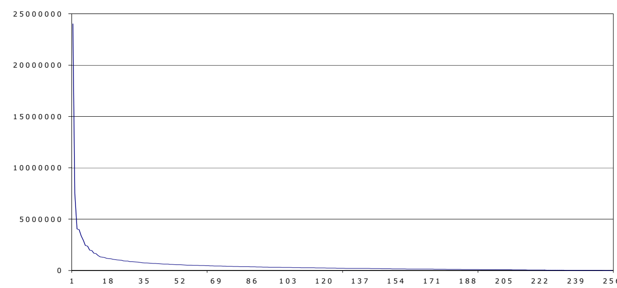
1. Apply the DCT to the whole cover image A.
2. Using the zig-zag sequence, map the DCT coefficients into 4 quadrants: B1, B2, B3, and B4.
3. Apply SVD to each quadrant: $A^k_{DCT} = U^k_{a_{DCT}} \Sigma^k_{a_{DCT}} V^{kT}_{a_{DCT}}$, k = 1,2,3,4, where k denotes B1, B2, B3, and B4 quadrants, and λ_i^k, $i = 1,\ldots,n$ are the singular values of $\Sigma^k_{a_{DCT}}$.
4. Apply DCT to the whole visual watermark W.
5. Apply SVD to the DCT-transformed visual watermark W_{DCT}: $W_{DCT} = U_{w_{DCT}} \Sigma_{w_{DCT}} V^T_{w_{DCT}}$, where λ_{wi}, $i = 1,\ldots,n$ are the singular values of $\Sigma_{w_{DCT}}$.
6. Modify the singular values in each quadrant Bk, k = 1,2,3,4, with the singular values of the DCT-transformed visual watermark: $\lambda_i^{*k} = \lambda_i^k + \alpha_k \lambda_{wi}$, $i = 1,\ldots,n$.
7. Obtain the 4 sets of modified DCT coefficients: $A^{*k}_{DCT} = U^k_{a_{DCT}} \Sigma^{*k}_{a_{DCT}} V^{kT}_{a_{DCT}}$, 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:

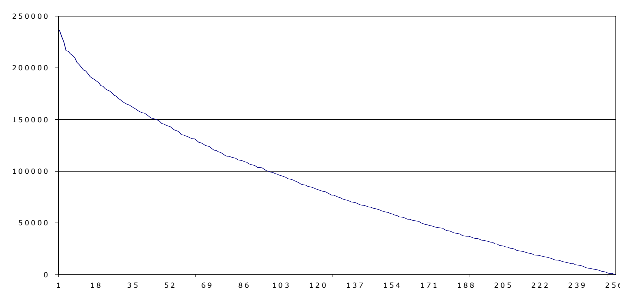
1. Apply the DCT to the whole watermarked (and possibly attacked) cover image A^*.
2. Using the zig-zag sequence, map the DCT coefficients into 4 quadrants: B1, B2, B3, and B4.
3. Apply SVD to each quadrant: $A^{*k} = U^k_a \Sigma^{*k}_a V^{kT}_a$, k = 1,2,3,4, where k denotes the attacked quadrants.
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:
$$W^k_{DCT} = U^k_{w_{DCT}} \Sigma^k_{w_{DCT}} V^{kT}_{w_{DCT}}, \; k = 1,2,3,4.$$
6. Apply the inverse DCT to each set to construct the four visual watermarks.

The magnitudes of the singular values for each quadrant of the cover image Lena used in our experiments are given in Table 1. The DCT coefficients with the highest magnitude are found in the B1 quadrant, and those with the lowest coefficients are found in the B4 quadrant. Correspondingly, the singular values with the highest magnitudes are in the B1 quadrant, and the singular values with the lowest magnitudes are in the B4 quadrant.

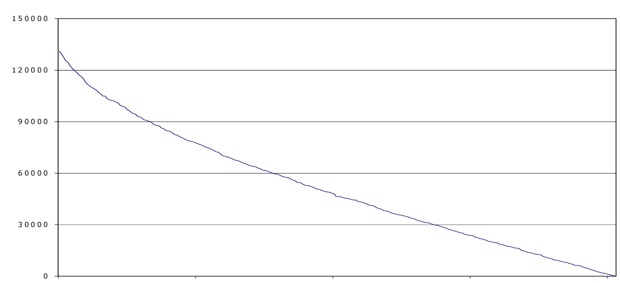
Table 1. Singular values of transformed Lena in 4 quadrants



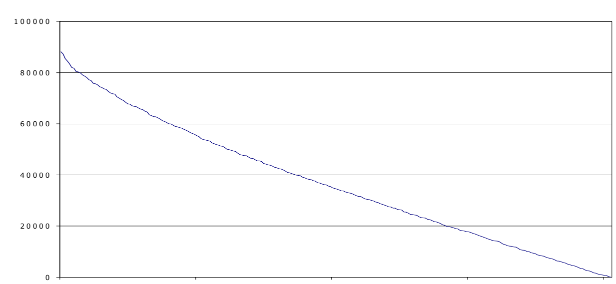
(a) B1



(b) B2



(c) B3



(d) B4

We also computed the largest singular values of the DCT coefficients in the four quadrants for six other common test images. They are given in Table 2 together with Lena's. The general trend is a decrease in their magnitudes as we go from the B1 quadrant to the B4 quadrant. The magnitudes of the largest singular values in the B2, B3, and B4 quadrants have the same order of magnitude. So, instead of assigning a different scaling factor for each quadrant, we decided to use only two values: One value for B1, and a smaller value for the other three quadrants.

Table 2. Largest singular values in 4 quadrants

Image/ Quadrant	B1	B2	B3	B4
Mandrill	18,478,800	820,423	556,3534	380,236
Lena	24,019,900	236,304	130,947	88,132
Barbara	29,737,800	893,738	635,670	199,455
Boat	32,007,000	377,477	166,474	89,828
Goldhill	35,067,000	339,540	228,007	114,731
Peppers	37,421,400	259,615	174,685	248,779
Airplane	57,248,500	291,741	118,816	65,230

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.

The DCT-SVD based watermarking scheme was tested using twelve attacks. The DCT was performed using the FFTW library [29], and the SVD was performed using an implementation of the CLAPACK library for MacOS 10.3 [30]. The chosen attacks were Gaussian blur, Gaussian noise, pixelation, JPEG compression, JPEG 2000 compression, sharpening, rescaling, rotation, cropping, contrast adjustment, histogram equalization, and gamma correction.

The attacked images are presented in Figure 3 together with the tools and parameters used for the attacks.

Cover image: Lena

Watermark: Boat

Watermarked Lena

Extracted Watermarks

Figure 2. Watermark embedding/extraction

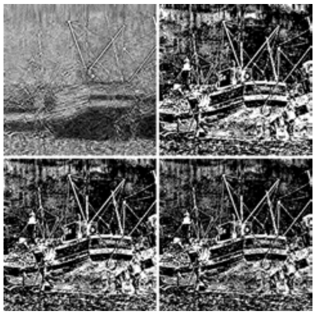
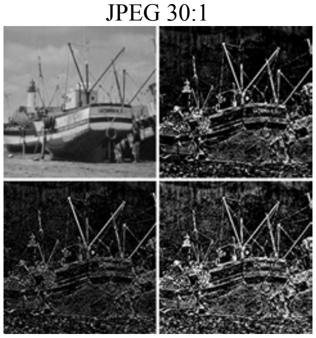
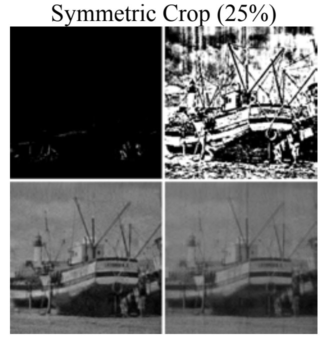
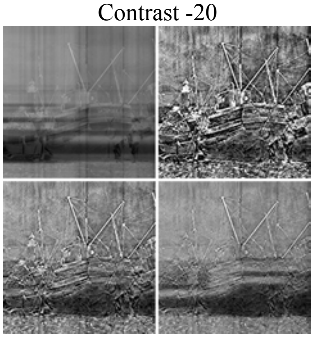
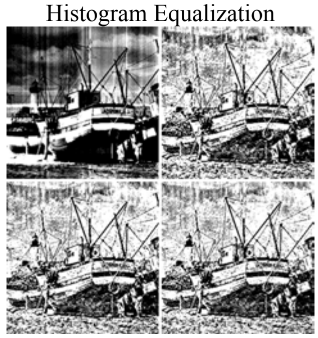
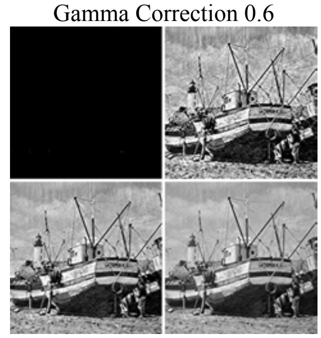
Table 3 includes the constructed watermarks from all quadrants for a given attack. The numbers below the images indicate the Pearson product moment correlation between the original vector of singular values and extracted vector of singular values for each quadrant. The Pearson product moment correlation 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. Negative coefficients imply that the singular values are very much different from those of the reference watermark. The observer is able to evaluate the quality of constructed watermarks subjectively through a visual comparison with the reference watermark. The other alternative is to correlate the extracted singular values with those of the reference watermark using the correlation coefficient.

According to Table 3, the watermarks constructed from the four quadrants look different for each attack. It is possible to classify the attacks into three groups:

1. Watermark embedding in the B1 quadrant is resistant to Gaussian blur, Gaussian noise, pixelation, JPEG compression, JPEG2000 compression, sharpening, and rescaling.
2. Watermark embedding in the B4 quadrant is resistant to, cropping, contrast adjustment, histogram equalization, and gamma correction.
3. Watermark embedding in the B2 quadrant is resistant to rotation.

Figure 3. Attacked Watermarked Images.

Table 3. Extracted Watermarks

Gaussian Blur 5x5  0.9894 -0.2173 -0.2261 -0.2136	Gaussian Noise 0.3  0.9942 0.2318 0.2199 0.2083	Pixelate 2  0.9939 0.3629 0.4833 -0.2035
JPEG 30:1  0.9998 -0.2662 -0.0874 -0.1036	JPEG2000 50:1  0.9994 -0.1568 0.0437 -0.1852	Sharpen 80  0.9275 0.5974 0.7303 0.8117
Rescale 512→256→512  0.9957 -0.2114 -0.0450 -0.1458	Rotate 20º  -0.8977 0.7617 0.6095 0.4426	Symmetric Crop (25%)  -0.9813 0.4790 0.9990 0.9990
Contrast -20  0.9883 0.9687 0.9845 0.9941	Histogram Equalization  0.5870 0.8045 0.8800 0.9148	Gamma Correction 0.6  -0.9857 0.9918 0.9975 0.9993

4. CONCLUSIONS

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

- SVD is a very convenient tool for watermarking in the DCT domain. We observed that the scaling factor can be chosen from a fairly wide range of values for B1, and also for the other three quadrants. As the B1 quadrant 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 contrast 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 B1 quadrant.

- Watermarks inserted in the lowest frequencies (B1 quadrant) are resistant to one group of attacks, and watermarks embedded in highest frequencies (B4 quadrant) are resistant to another group of attacks. If the same watermark is embedded in 4 blocks, it would be extremely difficult to remove or destroy the watermark from all frequencies.

- In some cases, embedding in the B2 and B3 quadrants is also resistant to certain attacks. Two examples of those attacks are histogram equalization and gamma correction. After the cropping attack, singular value extraction in the B3 and B4 quadrants produce almost identical results (as displayed by visual quality and correlation coefficient).

- 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.

In future research, our investigation will include different similarity measures, multiple images, and different watermark representations:

- Different measures can be used to show the similarity between the reference and the extracted singular values. Two examples of such a measure are

$$\sum_i W(i)\hat{W}(i) \Big/ \sqrt{\sum_i \hat{W}^2(i)}, \text{ and}$$

$$\sum_i W(i)\hat{W}(i) \Big/ \sqrt{\sum_i W^2(i)}\sqrt{\sum_i \hat{W}^2(i)},$$

  where W is the vector of singular values of the reference watermark, and $\hat{W}$ 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.

3. ACKNOWLEDGMENTS

Our thanks to Mr. Emir Ganic for the image input/output code that was used in this work.

4. REFERENCES

[1] C. I. Podilchuk and E. J. Delp, "Digital Watermarking: Algorithms and Applications," *IEEE Signal Processing Magazine*, July 2001, pp. 33-46.

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

[3] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk and E. J. Delp, "Advances in Digital Video Content Protection," *Proceedings of the IEEE, Special Issue on Advances in Video Coding and Delivery*, 2004.

[4] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proceedings of the IEEE*, Vol. 87, No. 7, July 1999, pp. 1079-1107.

[5] R. B. Wolfgang, C. I. Podilchuk and E. J. Delp, "Perceptual Watermarks for Digital Images and Video," *Proceedings of the IEEE*, Vol. 87, No. 7, July 1999, pp. 1108-1126.

[6] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, 6(12), December 1997, pp. 1673-1687.

[7] X.-G. Xia, C. G. Boncelet and G. R. Arce, "A Multiresolution Watermark for Digital Images," *Proceedings of the 1997 International Conference on Image Processing*, Washington, DC, October 26-29, 1997.

[8] M. Barni, F. Bartolini, V. Cappellini, A. Piva, "A DCT-Domain System for Robust Image Watermarking," *Signal Processing*, Volume 66, No. 3, May 1998, pp. 357-372.

[9] W. Zhu, Z. Xiong and Y.-Q. Zhang, "Multiresolution Watermarking for Images and Video," *IEEE Transactions on Circuits and Systems for Video Technology*, Volume 9, No. 4, June 1999, pp. 545-550.

[10] V. Fotopoulos and A. N. Skodras, "A Subband DCT Approach to Image Watermarking," *Proceedings of X European Signal Processing Conference*, Tampere, Finland, September 4 - 8, 2000.

[11] J. J. Chae and B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients," *Proceedings of the SPIE International Conference on Storage and Retrieval for Image and Video Databases VI*, San Jose, CA, January 28-30, 1998, Vol. 3312, pp. 308-317.

[12] S. D. Lin and C.-F. Chen, "A Robust DCT-Based Watermarking for Copyright Protection," *IEEE Transactions on Consumer Electronics*, Volume 46, No. 3, August 2000, pp. 415-421.

[13] Y. Wang, J. F. Doherty and R. E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images," *IEEE Transactions on Image Processing*, Volume 11, No. 2, February 2002, pp. 77-88.

[14] V. I. Gorodetski, L. J. Popyack, V. Samoilov and V. A. Skormin, "SVD-based Approach to Transparent Embedding Data into Digital Images," *International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2001)*, St. Petersbug, Russia, May 21-23, 2001.

[15] D. V. S. Chandra, "Digital Image Watermarking Using Singular Value Decomposition," *Proceedings of 45th IEEE Midwest Symposium on Circuits and Systems*, Tulsa, OK, August 2002, pp. 264-267.

[16] 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.

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

[18] H. C. Andrews and C. L. Patterson, "Singular Value Decomposition (SVD) Image Coding," *IEEE Transactions on Communications*, 24(4), April 1976, pp. 425-432.

[19] N. Garguir, "Comparative Performance of SVD and Adaptive Cosine Transform in Coding Images," *IEEE Transactions on Communication*s, 27(8), August 1979, pp. 1230-1234.

[20] D. P. O'Leary and S. Peleg, "Digital Image Compression by Outer Product Expansion," *IEEE Transactions on Communications*, 31(3), March 1983, pp. 441-444.

[21] J. F. Yang and C. L. Lu, "Combined Techniques of Singular Value Decomposition and Vector Quantization," *IEEE Transactions on Image Processing*, 4(8), August 1995, pp. 1141-1146.

[22] P. Waldemar and T. A. Ramstad, "Hybrid KLT-SVD Image Compression," *1997 IEEE International Conference on Acoustics, Speech and Signal Processing*, Vol. 4, Munich, Germany, April 21-24, 1997, pp. 2713-2716.

[23] S. O. Aase, J. H. Husoy and P. Waldemar, "A Critique of SVD-Based Image Coding Systems," *1999 IEEE International Symposium on Circuits and Systems VLSI*, Vol. 4, Orlando, FL, May 1999, pp. 13-16.

[24] K. Konstantinides and G. S. Yovanof, "Improved Compression Performance Using SVD-Based Filters for Still Images," *SPIE Proceedings*, Vol. 2418, San Jose, CA, February 7-8, 1995, pp. 100-106.

[25] K. Konstantinides and G. S. Yovanof, "Application of SVD-Based Spatial Filtering to Video Sequences," *1995 IEEE International Conference on Acoustics, Speech and Signal Processing*, Vol. 4, Detroit, MI, May 9-12, 1995, pp. 2193-2196.

[26] K. Konstantinides, B. Natarajan and G. S. Yovanof, "Noise Estimation and Filtering Using Block-Based Singular Value Decomposition," *IEEE Transactions on Image Processing*, 3(3), March 1997, pp. 479-483.

[27] R. Karkarala and P. O. Ogunbona, "Signal Analysis Using a Multiresolution Form of the Singular Value Decomposition," *IEEE Transactions on Image Processing*, 10(5), May 2001, pp. 724-735.

[28] 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.

[29] M. Frigo and S. G. Johnson, "FFTW: An Adaptive Software Architecture for the FFT," *Proceedings of 1998 IEEE International Conference on Acoustics Speech and Signal Processing*," Vol. 3, Seattle, WA, May 12-15, 1998, pp. 1381-1384.

[30] http://developer.apple.com/hardware/ve