A Noval technique for image Steganography using DWT & SVD

Mr. Praful Devaliya[1] Prof. Ashish Nimavat[2] Prof. Janak Tank [3]
[1] M.E. Student [2,3]Professor
[1,2] C.U.Shah College of Engineering [3]L.D.R.P. Institutes of Tech, & Research KSV, Gandhinagar.

Abstract**—** Protection of digital multimedia content has become an increasingly important issue for content owners and service providers. As watermarking is identified as a major technology to achieve copyright protection, the relevant literature includes several distinct approaches for embedding data into a multimedia element (primarily images, audio, and video). Because of its growing popularity, the Discrete Wavelet Transform (DWT) is commonly used in recent 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 scheme based on DWT and Singular Value Decomposition (SVD). After decomposing the cover image into four bands, we apply the SVD to each band, and embed the same watermark data by modifying the singular values. Modification in all frequencies allows the development of a watermarking scheme that is robust to a wide range of attacks.

Keywords— Electronic Commerce - cybercash, digital cash, distributed commercial transactions, electronic data interchange (EDI), intellectual property, payment schemes, security, Multimedia, Copyright, Protection, Image Watermarking, Discrete Wavelet Transform, Singular Value Decomposition, Visual Watermark.

I. 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].

An important criterion for classifying watermarking schemes is the type of information needed by the detector:

- Non-blind schemes: Both the original image and the secret key(s) for watermark embedding.
- Semi-blind schemes: The secret key(s) and the watermark bit sequence.
- Blind schemes: Only the secret key(s).

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, 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 used to receive the content, 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 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 least 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]. 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 [11,12,13,14,15,16]. The detector actually reconstructs the watermark, and computes its visual quality using an appropriate measure.

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 DWT-SVD watermarking.

II. DWT-SVD DOMAIN WATERMARKING

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. This process is continued until the desired number of levels determined by the application is reached. Figure 1 shows two levels of decomposition.

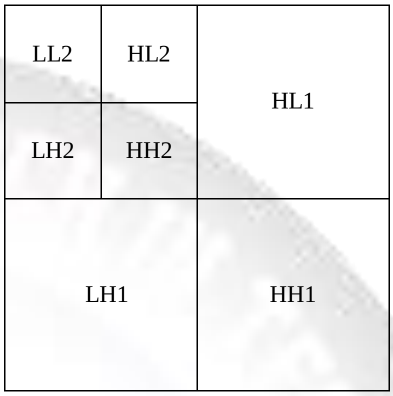

Fig. 1: DWT decomposition with two levels.

In DWT-based watermarking, the DWT coefficients are modified to embed the watermark data. Because of the conflict between robustness and transparency, the modification at a given level is usually made in HL, LH, and HH subbands.

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 $\Sigma = \text{diag}(\lambda_1, \lambda_2, \ldots)$. 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 layer.

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.

A theoretical analysis of the effects of ordinary geometric distortions on the singular values of an image is provided in a recent paper [29]:

- *Transpose*: A and its transpose A^T have the same non-zero singular values.
- *Flip*: A, row-flipped A_{rf}, and column-flipped A_{cf} have the same non-zero singular values.
- *Rotation*: A and A_r (A rotated by an arbitrary degree) have the same non-zero singular values.
- *Scaling*: B is a row-scaled version of A by repeating every row for L1 times. For each non-

zero singular value λ of A, B has $\sqrt{L1}$ λ. C is a column-scaled version of A by repeating every column for L_2 times. For each non-zero singular value λ of *A*, *C* has $\sqrt{L_2}\,\lambda$. If *D* is row-scaled by L_1 times, and column-scaled by L_2 times, for each non-zero singular value λ of *A*, *D* has $\sqrt{L1L2}\lambda$

– *Translation*: *A* is expanded by adding rows and columns of black pixels. The resulting matrix A_e has the same non-zero singular values as *A*.

Because of these properties, SVD may be used as a tool to develop semi-blind watermarking schemes.

In this paper, we will combine DWT 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 2*n*x2*n*.

A. *Watermark embedding:*

1. Using DWT, decompose the cover image *A* into 4 subbands: LL, HL, LH, and HH.
2. Apply SVD to each subband image: $A^k = U_a^k \Sigma_a^k V_a^{kT}$, $k = 1,2,3,4$, where *k* denotes LL, HL, LH, and HH bands, and λ_i^k, $i=1,\dots,n$ are the singular values of Σ_a^k.
3. Apply SVD to the visual watermark: $W = U_W \Sigma_W V_W^T$ where λ_{wi}, $i = 1,\dots,n$ are the singular values of Σ_W.
4. Modify the singular values of the cover image in each subband with the singular values of the visual watermark: $\lambda_i^{*k} = \lambda_i^k + \alpha_k \lambda_{wi}$, $i = 1,\dots,n$, and $k = 1,2,3,4$.
5. Obtain the 4 sets of modified DWT coefficients: $A^{*k} = U_a^k \Sigma_a^{*k} V_a^{kT}$, $k = 1,2,3,4$.

B. *Watermark extraction:*

1. Using DWT, decompose the watermarked (and possibly attacked) cover image A^* into 4 subbands: LL, HL, LH, and HH.
2. Apply SVD to each subband image: $A^{*k} = U_a^k \Sigma_a^{*k} V_a^{kT}$, $k = 1,2,3,4$, where *k* denotes the attacked LL, HL, LH, and HH bands.
3. Extract the singular values from each subband: $\lambda_{wi}^k = (\lambda_i^{*k} - \lambda_i^k)/\alpha_k$, $i = 1,\dots,n$, and $k = 1,2,3,4$.
4. Construct the four visual watermarks using the singular vectors: $W^k = U_W \Sigma_W^k V_W^T$, $k = 1,2,3,4$.

We computed the largest singular values in the four subbands for six common test images. They are given in Table 1. Although the general trend is a decrease in their magnitudes as we go from the LL subband to the HH subband, there are exceptions. So, instead of assigning a different scaling factor for each subband, we decided to use only two values: One value for LL, and a smaller value for the other three subbands.

Image / Subband	LL	HL	LH	HH
Peppers	54,464	1,750	1,326	272
Goldhill	60,779	1,042	450	193
Barbara	61,840	1,330	795	804
Lena	64,462	586	313	182
Boat	72,446	882	795	204
Airplane	92,047	1,782	1,862	175

Table. 1: Largest singular values for test image

The magnitudes of the singular values for each subband of the cover image Lena used in our experiments are given in Table 2. The wavelet coefficients with the highest magnitude are found inthe LL subband, and those with the lowest coefficients are found in the HH subband. Correspondingly, the singular values with the highest magnitudes are in the LL subband, and the singular values with the lowest magnitudes are in the HH subband.

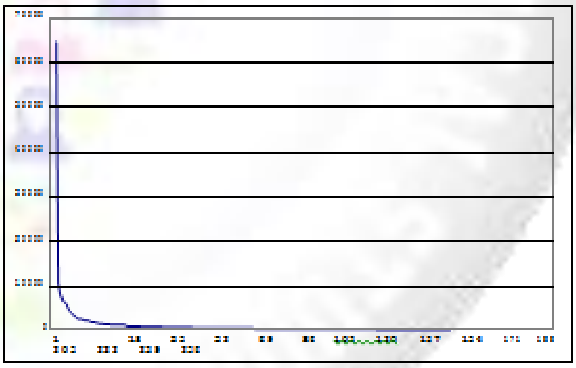

Fig. 2: Singular values LL subbands

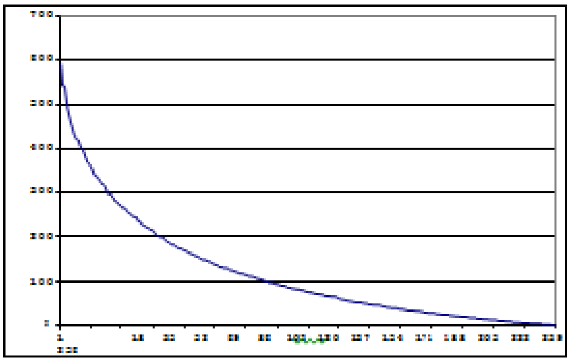

Fig. 3: Singular values HL subbands

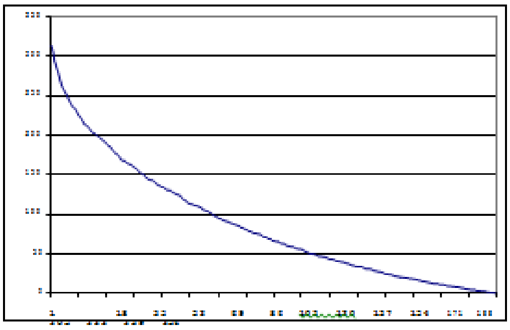

Fig. 4: Singular values LH subbands

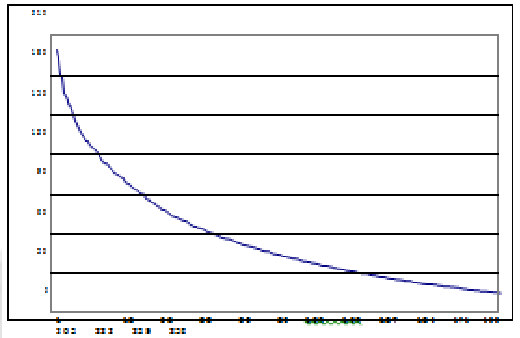

Fig. 5: Singular values HH subbands

III. EXPERIMENTS

Figure 6 shows the 512x512 gray scale cover image Lena, the 256X256 gray scale visual watermark Cameraman, the watermarked cover image, and the watermarks constructed from the four subbands. The scaling factor for the LL subband is 0.05, and the scaling factor for the other three subbands is 0.005.

The DWT-SVD based watermarking scheme was tested using twelve attacks. The DWT was performed using the Haar wavelet filter, and the SVD code was purchased from Numerical Recipes [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.

Watermarked Lena Constructed Watermarks

Fig. 6: Embedding a visual watermark into an image

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

Table 3 includes the constructed watermarks from all subbands for a given attack. The numbers below the images indicate the Pearson's correlation between the original vector of singular values and extracted vector of singular values. Ranging from +1 to -1, Pearson's correlation shows the degree of linear relationship between two variables. 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.

Fig. 3: Attacked images

According to Table 3, the watermarks constructed from the four subbands look different for each attack. Using the Pearson correlation coefficient as our criterion, it is possible to classify the attacks into three groups:

(1) Watermark embedding in the LL subband is resistant to attacks including Gaussian blur, Gaussian noise, pixelation, JPEG compression, JPEG2000 compression, and rescaling.

(2) Watermark embedding in the HH subband is resistant to attacks including sharpening, cropping, contrast adjustment, histogram equalization, and gamma correction.

(3) Watermark embedding in the LH subband is resistant to the rotation attack.

In watermark extraction, when 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, then the constructed visual watermark looks like a negative film (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.

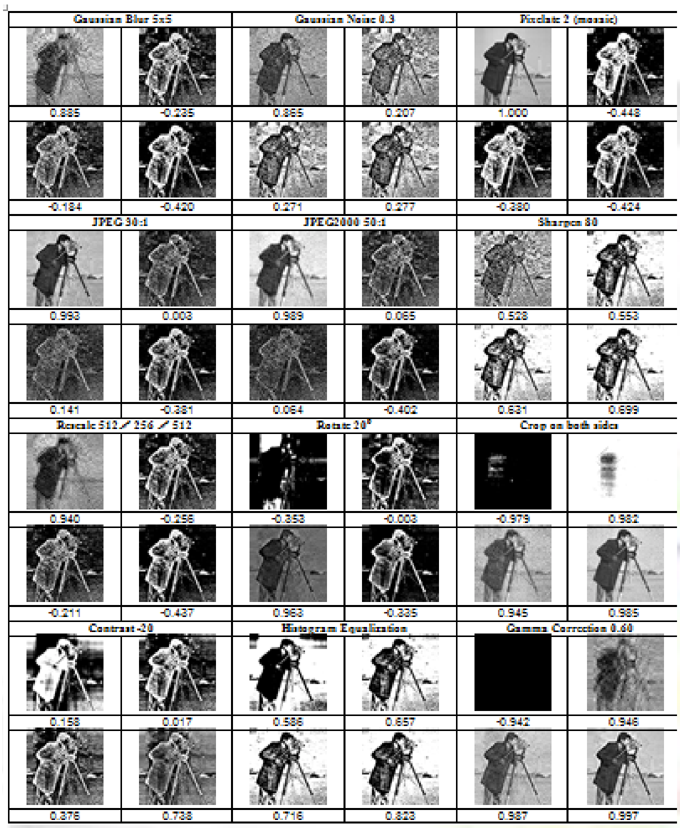

Table. 3: Constructed watermarks

We have used the same idea in the DCT-SVD domain, and obtained almost identical results [31]. After computing the DCT of the cover image, we map the DCT coefficients in a zig-zag order into four quadrants, and apply the SVD to each quadrant. The singular values in each quadrant are modified by the singular values of the DCT-transformed visual watermark.

IV. Conclusions

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

- SVD is a very convenient tool for watermarking in the DWT domain. We observed that the scaling factor can be chosen from a fairly wide range of values for LL, and also for the other three bands. As the LL band contains the largest wavelet coefficients, the scaling factor is chosen accordingly. We tried up to 0.5 for LL, and .01 for the other bands. For this pair of values, there was no degradation in the watermarked image. When the scaling factor for LL is increased to an unreasonable value, the image becomes lighter while an increase in the scaling factor for the other bands results in vertical and horizontal artifacts.
- In most DWT-based watermarking schemes, the LL band is not modified as it is argued that watermark transparency would be lost. In the DWT-SVD based approach, we experienced no problem in modifying the LL band.
- Watermarks inserted in the lowest frequencies (LL subband) are resistant to one group of attacks, and watermarks embedded in highest frequencies (HH subband) 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 HL and LH subbands 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 HL subband does not allow proper construction of the watermark although the correlation coefficient is high. We are currently investigating such exceptional irregularities.
- 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. In our experiments, we also used Mandrill as the visual watermark, and embedded its largest 256 singular values. Similar results were obtained in watermark extraction. This SVD property has 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 subband with the highest resistance.

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

- Different measures can be used to show the similarity between the reference and the extracted singular values. One example of such a measure is

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

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 levels of DWT decomposition will help us understand the best level for watermark embedding. Obviously, higher decompositions result in smaller blocks to embed the watermark.
- 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 subband?

- 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.

REFERENCES

[1] C. I. Podilchuk and E. J. Delp, "Digital Watermarking: Algorithms and Applications," *IEEE Signal Processing Magazine*, July 2011, pp. 33-46.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2012.

[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*, 2013.

[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 2011, 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 2013, 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, 2001

[8] M. Barni, F. Bartolini, V. Cappellini, A. Piva, "A DCT- Domain System for Robust Image Watermarking," *Signal Processing*, Volume 66, No. 3, May 2000, 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] 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.

[18] 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.

[19] B. Zhou and J. Chen, "A Geometric Distortion Resilient Image Watermarking Algorithm Based on SVD," *Chinese Journal of Image and Graphics*, Vol. 9, April 2004, pp. 506-512.

[20] http://www.nr.com

[21] A. Sverdlov, S. Dexter, and A. M. Eskicioglu, "Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in All Frequencies," submitted to Multimedia Computing and Networking 2005 Conference, San Jos.