DWT-DCT-SVD Based Watermarking

Navas K A[a], Ajay Mathews Cheriyan[b],Lekshmi.M[b], Archana Tampy.S[c], Sasikumar M[d]
[a]Asst Professor, [b]UG Student, [b]PG Student, [d]Professor (Retd.)
Electronics and Communication Engineering Dept.
College of Engineering Trivandrum
Kerala, India
kanavas@rediffmail.com

Abstract- Some works are reported in the frequency domain watermarking using Single Value Decomposition (SVD). The two most commonly used methods are based on DCT-SVD and DWT-SVD. The commonly present disadvantages in traditional watermarking techniques such as inability to withstand attacks are absent in SVD based algorithms. They offer a robust method of watermarking with minimum or no distortion. DCT based watermarking techniques offer compression while DWT based compression offer scalability. Thus all the three desirable properties can be utilized to create a new robust watermarking technique. In this paper, we propose a method of non-blind transform domain watermarking based on DWT-DCT-SVD. 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 only reasonable amount of distortion even in the case of attacks. Thus the method can be used to embed copyright information in the form of a visual watermark or simple text.

Keywords: SVD, watermarking, robust, DWT

I. INTRODUCTION

Watermarking is the process of embedding data into a multimedia element such as an image, audio or video file for the purpose of authentication [1]. 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 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 [2]. 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 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 upon 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 [3]. 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 [3]. 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 [6]. In 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.

Recently, Singular Value Decomposition (SVD) was explored for watermarking [4]. The SVD was originally developed by geometers, who wished to determine whether a real bilinear form could be made equal to another by

independent orthogonal transformations of the two spaces it acts on.

II. SINGULAR VALUE DECOMPOSITION

In linear algebra, the singular value decomposition (SVD) is an important factorization of a rectangular real or complex matrix, with several applications in signal processing and statistics. The spectral theorem says that normal matrices can be unitarily diagonalized using a basis of eigen vectors. The SVD can be seen as a generalization of the spectral theorem to arbitrary, not necessarily square, matrices.

Suppose M is an m-by-n matrix. Then there exists a factorization for M of the form $M = U\sum V^T$ where, U is an m-by-m unitary matrix, the matrix Σ is m-by-n with nonnegative numbers on the diagonal and zeros on the off diagonal, and V^T denotes the conjugate transpose of V, an n-by-n unitary matrix. Such a factorization is called a singular-value decomposition of M.

- The matrix V thus contains a set of orthonormal 'input' vector directions for the matrix M.
- The matrix U contains a set of orthonormal 'output' basis vector directions for the matrix M
- The matrix Σ contains the singular values, which can be thought of as scalar 'gain controls' by which each corresponding input is multiplied to give a corresponding output.

III. DCT-SVD BASED WATERMARKING

Robustness, capacity and imperceptibility are the three important requisites of an efficient watermarking scheme. Ordinary SVD based watermarking scheme has high imperceptibility. Although the SVD based scheme withstands certain attacks, it is not resistant to attacks like rotation, sharpening etc. Also SVD based technique has only limited capacity [4]. These limitations have led to the development of a new scheme that clubs the properties of DCT and SVD. DCT based technique is one of the most popular transform domain techniques. This particular algorithm proves to be better than ordinary DCT based watermarking and ordinary SVD based watermarking scheme.

A. A. Observations

- The DCT coefficients with the highest magnitudes are found in quadrant B1 (top left quadrant), and those with the lowest magnitudes are found in quadrant B4 (bottom right quadrant). 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 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, there is no problem in modifying the coefficients in quadrant $B1$.

IV. DWT-SVD BASED WATERMARKING

The above mentioned SVD-DCT scheme has enormous capacity because data embedding is possible in all the sub-bands. Watermark was found to be resistant to all sorts of attacks except rotation and achieved good imperceptibility. The disadvantage is that the embedding and the recovery are time consuming process because the zigzag scanning to map the coefficients into four quadrants based on the frequency, is a time consuming process. Alternatively if we apply DWT we get the four frequency sub-bands directly namely; approximation, horizontal, vertical and diagonal bands [5]. So the time consumption will be greatly reduced.

A. A. Observations

- SVD is a very convenient tool for watermarking in the DWT domain. The effect of every pixel of the watermark in the watermarked image is reduced by means of a scaling factor instead of adding the pixel values of the host image and the watermark to obtain the watermarked image. 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 i.e., up to 0.5 for LL, and 0.01 for the other bands. For this pair of values, there was no degradation in the watermarked image. When the scaling factor for LL was increased to an unreasonable value, the image became lighter while an increase in the scaling factor for the other bands resulted 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, no problem was experienced in modifying the LL band.
- Watermarks inserted in the lowest frequencies (LL sub band) are resistant to one group of attacks, and watermarks embedded in highest frequencies (HH sub-band) 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.

V DWT-DCT-SVD BASED WATERMARKING

This method utilizes the wavelet coefficients of the cover image to embed the watermark. Any of the four sets of wavelet coefficients can be used to watermark the image. The DCT coefficients of the wavelet coefficients are calculated and singular values decomposed. The same procedure is applied to the watermark also. The singular values of the cover image and watermark are added to form the modified singular values of the watermarked image. The modified DCT coefficients form the singular value decompositions triangular matrices. Then the inverse DCT transform is applied followed by the inverse DWT. This is the algorithm that clubs the properties of SVD, DCT and DWT. This is a technique that has never been used before. Watermark embedded using this algorithm is highly imperceptible. This scheme is robust against all sorts of attacks. It has very high data hiding capacity.

B. Watermark Embedding Algorithm

Let '*A*' be the cover image. Apply DWT to decompose the image into four sub-bands LL, HL, LH and HH. Take any of these four sub-bands. Apply DCT to the chosen sub-band. Let '*B*' denote the matrix obtained after applying DCT. Now *B* acts as the host image. Apply SVD so that '*B*' can then be written as $B = U_B \Sigma_B V_B^T$ where U_B and V_B^T are the orthonormal unitary matrices of *B*. The term Σ_B constitutes the singular values of the matrix of *B*.

Let '*W*' represent the watermark. Apply DWT and take any of the four sub-bands. Apply DCT to the chosen sub-band. Let '*S*' denote the matrix obtained after applying DCT. Now *B* acts as the host image. Apply SVD so that '*S*' can then be written as $S = U_S \Sigma_S V_S^T$ where $U_{S \text{ and }}$ V_S^T are the orthonormal unitary matrices of *S* . The term Σ_S constitute the singular values of the matrix *S*. Modify the singular values of *B* using singular values of *S*. Then perform IDCT followed by IDWT to obtain the watermarked image. The four sets of DWT coefficients can be used to embed four different visual watermarks or the same watermark.

C. Watermark Recovery Algorithm

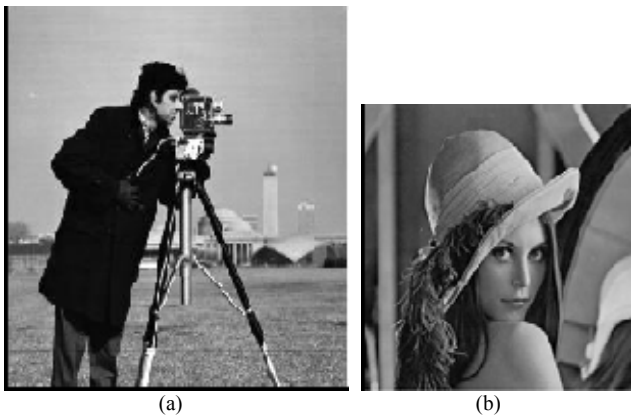
Let '*A*' be the cover image. Apply DWT and take any of the four sub-bands. Apply DCT to the chosen sub-band. Let '*B*' denote the matrix obtained after applying DCT. Now *B* acts as the host image. Apply SVD so that '*B*' can then be written as $B = U_B \Sigma_B V_B^T$ where U_B and V_B^T are the orthonormal unitary matrices of *B*. Term Σ_B constitutes the singular values of the matrix of *B*.

Let 'w*' be the watermarked image. Apply DWT and take any of the four sub-bands. Apply DCT to the chosen sub-band. Let '*A**' denote the matrix obtained after applying DCT. Now *A** acts as the host image. Apply SVD so that '*B*' can then be written as $B = U_{A*} \Sigma_{A*} V_{A*}^T$ where U_{A*} and V_{A*}^T are the orthonormal unitary matrices of *A**. Term Σ_{A*} constitutes the singular values of the matrix of *A**. Watermark is extracted by subtracting the singular values obtained above.

VI IMPLEMETATION

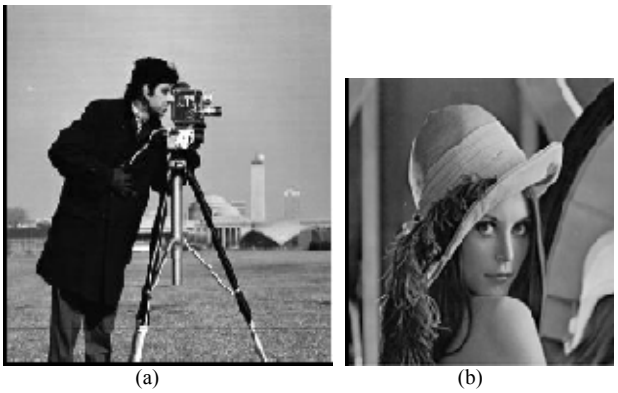
In our experiments 256x256 gray scale Cameraman image was taken as the cover image and 128x128 gray scale Lena was used as the watermark. Figure below shows the results of our method.

The DCT coefficients with the highest magnitudes are found in quadrant *B*1, and those with the lowest magnitudes are found in quadrant *B*4. Correspondingly, the singular values with the highest values are in quadrant *B*1, and singular values with the lowest values are in the quadrant *B*4. The largest singular values in the quadrants *B*2, *B*3, and *B*4 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 *B*1, and a smaller value for the other three quadrants.



(a) (b)

Fig.1. (a) Original image (b) Watermark



(a) (b)

Fig.2. (a) Watermarked image (b) Retrieved image

A. Attack modeling

Various attacks have been modeled on the watermarked image and in all cases, the watermark was recovered. In some cases, distortion was present. However, the watermark was found to be discernible with reasonable accuracy. The various attacks which were used are JPEG compression, Gaussian low pass filtering, Averaging Filter and Motion Blur. JPEG is a standard compression technique. When an image is compressed using JPEG standard the high

frequency components will be lost. If the high frequency components contain significant data, then that data would be lost. Here the watermarked image is JPEG compressed and the watermark is retrieved. When the compression ratio is low, the watermark is retrieved as such. When the compression ratio is increased to a high value, the retrieved watermark suffers from distortions. Gaussian filter is another low pass filter. Here the filter response has a Gaussian profile. The watermarked image is Gaussian filtered. All the high frequency components will be lost as a result of this. As a result any data that is stored in the high frequency components would be lost. In many cases the recovery is not possible. Here the recovery of the data is possible with a minimal amount of distortion.

Fig.3. (a) Average Filtering (b) Gaussian Blur
(c) JPEG Compression (d) Motion Blur

VII. RESULTS

1. The DWT-DCT-SVD based watermarking algorithm was found to be a very robust method of non-blind watermarking which can be used to embed copyright information in the form of a visual watermark or text. Watermark can be recovered even with the help of an attacked watermarked image.

2. Embedding can be carried out in all the frequencies without reasonable distortion in the visual watermark. For textual embedding however, recovery was found to be difficult from the attacked watermarked image.

3. In most of the DCT-based watermarking schemes, the lowest frequency coefficients are not modified as it is argued that watermark transparency would be lost. In this approach, we did not experience any problem in modifying the coefficients.

4. Watermarks inserted in the lowest frequencies are resistant to one group of attacks, and watermarks embedded in highest frequencies are resistant to another group of attacks.

5. 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 can be exploited to develop algorithms for lossy image compression.

VIII. CONCLUSION

A novel approach of watermarking based on DWT-DCT-SVD is suggested. The DCT-SVD based method is very time consuming though it offers better capacity and imperceptibility. DWT-SVD method is found to be similar to the DCT-SVD scheme except that the process was fast. The new method was found to satisfy all the requisites of an ideal watermarking scheme such as imperceptibility, robustness and good capacity. This method can be used for authentication and data hiding purposes. The future work includes the extension of this technique to other category and formats of images, for example, color images and DICOM images.

REFERENCES

[1] Stefan Katzenbeisser and Fabien A. P. Petitcolas, "I*nformation Hiding Techniques for Steganography and Digital Watermarking*," Artech house, Computer security series, pp.15-23, 97-109, 2000.

[2] Neil F.Johnson, Zoran Duric and Sushil Jajodia, "*Information Hiding, Steganography and Watermarking-Attacks and Counter Measures*," Kluwer academic publisher, pp. 15-29, 2003.

[3] Navas. K A, Sreevidya S, Sasikumar M "A *benchmark for medical image watermarking*", 14th International workshop on systems, signals & image processing and 6th EURASIP Conference focused on speech & image Processing, Multimedia Communication and services IWSSIP-2007 & EC-SIPMCS-2007, Maribor, Slovenia, 27-30 June 2007, pp 249-252.

[4] Alexander Sverdlov, Scott Dexter, Ahmet M. Eskicioglu "*Robust SVD DCT based watermarking for copyright protection*",IEEE Transactions on Image Processing, 10(5), May 2001, pp. 724-735.

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

[6] 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.