

Dual Image Watermarking Scheme based on DWT-SVD

D. M. Gaikwad

PG Student, Electronics and Telecommunication Dept.
Government College of Engineering, Aurangabad
Aurangabad, India
dnyangaik@gmail.com

A. R. Karwankar

Associate Professor, Electronics and Telecommunication Dept
Government College of Engineering, Aurangabad
Aurangabad, India
karwankar@yahoo.com

Abstract—The active development of internet, advance smart hand held devices and multimedia technologies have made it possible to easily create, copy, transmit, and distribute multimedia data instantly. Besides all of these advantages, there are many undesired issues including the piracy of digital data. It creates an issue like protection rights of the content and ownership. This concern has drawn the attention of the researchers toward the development of multimedia protection schemes using digital watermark. In this paper, a new image watermarking algorithm is presented which is robust against various attacks. DWT and SVD have been used to embed two watermarks in the HL and LH bands of the host image. Simulation evaluation demonstrates that the proposed technique withstands various attacks.

Keywords-Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Peak Signal to Noise Ratio (PSNR), Normalized Correlation (NC) coefficient.

I. INTRODUCTION

With the rapid development of the Internet and the wide availability of computers, scanners and printers make digital data acquisition, storage, exchange, and transmission very simple task. However, easily accessible digital data through networks to others also creates opportunities for malicious parties to make multiple saleable copies of copyrighted content without permission of the content owner [1]–[5]. Digital watermarking techniques have been proposed in recent years as methods to protect the copyright of multimedia data. Digital technology has many superior properties as compared to the analogue technology. It provides sophisticated processing capabilities, flexibility, and reliability at lower costs. In traditional copying the quality of the duplicated content is degraded. Digital tools can easily produce large amounts of perfect copies of digital documents in a short period of time. As a result, digital image acquisition, storage, processing and reproduction systems have been steadily replacing their analogue counterparts. Watermarking is in fact a centuries old mechanism for copyright protection. Currency notes are watermarked for preventing forgeries. The embedding of a hidden stream of bits in a digital media is called Digital Watermarking. The media could be an image, text, audio or video. Digital watermarking finds numerous applications in the field of device control and file reconstruction, transaction tracking, broadcast monitoring, owner identification, proof of ownership, content authentication, copy control, [6]–[7].

Broadly, there are two types of watermark embedding: one is a numerical sequence, which is usually a pseudo random noise like sequence embedding behaves like random noise. To detect this type of embedded watermarks, correlation calculation technique is commonly used. The other is a specific mark, which is usually a small meaningful logo. This meaningful logo watermarking has attracted more and more interest since the presentation of a recognizable logo is more perceivable than a numerical sequence. In the last decade, several image watermarking algorithms have been

proposed and most of them embed watermarks in spatial domain or transform domain. Watermarks in spatial domain are easy to destroy, which are usually designed as fragile watermarks. Whereas, transform domain watermark distributes information all over, making them not easily perceivable. Robust watermarks are usually designed in transform domain. Because of the multi-resolution property of the wavelet decomposition, more and more wavelet-based watermarking techniques considering human visual system (HVS) are proposed. Traditional watermarking achieves only one goal. If we want to achieve several goals, for example, protect the copyright of one product with several owners in different phases, or verify the integrity of the content and protect the copyright at the same time, we have to turn to multiple watermarking, that is, embed more than one watermark into the same multimedia object. It has great advantages on multimedia data tracing, data usage monitoring and multiple property management. Most current multiple watermarking schemes use a double watermarking algorithm, which combines a robust watermark and a fragile watermark [8].

DWT is very suitable to identify areas in the host image where a watermark can be imperceptibly embedded due to its excellent spatio – frequency localization properties. Slight variations of singular values do not affect the visual perception of the host image, an important mathematical property of SVD motivates the watermark embedding procedure to achieve good transparency and robustness [9]. The proposed watermarking scheme is based on DWT and SVD technique. In this, first host image is decomposed using two-level DWT and watermark images are embedded in the LH and HL bands of the host image.

The embedding is done by modifying the singular values in LH and HL bands of the host image with the singular values of the watermark images. Then the watermarked images are tested against various attacks.

The paper is organized as follows. Section II describes need and properties of watermarking. Section III discusses related previous work. Section IV explains the terminology of

SVD and DWT. Section V describes the proposed system. Section VI gives the simulation results and performance analysis. Finally section VII gives the conclusion.

II. NEED AND PROPERTIES OF WATERMARKING

The idea behind the digital watermarking is to provide copyright protection and ownership for intellectual property that is in digital format, such that nobody can tamper the data without consent of the owner. Watermarking technique can be divided into number of properties that are fidelity, data payload, security, robustness, capacity, false positive rate. We have to consider these requirements while designing the watermarking system. The properties of image watermarking are as follows

a) Fidelity or Transparency: After embedding the watermark, the quality of the image should remain intact. In other words, human visual system will not be disturbed by embedded watermark.

b) Robustness: Robustness is the ability to remain intact when undergoes common image operations like rotation, filtering, scaling, cropping, compression and additive Gaussian noise. Watermark should be strong and robust against geometrical and non-geometrical attacks.

c) Capacity or Payload: It describes how much data should be embedded as a watermark which will be successfully detected during extraction. Watermark should to carry enough information to represent the uniqueness of the image. Payload requirement varies as per the application

d) Imperceptibility: When watermark is embedded in the host image then the perceived quality of the host image should not be distorted by the presence of the watermark. The watermark should be imperceptible to human observation while the host image is embedded with secret data.

e) Complexity: It describes the cost to detect and encode the watermark information. So, it is challenging task to design complex watermarking procedure and algorithm. So that it can be integrated with different watermarks [5],[9].

A wide variety of image watermarking schemes has been proposed addressing many different application scenarios. Broadly, the watermarking schemes can be classified into two categories: spatial-domain watermarking schemes and frequency-domain watermarking schemes. In a spatial domain watermarking scheme, the watermark is embedded by directly modifying the spatial characteristics, such as pixel values and statistical traits. In contrast, frequency-domain watermarking schemes first transform an image into frequency domains, such as discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT), Fourier Mellin transform (FMT), fractal transform etc. The watermark is then embedded by altering the frequency coefficients. Since low and middle frequency coefficients are less likely to be affected by common signal processing than high frequency coefficients, the watermark is preferably embedded into the low and middle frequency coefficients.

Spatial domain methods (least significant bit substitution, spread spectrum etc.) are simple, high capacity but are not robust against common signal processing attacks. Transform domain methods (DFT, DWT, DCT, and SVD etc.) are more robust against common signal processing attacks but the

computational complexity is higher than that of spatial domain methods.

III. RELATED WORK

Various types of watermarking methods have been proposed for different applications and these can be broadly classified into two domains: Spatial domain and Transform domain. In spatial domain data is embedded directly by modifying pixel values of host image, while in transform domain data is embedded by modifying transform domain coefficients. Transform domain shows more robustness against various attacks so it is more preferred than spatial domain [10].

Dhanalakshmi and Thaiyalnayaki [9] proposed a dual watermarking method based on DWT-SVD and chaos encryption. They have embedded secondary watermark into primary watermark and the resultant watermark has been encrypted. Now, the combined encrypted watermark has been embedded into the host image. The method proposed in [10] is also embedding multiple watermarks in the host image. In the embedding process, a sign is first embedded into logo image and then a signed logo is embedded into the host image. Also, pseudo random generator based on the mathematical constant π has been developed and used at different stages in the method. Mahajan and Patil [11] have proposed a dual watermarking method based on DWT-SVD. In the watermark embedding process, first the secondary watermark is embedded into primary watermark then the combined watermark is embedded into the host image. In the recent years, singular value decomposition based image watermarking schemes have been proposed [14]. The SVD-based watermarking scheme is found to be weak against cropping attacks [15] and the DWT-SVD based scheme is able to remove this disadvantage. Liu et al. proposed a multiscale fullband image watermarking scheme by merging DWT-based and SVD-based techniques utilizing the advantages of both [16].

IV. TERMINOLOGY

A. Singular Value Decomposition

Let A be a general real(complex) matrix of order $m \times n$. The singular value decomposition (SVD) of A is the factorization

$$A = U * S * V^T \quad (1)$$

where U and V are orthogonal(unitary) such that $UU^T = ID$ and $VV^T = ID$, (ID denotes an identity matrix) and $S = \text{diag}(\sigma_1, \sigma_2, \dots, \sigma_r)$, where $\sigma_i, i = 1(1)r$ are the singular values of the matrix A with $r = \min(m, n)$ and satisfying

$$\sigma_1 \geq \sigma_2 \geq \sigma_3 \dots \geq \sigma_r \quad (2)$$

The first r columns of V the right singular vectors and the first r columns of U the left singular vectors.

In image processing applications, SVD has two main properties: (i) the singular values of an image have very good stability, when a small perturbation is added to an image, its singular values do not change significantly, and (ii) singular values represent the intrinsic algebraic image properties. The use of SVD in digital image processing has following advantages

- i) the size of the matrices from SVD transformation is not fixed. It can be either a square or rectangle.
- ii) In digital image singular values are less affected if general image processing is performed.
- iii) singular values contain intrinsic algebraic image properties.

B. Discrete Wavelet Transforms (DWT)

The DWT is a filters based system, which decomposes an image into a set of four non-overlapping multi-resolution sub bands denoted as LL (Approximation sub band), LH (Horizontal sub-band), HL (Vertical sub-band) and HH (Diagonal sub-band), where LH, HL, and HH subband represent the finest scale wavelet coefficients and LL subband stands for the coarse-level coefficients. The process can be repeated to obtain multiple scale wavelet decomposition, which is shown in Fig. 1.

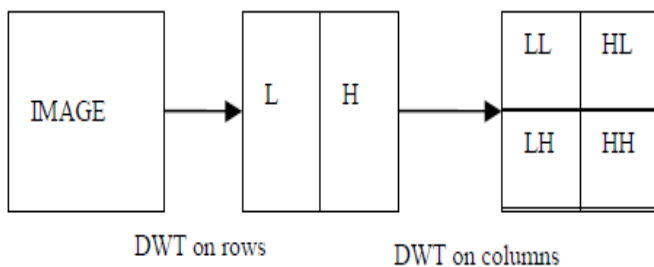


Figure 1. First level of decomposition of the input image

DWT plays an important role in the image processing field. It has many special advantages over other conventional transforms such as Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT). The DFT and DCT are full frame transforms and hence any change in the transform coefficient affects the entire image. DWT is very useful to identify the areas in the host image where a watermark can be embedded effectively. This technique allows the exploitation of the masking effect of the human visual system. The wavelet based watermarking techniques are getting more significance. When a DWT coefficient is modified, theregion only corresponding to that coefficient is modified. In general, most of the image energy is concentrated at the lower frequency subbands LL. Therefore embedding watermarks in LL sub bands may significantly degrade the image. Embedding in the low frequency sub-bands, however, significantly improves the robustness. Whereas, the high frequency sub-bands HH include the edges and textures of the image and the human eye is less sensitive to changes in such sub-bands. It allows the watermark to be embedded without being perceived by the human eye. So as to improve the robustness and imperceptibility, watermark embedding is done in the intermediate frequency bands HL and LH [19].

i) Haar Transform

The discussion of wavelets begins with the first and simplest Haar wavelet. It is discontinuous, and resembles a step function. It is similar to as Daubechies db1 wavelet. The first DWT was invented by the Hungarian mathematician Alfred Haar. When an input represented by a list of numbers, the Haar wavelet transform simply pair up input values, stores the difference and passes the sum. This process is repeated

recursively, pairing up the sums to provide the next scale, finally resulting in differences and one final sum. It is function of compression which involves averaging and differencing terms, storing detail coefficients, eliminating data, and reconstructing the matrix such that the resulting matrix is similar to the initial matrix. It uses these functions to furnish an example of an orthonormal system for the space of square-integrable function on the unit interval [0, 1].

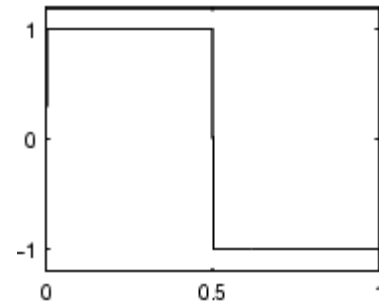


Figure 2. Haar Wavelet

ii) Daubechies Transform

Compactly supported orthonormal wavelets are invented by Ingrid Daubechies, a wavelet researcher. Thus making discrete wavelet analysis practicable. The names of the Daubechies family wavelets are described as dbN, where N is the order, and db the surname of the wavelet. The db1 wavelet is the same as Haar wavelet. Here is the wavelet functions psi of the next nine members of the family.

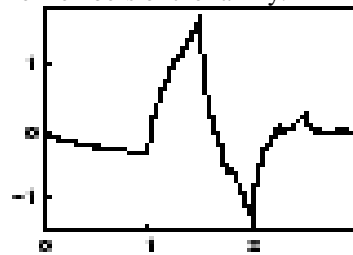


Figure 3. Daubechies Wavelet

The Daubechies wavelet resembles Haar wavelet transform by computing the running averages and differences via scalar products with scaling signals and wavelets the only difference between them consists in how these scaling signals and wavelets are defined. This wavelet has balanced frequency responses but its phase response is non-linear. Daubechies wavelets use overlapping windows, such that the high frequency coefficient spectrum reflects all high frequency changes. Therefore Daubechies wavelets are useful in compression and noise removal of audio signal processing [18].

V. PROPOSED SYSTEM

The proposed system is based on DWT-SVD technique. Daubechies wavelet is used for the decomposition of host and watermark images. Two level DWT decomposition was applied on the host image and single level decomposition on the watermark images. By modifying the singular values of the host image, watermark is embedded on HL and LH bands of the host image. Figure 4 shows the proposed method.

A. Algorithm – Embedding watermark

- i) Apply 2-level wavelet transform on the host image

ii) Apply SVD in the HL and LH band of host image.

$$H_1 = P_{H_1} * Q_{H_1} * R_{H_1}^T \quad (3)$$

$$H_2 = P_{H_2} * Q_{H_2} * R_{H_2}^T \quad (4)$$

iii) Apply first level Haar wavelet transform on the watermark images.

iv) Apply SVD on HL band of watermark image1

$$W_1 = P_{W_1} * Q_{W_1} * R_{W_1}^T \quad (5)$$

v) Apply SVD on LH band of watermark image2.

$$W_2 = P_{W_2} * Q_{W_2} * R_{W_2}^T \quad (6)$$

vi) Modify the singular value of the host image with the singular value of the watermark images.

$$Q_{WM} = Q_H + \alpha * Q_W \quad (7)$$

vii) Obtain the modified image.

$$I = P_H * Q_{WM} * R_H^T \quad (8)$$

viii) Apply inverse DWT to obtain the watermarked image.

B. Algorithm – Extracting the watermark

i) Apply 2-level wavelet transform on the watermarked image.

ii) Perform SVD on the HL and LH bands of the watermarked image.

$$I_{WM} = P_{WM} * Q_{WM} * R_{WM}^T \quad (9)$$

iii) Singular values of secondary watermark can be extracted as

$$Q'_W = \frac{(Q_{WM} - Q_H)}{\alpha} \quad (10)$$

iv) The watermark image can be obtained as

$$W' = P_W * Q'_W * R_W^T \quad (11)$$

VI. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

The proposed algorithm is demonstrated using MATLAB. 8-bit gray scale Lena image of size 512x512 is selected as host image. The primary and secondary watermarks gray level images of building and a meaningful logo ET of size 256x256 are used respectively. To embed the watermarks into host image, I have performed 2-level of decomposition using Daubechies filter bank.

The embedding is done by modifying the singular values in LH and HL bands of the host image with the singular values of the watermark images. Then the watermarked image are tested against various attacks.

To investigate the robustness of the algorithm, the watermarked image is attacked by No attack, Salt & Pepper noise, Average and Mean filtering, Gaussian noise, Poisson noise, Average Filtering (5x5), Resizing, Rotation, Cropping. After these attacks on the watermarked image, the extracted watermarks are compared with the original one. The watermarked image quality is measured using PSNR (Peak Signal to Noise Ratio). Watermarked Lena image has PSNR value of 73.5684.

Figure 4 shows the original watermark, primary watermark1 and secondary watermark2. The extracted primary and secondary watermarks are shown in figure 5. Here the extracted watermarks closely resembles with the original one showing highest correlation. The result of Salt & pepper noise is shown in figure 6.



Figure 4. Original Images a) Host image b) Primary Watermark1 c) Secondary Watermark2



Figure 5. No attack a) Attacked Host Image b) Extracted Primary Watermark1 c) Extracted Secondary Watermark2



Figure 6. Salt & Pepper noise a) Attacked Host Image b) Extracted Primary Watermark1 c) Extracted Secondary Watermark2

The result of Average filtering (5x5) and median filtering is shown in figure 7 and 8 respectively. It can be observed that after applying these filters, the images are much degraded with huge data loss but the extracted watermarks can be recognizable. The quality of extracted watermark is not good but still it is recognizable.

The figure 9, 10 and 11 show the results of resizing, rotation and cropping. First the size of watermark is reduced to 128x128 and again expanded to its original size of 512x512. For rotation the watermarked image is rotated by 30° and extracted which is shown in figure 10. The 50% are remaining attacked and extraction result of cropping shown in figure 11.

As a quantitative measure, following metrics are used. The notations used are given below.

X_i : Original image, X'_i : Watermarked image, and
 N_t : Size of image

PSNR is calculated between the original and the watermarked image. If PSNR values are high, that indicates low degradation, so the watermarking technique is more robust to various attacks.

$$PSNR = 10 * \log_{10} \left(\frac{255 * 255}{MSE} \right) \quad (12)$$

Mean Square Error between original image and watermarked image is calculated as follows:

$$MSE = \frac{1}{N_t} \sum_{i,j} \{ (X(i,j) - X'(i,j))^2 \} \quad (13)$$



Figure 7. Average Filtering attack (5X5) a) Attacked Host Image b) Extracted Primary Watermark1 c) Extracted Secondary Watermark2



Figure 8. Median Filtering attack a) Attacked Host Image b) Extracted Primary Watermark1 c) Extracted Secondary Watermark2



Figure 9. Resizing attack (512-128-512) a) Attacked Host Image b) Extracted Primary Watermark1 c) Extracted Secondary Watermark2

It can be observed that after applying Resizing attack Cropping attack, the images are degraded at large extent with huge data loss but the extracted watermarks can be recognizable. The quality of extracted watermark is not good but still it is recognizable.



Figure 10. Rotation attack (45°) a) Attacked Host Image b) Extracted Primary Watermark1 c) Extracted Secondary Watermark2



Figure 11. Cropping attack (50% area remaining) a) Attacked Host Image b) Extracted Primary Watermark1 c) Extracted Secondary Watermark2

To detect the presence of watermark different measures are used to show the similarity between the extracted and original watermark. To check the similarities between the original and extracted watermarks, the correlation coefficient was employed. The normalized coefficient (NC) gives a measure of the robustness of watermarking and its peak value is 1.

The notations are used below.

$W(i,j)$ = Original Watermark

$W'(i,j)$ = Extracted Watermark

$$NC = \frac{\sum_i \sum_j W(i,j) W'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2} \sqrt{\sum_i \sum_j W'(i,j)^2}} \quad (14)$$

Table 1. Correlation coefficient of Extracted Primary1 and Secondary watermark2

Sr. No.	Type of Attack	NC1	NC2
1	No attack	1.0000	0.9972
2	Salt & Pepper noise	0.9701	0.9639
3	Average Filtering (5x5)	0.8877	0.8904
4	Median	0.9744	0.9363
5	Resizing(512- 128-512)	0.8714	0.8808
6	Rotation (45°)	0.9175	0.9412
7	Cropping(50%)	0.8852	0.8749

Looking at the observations, regarding geometric including rotation, translation and scaling, that the algorithm is robust against attacks.

VII. CONCLUSIONS

In proposed scheme the watermarks are either a gray scale image or visually meaningful gray scale logo instead of a noise type Gaussian sequence. The proposed scheme is reliable for watermark extraction of both primary and secondary watermark. In this method, robustness is verified by variety of attacks. The algorithm uses DWT decomposition for images, and modifies its singular value matrix with a watermark matrix before reconstituting the signal. This dual watermarking algorithm is useful for identification of ownership of digital images and extraction of manipulations in the images.

REFERENCES

[1] Ruizhen Liu and Tieniu Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE Transactions on Multimedia, Vol. 4, No. 1, March 2002.
 [2] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, "A Dual Digital-Image Watermarking Technique", International Journal of Computer and Information Engineering Vol: 1, No: 5, 2007.
 [3] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, "A Dual Digital-Image Watermarking Technique", International Journal of Computer and Information Engineering, Vol. 1, No: 5, 2007.

[4] Gaurav Bhatnagar, Balasubramanian Raman, K. Swaminathan, "DWT-SVD based Dual Watermarking Scheme", IEEE, 2008.
 [5] Vaishali S. Jabade, Dr. Sachin R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques", IJCA, Volume: 31, No.1, October 2011.
 [6] Bhupendra Ram, "Digital Image Watermarking Technique Using DiscreteWavelet Transform And Discrete Cosine Transform", International Journal of Advancements in Research & Technology, Volume 2, Issue4, ISSN 2278-7763, April-2013.
 [7] R.Dhanalakshmi, K.Thaiyalnayaki, "Dual Watermarking Scheme with Encryption", International Journal of Computer Science and Information Security (IJCSIS), Vol. 7, No. 1, 2010.
 [8] Hong Shen, Bo Chen, "From single watermark to dual watermark: A new approach for image watermarking", Computers and Electrical Engineering 38 (2012), 1310-1324.
 [9] Anumol Joseph, K. Anusudha, "Robust watermarking based on DWT SVD", International Journal of Signal & Image Processing, Issue. 1, Vol. 1, October 2013.
 [10] Anjali Kathpal, Sonika Jindal, "Dual Image Watermarking Algorithm with SVD-DWT and Edge Detection on Different Layers of Colored Image", International Journal of Computer Applications (0975- 8887) Volume: 126, No.5, September 2015.
 [11] Amit Kumar Singh, Basant Kumar, Mayank Dave, Anand Mohan, "Robust and Imperceptible DualWatermarking for Telemedicine Applications", Wireless Pers Commun (2015) 80:1415–1433, DOI 10.1007/s11277-014-2091-6.
 [12] Dhanalakshmi, R., & Thaiyalnayaki, K. (2010). Dual Watermarking Scheme with Encryption. International Journal of Computer Science and Information Security, 7, 248-253.
 [13] Tripathi, S., Ramesh, N., Bernito, A., & Neeraj, K. J. (2010). A DWT based Dual Image WatermarkingTechnique for Authenticity and Watermark Protection. Signal & Image Processing: An International Journal (SIPIJ), 1, 33-45.
 [14] R. Liu and T. Tan, An SVD-based Watermarking scheme for protecting rightful ownership, *IEEE Transaction on Multimedia*, vol. 4, no. 1, pp. 121-128, 2002.
 [15] M. Prasad R. and S. Koliwad, A Comprehensive survey of contemporary researches in watermarking for copyright protection of digital images, *IJCSNS*, vol. 9, no. 4, pp. 91-107, April 2009.
 [16] J-C. Liu, C-H.Lin, L-C.Kuo and J-C. Chang, Robust multi-scale full-band image watermarking for copyright protection, Lecture Notes in Computer Science, *Springer Berlin, Heidelberg*, vol. 4570, pp. 176-184, 2007.
 [17] Ms. Sonam Malik and Mr. Vikram Verma, "Comparative analysis of DCT, Haar and Daubechies Wavelet for Image Compression", International Journal of Applied Engineering Research, ISSN: 0973-4562, Vol.7, No.11 (2012).