Robust Digital Image Watermarking Scheme for Copyright Protection

Harshita Rawat
Asst. Prof., Dept. of CSE
National Institute of Technology,
Srinagar, Uttarakhand, INDIA

Ashwani Kumar
Asst. Prof., Dept. of CSE
G. B. Pant Engineering College,
Pauri, Uttarakhand, INDIA

Satendra Kumar
Asst. Prof., Dept. of CSE
Seemant Institute of Technology,
Pithoragarh, Uttarakhand, INDIA

ABSTRACT

As the popularity of digital media is growing, and world is becoming smaller, all due to the internet connectivity and WWW phenomena, the copyright protection of intellectual properties have become a necessity for prevention of illegal copying and content integrity verification. Digital watermarking is a technique of embedding some information (usually hidden copyright notices) into an image.

The proposed approach a Robust Digital image watermarking algorithm using two levels discrete wavelet transform with Singular value decomposition. Second level DWT is performed on HL sub-band. One of the main contributions of the proposed technique is in decomposing the host image. Primarily the proposed technique aims to improve the robustness of the other watermarking techniques and keeps the watermarked image imperceptible. To increase and control the strength of the watermark, we used a scale factor. Experimental results clearly show that this proposed scheme is quite resilient to various image processing attacks.

Keywords

Watermarking, Wavelet transform, singular value decomposition (SVD), Peak signal to noise ratio (PSNR), Normalized cross correlation (NCC).

1. INTRODUCTION

Over the past two decades, there has been a tremendous growth in computer networks and more specifically, the World Wide Web. Apart from that, it is becoming a challenge to provide the ownership for the creators from the unauthorized persons who are duplicating their data or work. This along with the exceptional increase in Computer performance has facilitated extensive distribution of multimedia data such as images over the internet quite easily. Publishers, artists, and photographers, however, may be unwilling to distribute pictures over the Internet due to a lack of security, images can be easily duplicated and distributed without the owner's consent. Digital watermarks have been proposed as a way to tackle this tough issue [13,15].

The copyright protection of the digital media is very important because it has identified the protection of intellectual property rights. If a copyright has some problems such as copied, modified and attack, the other person is claiming that they had owned the multimedia objects.

Copyright protects is usually embedded with information about the multimedia that is the copyright of owner.

There are many solutions that have been proposed like Cryptography [16], Steganography and Watermarking [17].

The introduction of image processing tools has resulted in increased vulnerability for unauthorised copying, modifications of digital images. Besides, the data hiding technologies for digital data like digital watermarking have attracted immense attention recently [4-9].

Digital Watermarking is defined as the process of hiding a piece of digital data in the cover data which is to be protected and extracted later for ownership verification, since it makes possible to identify the author of an image by embedding secret information in it[13]. Some of the important applications of watermarking technique are copyright protection, ownership verification, finger printing, and broadcast monitoring. Digital watermarking provides a possible solution to the problem of easy editing and duplication of images, [2-3].

Depending upon the domain in which the watermark is inserted, these techniques are basically classified into two categories, i.e., spatial-domain and transform-domain methods. Embedding the watermark into the spatial domain component of the original image is an easy technique as watermark is inserted directly onto the pixel level. It provides some advantages of low complexity and easy implementation. However, the spatial-domain methods are generally fragile to image processing operations or other attacks. Transform domain techniques are used to embed the watermark by modulating the magnitude of coefficients in a transform domain, such as discrete cosine transform, discrete wavelet transform (DWT), and singular value decomposition (SVD) [3-6]. The transform domain techniques are usually preferred over spatial domain techniques because they are much more I secure in presence of noise.

A digital watermark is an unnoticeable signal added to digital data, known as cover work, which can possibly be identified at a later stage for ownership proof.

Ideal properties of a digital watermark:

1. A digital watermark should be imperceptible, meaning that it should be perceptually invisible to prevent obstruction of the original image.

2. Watermarks should be robust to filtering, additive noise, compression, cropping and other forms of image manipulations.Watermarks can be categorized into non blind, semi-blind and blind schemes on basis of the requirements for watermark extraction [7].This paper, proposed an embedding scheme uses a two level

decomposition. One of the main contributions of the proposed technique is in decomposing the host image. Primarily the proposed technique aims to improve the robustness of the other watermarking techniques and keeps the watermarked image imperceptible.The rest of the paper is organized as follow. Section II describes the related work. Section III describes the proposed technique watermark embedded and extraction process in Section IV we shows the experimental results against various attacks. Conclusion and future work are presented in section V and all the used references are describes in section VI.

2. RELATED WORK

Xia, Boncelet, and Arce [15] proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. This algorithm proposed that decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire, extracted watermark was correlated with the entire, original watermark. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and half-toning were performed on the watermarked images.

S.Ramakrishnan, T.Gopalakrishnan, K.Balasam [1] proposed a hybrid image watermarking algorithm which satisfies both imperceptibility and robustness requirements and used singular values of Wavelet Transformation's HL and LH sub bands to embed watermark. Further to increase and control the strength of the watermark, an optimal watermark embedding method is developed to achieve minimum watermarking distortion. A secret embedding key is designed to securely embed the fragile watermarks, so that the new method is robust to counterfeiting.

Chih-Chin Lai and Cheng-Chih Tsai [2] proposed an image-watermarking technique to satisfy both imperceptibility and robustness requirements. To achieve this, they proposed a hybrid image-watermarking scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD). The proposed approach is not embedded watermark directly on the wavelet coefficients but rather than on the elements of singular values of the cover image's DWT sub-bands.

3. BACKGROUND REVIEW AND PROPOSED WORK

3.1 DWT

Discrete wavelet transform is a multi-resolution decomposition of a signal. The low pass filter applied along a certain direction extracts the low frequency (approximation) coefficients of a signal. On the other hand, the high pass filter extracts the high frequency (detail) coefficients of a signal [11]. In 2D applications, for each level of decomposition, first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. Each component undergoes two levels of decomposition. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL1 contains

the lowest frequency band. The two-level DWT decomposition is shown in Figure 1.

LL	LL1	HL1
	LH1	HH1
LH	HH	
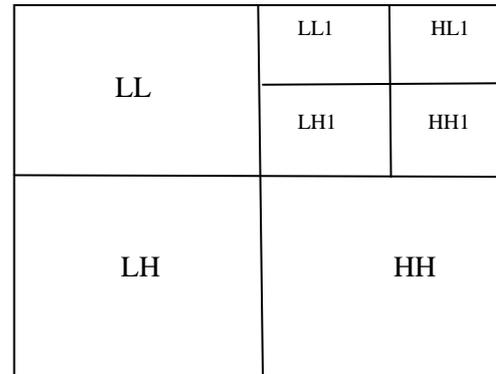
Fig 1: Two level DWT decomposition

3.2 SVD

Singular value decomposition is a linear algebra technique used to solve many mathematical problems [8].

Any image can be considered as a square matrix without loss of generality. So SVD technique can be applied to any kind of images. SVD approach has found use in watermarking field because of the fact that singular values obtained after decomposition of the image matrix are very stable and do not change on introduction of small perturbations[14].

The SVD belongs to orthogonal transform which decompose the given matrix into three matrices of same size [11]. To decompose the matrix using SVD technique it need not be a square matrix. Let us denote the image as matrix A. The SVD decomposition of matrix A is given using equation

$$A = USV^T$$

U and V are unitary matrices such that

$$U*U^T = I$$

$$V*V^T = I$$

Where, I is an Identity matrix.

S is the diagonal matrix having in its main diagonal all non-negative singular values of A. These positive singular values can be used to embed watermark. The order of singular matrix S is same as original matrix A[2].

3.3 Proposed Approach

The proposed DWT-SVD watermarking scheme is formulated as given here.

3.3.1 Watermark embedding:

1) Use one-level DWT to decompose the cover image A into four sub-bands (i.e., LL, HL, LH, and HH). Further apply next one-level DWT to decompose the HL subband into four subbands (i.e., LL1, HL1, LH1, and HH1).

2) Apply SVD to HL1 subband i.e

$$A_{HL1} = USV^T \tag{1}$$

3) Modify the singular values of HL1 subband with Watermark image, i.e.

$$S + \alpha * W = U_W S_W V_W{}^T \tag{2}$$

Where, α denotes the scale factor. To control the strength of the inserted watermark scale factor is used [12].

4) Obtain modified DWT coefficients, i.e.

$$A_{HL}* = U S_W V^T \tag{3}$$

5) Obtain the watermarked image AW by performing two level inverse DWT.

3.3.2 Watermark extraction:

1) Use first level Haar DWT to decompose the watermarked image Aw into four subbands: LL, HL, LH, and HH. Further obtained LL1, HL1, LH1 and HH1 subbands by performing 2nd level DWT on HL subband.

2) Apply SVD to the HL1 subband, i.e.,

$$A_{W_{HL}}* = U^* S_W{}^* V^{T*} \tag{4}$$

3) Compute difference

$$D_W = U_W S_W * V_W{}^T \tag{5}$$

4) Extract the watermark, i.e.

$$W = \frac{D_W - S}{\alpha} \tag{6}$$

4. EXPERIMENTAL RESULTS

For testing the performance of our proposed watermarking schemes for gray scale images, we are using two standard test images, gray level test images of Lena, Mandrill image [512x512] for cover images and for watermark we are using cameraman image [128x128] pixel.

Quality of the watermarked image is calculated using peak signal to noise ratio (PSNR). PSNR of an image can be calculated using the mean squared error. The mean squared error (MSE) between the original image and the watermarked image is given by:

$$MSE = \frac{1}{M.N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - I'(i,j)]^2 \tag{7}$$

where, $I(i,j)$ and $I'(i,j)$ denote the pixel value at position (i,j) of the original image I and the watermarked image I'. Both having sizes M x N pixels. Thus, Peak signal to noise ratio (PSNR) can be given by

$$PSNR = 10 \log_{10} \left[\frac{255^2}{MSE} \right] \tag{8}$$

To test the robustness of the proposed scheme, the watermarked image is tested against various image processing attacks like cropping (CR), rotation (RO), Gaussian noise (GN, variance 0.01), salt & pepper noise (S & P, 0.05), Median filtering (MF, [3 3]), Average filtering (AF), JPEG compression (JPEG, 30%), Contrast Adjustment (CA, 1.5) and histogram equalization (HE). Normalized correlation

(NC) is employed to evaluate the robustness of the algorithm. The Normal Correlation (NC) between the embedded watermark, W (i, j) and the extracted watermark W*(i, j) is given by,

$$NC = \frac{\sum_{i=1}^{Mw} \sum_{j=1}^{Nw} [W(i,j)].[W^*(i,j)]}{\sqrt{\sum_{i=1}^{Mw} \sum_{j=1}^{Nw} [W(i,j)]^2} \sqrt{\sum_{i=1}^{Mw} \sum_{j=1}^{Nw} [W^*(i,j)]^2}} \tag{9}$$

Here W and W_f are the original watermark and extracted watermark.

(a) Original image   (b) Watermark image

Table 1: shows the scale factor, PSNR and NC without any image processing attack

Scale Factor	PSNR	NC
0.01	69.6876	1
0.03	51.8430	1
0.05	46.0586	1
0.07	42.5685	1
0.09	40.0637	1

Table 2: Normalized Correlation Values of Extracted Watermarks against Different Attacks

SF	GN	RO	JPEG	CR
0.01	0.9885	0.9955	0.9470	0.9988
0.03	0.9498	0.9750	0.9842	0.9648
0.05	0.9577	0.9690	0.9929	0.9543
0.07	0.9570	0.9334	0.9961	0.9803
0.09	0.9653	0.9133	0.9978	0.9909

Experimental results shown in Table II describe the resilient nature of the watermarking scheme for aforementioned attacks. As the scale factor (SF) is gradually increased from 0.01 to 0.09, we can observe an increase in the normalized correlation values of the extracted watermarks also signifying degradation in the watermarked image quality as increasing the scale factor adversely affects the imperceptibility of the embedded watermark. Table III also suggests that we obtain moderate results in case of Gaussian noise introduction.

Table 3: *Experimental Result under Gaussian Noise and* Rotation *(NC values)*

Standard Variance	0.01	6	20	60	100
Proposed Scheme	0.95	0.86	0.86	0.86	0.86
Rotation (clockwise)		**45°**	**135°**	**225°**	**315°**
Proposed Scheme		0.88	0.83	0.88	0.83

SF	S&P	MF	HE	CA
0.01	0.9955	0.9968	0.9985	1.0000
0.03	0.9504	0.9829	0.9775	1.0000
0.05	0.9400	0.9769	0.9776	1.0000
0.07	0.9460	0.9744	0.9782	1.0000
0.09	0.9543	0.9718	0.9762	1.0000

To test the robustness of the watermarking scheme, to a greater extent, we subject the watermarked image to various image processing attacks varying different parameter and keeping the scale factor constant (0.05). In case of Gaussian noise we vary the standard variance. In case of rotation we rotate the watermarked image clockwise at various angles. JPEG compression is one of the most important attacks which can have extremely adverse effect on the watermarked image as well as the embedded watermark. Lastly, we carry out cropping of the watermarked image and extract corresponding watermark.

Results of all these attacks have been provided in the above mentioned tables. From Table III it is clear that there is no significant degradation in the extracted watermark quality even in the presence of a large amount of noise, this proves the robustness of the proposed scheme. Moreover, it ensures watermark delivery in every condition. Table II show the robustness of the proposed scheme for the aforementioned attacks. Table IV shows the efficiency comparison of proposed algorithm. Clearly the proposed scheme is resilient to various image processing attacks. MATLAB 7.6 software is being used to carry out all the experiments.

(c)   *(d)*

(e)   *(f)*

(g)   *(h)*

(i)   *(j)*
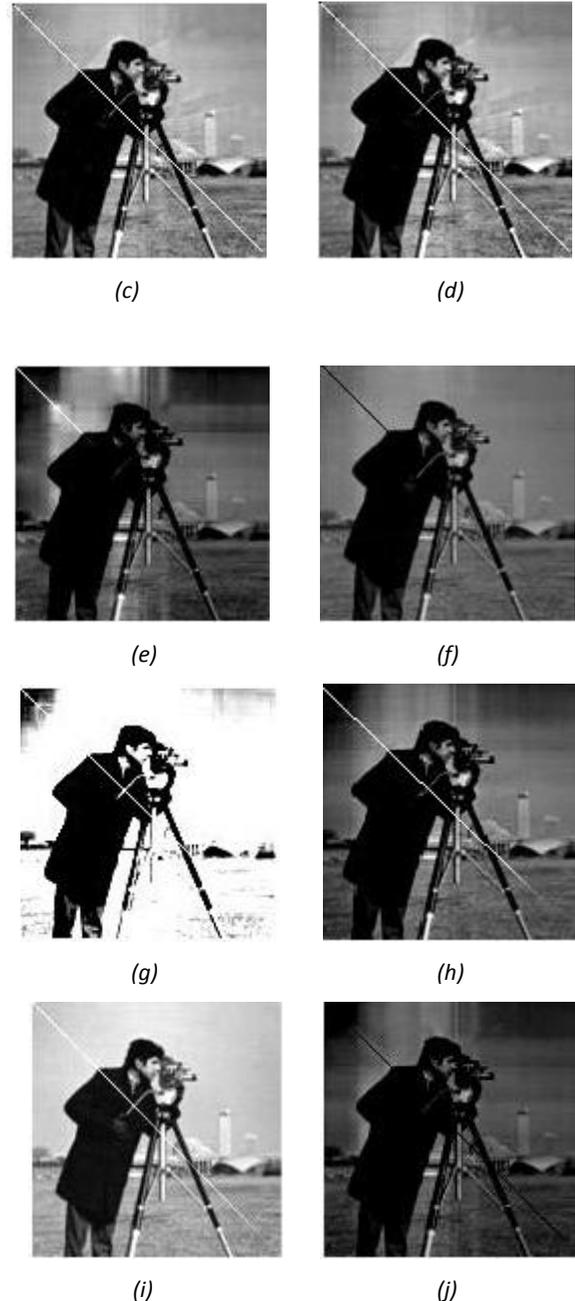
Figures: Extracted Watermark Images against various image processing attacks, (c) Gaussian noise (GN ,0.01), (d) average filtering (AF), (e) Contrast Adjustment (CA), (f) cropping (CR), (g) histogram equalization(HE), (h) JPEG compression (JPEG), (i) rotation (RO), (j) salt and pepper noise.

Table 4: Comparison of Efficiency For Chih-Chin Lai And Cheng-Chih Tsai [46] And Our Algorithm (Unit: Seconds*)*

	Chih-Chin Lai and Cheng-Chih Tsai [2]	Proposed Scheme
Watermark Embedding	3.7752	2.0280
Watermark Extraction	1.4508	0.1716

5. CONCLUSION AND FUTURE WORK

In this paper, a hybrid image-watermarking technique based on DWT and SVD has been presented. The experimental result shows that proposed technique fully exploits the respective feature of frequency localization of DWT and SVD efficiently represents intrinsic algebraic properties of an image. Experimental results of the proposed technique have shown both the significant improvement in imperceptibility and the robustness under attacks. Maximum achievable PSNR value of our proposed algorithm is 69.6876 on Lena cover image. An image quality metric especially for watermarking and data hiding purposes is to be developed. PSNR, NC as

well as the other quality metrics are for general purposes and sometimes do not give credible measurements for watermarked images. This metric should take account the special features of the Human Visual System (HVS) as well as the effects of information embedding in an image. A series of images should pass objective evaluation and by comparing the objective and the quality metric's results the quality metric could be fine-tuned in order to simulate HVS criterions. Further work challenges for digital image watermarking techniques are optimization of scale factor and technique integrating the human visual system characteristics.
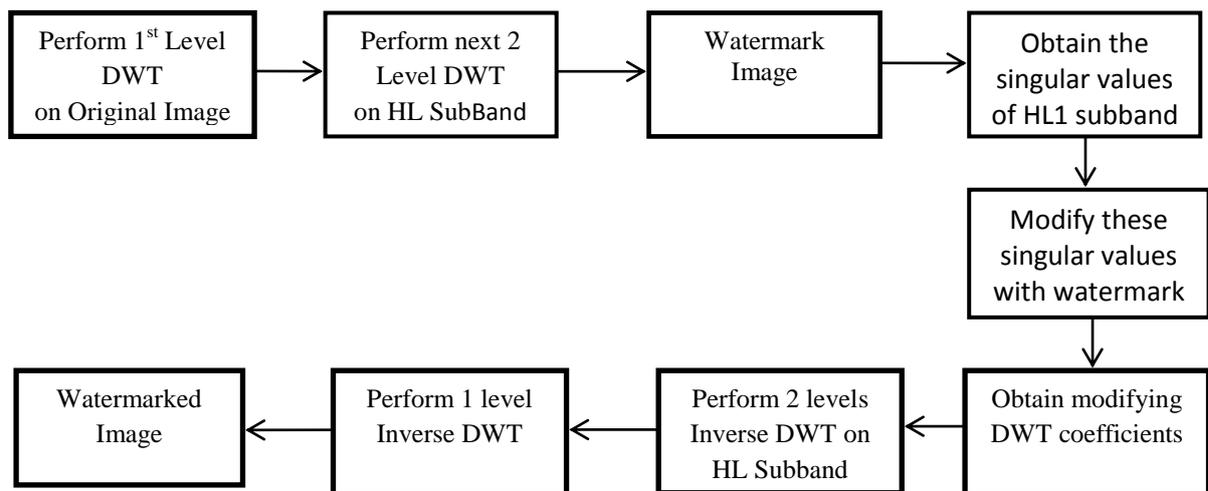
Fig 2: Proposed approach Watermark embedding process

6. REFERENCES

[1] S.Ramakrishnan1, T.Gopalakrishnan, K.Balasamy, "SVD Based Robust Digital Watermarking For Still Images Using Wavelet Transform" CCSEA 2011, CS & IT 02, pp. 155–167, 2011.

[2] Chih-Chin Lai, Cheng-Chih Tsai 2010. "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition". IEEE Transactions On instrumentation And Measurement, Vol. 59, No. 11, November 2010.

[3] Satendra Kumar, Nitin Arora, Jaydepp Kishore, "SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform" International Journal of Computer Applications (0975-8887) Volume 57–No.11, Nov 2012.

[4] Chunlin Song, Sud Sudirman and Madjid Merabti, "Robust Digital Image Watermarking using Region Adaptive Embedding Technique" 978-1-4244-6789-1110, 2010 IEEE

[5] Sanaz Shahraeini and Mahdi Yaghoobi, 2011. "A Robust Digital Image Watermarking Approach against JPEG Compression Attack

[6] Praful Saxena, Shanon Garg and Arpita Srivastava, "DWT-SVD Semi-Blind Image Watermarking Using High Frequency Band" 2nd International Conference on Computer Science and Information Technology (ICCSIT'2011)

[7] Ahmed Salama, Randa Atta, and Rawya Rizk, "A Robust Digital Image Watermarking Technique Based on Wavelet Transform" 2011 IEEE International Conference on System Engineering and Technology (ICSET)

[8] Satyanarayana Murty and Dr.P. Rajesh Kumar, "A Robust Digital Image Watermarking Scheme Using Hybrid DWT-DCT-SVD Technique" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.10, October 2010

[9] V.Santhi and Dr. Arunkumar Thangavelu, "DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space" International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009.

[10] Suhad Hajjara, Moussa Abdallah, Amjad Hudaib 2009. Digital Image Watermarking Using Localized Biorthogonal Wavelets European Journal of Scientific Research ISSN 1450-216X Vol.26 No.4 (2009)

[11] G.RoslineNesaKumari, B. VijayaKumar, L.Sumalatha, and Dr V.V.Krishna, "Secure and Robust Digital Watermarking on Grey Level Images" International Journal of Advanced Science and Technology Vol. 11, October, 2009

[12] Swanirbhar Majumder, Madhusudhan Mishra and A. Dinamani Singh, "A Hybrid SVD and Wavelet based Watermarking" 2nd National Conference Mathematical Techniques: Emerging Paradigms for Electronics and IT Industries, 2008

[13] Samira Mabtoul, EI hassan Ibn Elhaj and Driss Aboutajdine, "A Robust Digital Image Watermarking Method Using Dual Tree Complex Wavelet Transform" 978-1-4244-2703-1/08, 2008 IEEE

[14] Soo-Chang Pei, Ja-Han Chang, Jian-Jiun Ding and Ming-Yang Chen, "Eigenvalues and Singular Value Decompositions of Reduced Biquaternion Matrices" IEEE Transactions On Circuits And Systems, Vol. 55, No. 9, October 2008

[15] X. Xia, C. Boncelet, and G. Arce 1997 A Multiresolution Watermark for Digital Images. IEEE Conf. on Image Processing, vol. I, pp. 548-551, Oct. 1997.

[16] Jieh-Ming Shieh and Der-Chyuan Lou and Hao-Kuan Tso, "A Robust Watermarking Scheme for Digital Image Using Self Similarity" 0-7803-8932-8/05 2005 IEEE

[17] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121–128, March 2002.