Enhanced Digital Image Watermarking Scheme based on DWT and SVD

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

Jaydeep Kishore
Asst. Prof., Dept. of CSE
Seemant Institute of Technology, Pithoragarh

Nitin Arora
Asst. Prof., Dept. of CSE
Women's Institute of Technology, Dehradun

ABSTRACT
Digital watermarking is a technique of embedding some information (usually hidden copyright notices) into an image. Number of applications has been found in various fields like copyright protection, content authentication, document annotation, medical imaging. So, an enhanced semi-blind, hybrid digital image watermarking scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD) is our proposed approach in this paper. To increase and control the strength of the watermark, we used a scale factor. our proposed approach, the watermark is not embedded directly on the wavelet coefficients but rather than watermark wavelet coefficient are inserted on singular values of the cover images with modifying wavelet transform (DWT) HL1 sub band. Experimental results clearly show that this proposed scheme is quite resilient to various image processing attacks.

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

1. INTRODUCTION
Internet has made it extremely easy for anyone to share any kind of data with or without the consent of its owner; to curb this menace of unauthorized data transmission digital watermarking [2], [3] came out as a solution. In digital image watermarking we embed a hidden copyright notice onto the cover image. Later it could be extracted to claim the ownership of the image. It is also being used for content authentication, document annotation, biomedical image processing [4], [5], secret communication [1]. A good watermark should be robust and imperceptible. Robustness refers to resilience of the watermark towards common image processing attacks as well as intentional attacks. In particular, watermark should still be detectable or extractable even after common signal processing operations (such as geometric transformations, cropping, compression, filtering, resampling, scaling, rotation etc.) have been applied to the watermarked image. Imperceptibility means that it should not affect the visual quality of the cover image due to its presence. Robustness and imperceptibility of the watermark have a trade-off between them. It is desirable for a watermarking scheme to achieve a balance between both these properties. Watermarking can be categorized into spatial domain or transform domain depending upon how the watermark is being embedded. In spatial domain the watermark is directly embedded onto the pixel level itself. It has the advantage that it is fast and easy to implement but the embedded watermark gets distorted even in the slightest introduction of noise or in case of any tampering. In transform domain, watermark is added onto the coefficients of the cover image obtained after the transformation e.g. discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD). Transform domain techniques are usually preferred over spatial domain techniques because of the fact that they are more resilient to various image processing attacks.

One of the important properties [6] of the SVD is that singular values of a matrix do not exhibit prominent change when slight variation in the matrix elements is being carried out. This property encourages watermark insertion onto the singular values of the matrix. In this paper we propose a hybrid digital image watermarking technique combining both these transformation methods. Experimental results have also been provided to prove extreme robustness of this proposed scheme.

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 embedding scheme uses a two level Discrete Wavelet decomposition is presented. One of the main contributions of the proposed technique is in decomposing the host image. Second main contribution of proposed scheme the watermark is not embedded directly in SVD wavelet coefficient rather than the value of inserted Watermark Wavelet coefficient are inserted in SVD 2nd Level Wavelet coefficient elements of the Cover image. Primarily the proposed technique aims to improve the robustness of the others existing watermarking techniques and keeps the watermarked image imperceptible.

The main impediments of SVD based watermarking schemes are robustness, transparency, and the diagonal line problem in extracting watermarks.

2. BACKGROUND REVIEW AND PROPOSED WORK

Chih-Chin Lai and Cheng-Chih Tsai [10] proposed an image watermarking technique to satisfy both imperceptibility and robustness requirements. To achieve this objective, they proposed a hybrid image-watermarking scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD). In this approach, the watermark is not embedded directly on the wavelet coefficients but rather than on the elements of singular values of the cover image's DWT sub-bands. Problem of occurrence of two lines in diagonally in the reconstructed watermark occurred here against various attacks.

2.1 2D 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 [7]. The 2D DWT is computed by performing low-pass and high-pass filtering of the image pixels. At each level, the high-pass filter generates detailed image pixel information, while the low-pass filter produces the coarse approximations of the input image. 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: LL, LH, HL, and HH. For next each successive level of decomposition, in our proposed approach the LH sub band of the previous level is used as the input. HL component undergoes second level of decomposition. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL1 contains the lowest frequency component.

Two-level DWT decomposition is shown in Figure 1.

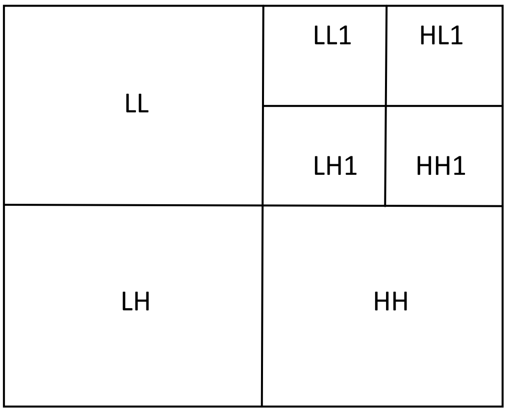


Fig 1: Two level DWT decomposition

2.2 SVD

Singular value decomposition is a linear algebra technique used to solve many mathematical problems [11].

Any image can be considered as a square matrix without loss of generality. So SVD technique can be applied to any kind of images either same or different dimensions[15].

The SVD belongs to orthogonal transform which decompose the given matrix into three matrices of same size. 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

$$A = USV^T \qquad \text{……... (1)}$$

Where U and V are unitary matrices such that

$UU^T = I$, and $VV^T = I$

Where, I is an Identity matrix.

And 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 [10].

2.3 Proposed Approach

In proposed approach watermark is not embedded directly in the Wavelet Coefficients rather than watermark image approximation Wavelet coefficient values are inserted to the cover image Wavelet Coefficients. Approximation Wavelet coefficient has the maximum information of original watermark image [12].

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

2.3.1 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 next one-level DWT to decompose the HL subband into four sub-bands (i.e., LL1, HL1, LH1, and HH).

2. Apply SVD to HL1 subband i.e

$$A_{HL1} = USV^T \qquad \text{……..(2)}$$

3) Apply one-level HAAR, DWT to decompose the Watermark image W into four sub-bands (LL_w, HLw, LH_w, and HH_w).

4) Modify the singular values of HL1 subband with Watermark image LL_w coefficients, i.e.

$$S + \alpha * LL_W = U_W S_W V_W{}^T \qquad \text{………(3)}$$

Where, α denotes the scale factor. To control the strength of the inserted watermark scale factor is used [10].

5) Obtain modified DWT coefficients, i.e.

$$A_{HL}* = US_W V^T \qquad \text{……..(4)}$$

6) Obtain the watermarked image A_W by performing Two level inverse DWT.

2.3.2 Watermark extraction:

1) Use first level Haar DWT to decompose the watermarked image A_w 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.,

$$A_{W_{HL}}* = U^{*} S_{W}^{*} V^{T*} \quad ……….(5)$$

3) Compute difference

$$D_W = U_W S_W * V_W^{\,T} \quad ……....(6)$$

4) Extract watermark wavelet coefficients HL subband, i.e.

$$W_{HL} = \frac{D_W - S}{\alpha} \quad ……..... (7)$$

5) Obtain the watermarked image W_f by performing inverse DWT with extracted watermark coefficients.

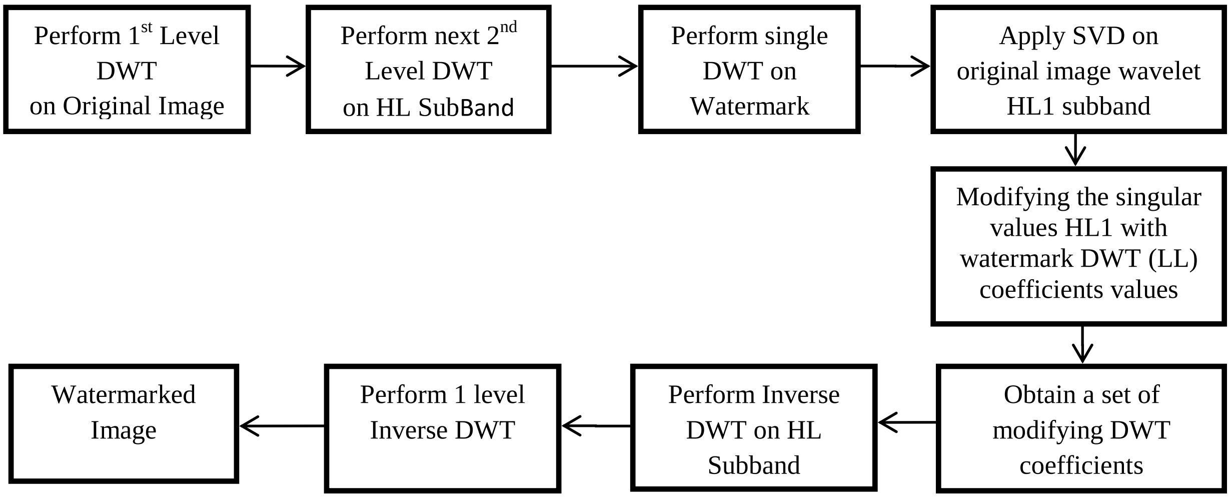


Fig 2: Proposed approach Watermark embedding process

3. EXPERIMENTAL RESULTS

A number of experiments are performed on the watermarked image to test the resilience of the proposed scheme towards common image processing attacks. 512x512 gray scale “Lena” and 256x256 “baboon” images are used as cover image and watermark image, respectively. These images are shown in Fig. 1(a) and (b). Fig. 1(c) and (d) show the watermarked image and the extracted watermark image respectively.

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \quad (8)$$

Where, Mean Square Error (MSE) and NCC

$$MSE = \frac{1}{N*N}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\left(I_{ij} - I'_{ij}\right)^2$$

$$NCC = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} W(i,j) * W_f(i,j)}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m}(W(i,j))^2}\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m}(W_f(i,j))^2}} \quad (9)$$

$I(i\ ,\ j)$ 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 and W and W_f are the original watermark and extracted watermark.

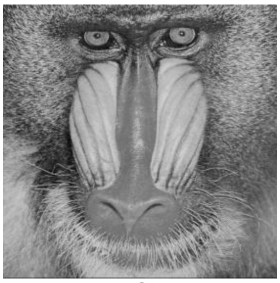
Experimental results are shown in Table first and Table second, describes the resilient nature of the watermarking scheme for mentioned attacks.

As the scale factor (*SF*) is continuously increased from 0.02 to 0.05, we can observe an increase in the normalized cross 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 1 suggests PSNR and NCC that we obtain results without any attacks. Table 2 and 3 shows the value of PSNR and NCC with respect to various image processing attacks. MATLAB 7.6 software is being used to carry out all the experiments.

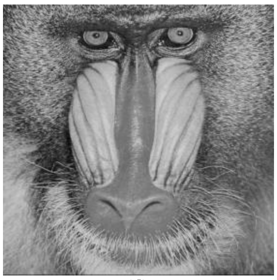
Table1: Shows the Scale factor, PSNR and NCC without any image processing attack

Scale Factor	PSNR	NCC
0.02	59.8081	.9991
0.03	51.2392	1
0.04	47.5312	1
0.05	45.2677	1

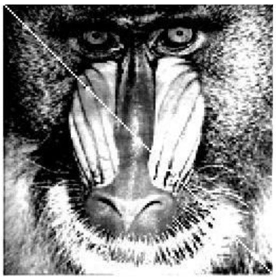

(a)


(b)


(c)


(d)

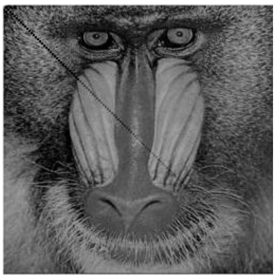

(e)


(f)


(g)


(h)


(i)


(j)

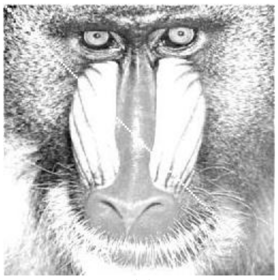

(k)


(l)


(m)


(n)


(o)


(p)

Figures:- Fig: a Cover image, Fig: b Original watermark image, Fig: c watermarked image, Fig: d extracted watermark image without any attack, Fig: e: watermarked image with Guassian Noise (GN), Fig f: extracted watermark image with Guassian Noise, Fig: g: watermarked image after rotation (RO), Fig h: extracted watermark image with rotation, Fig: i: watermarked image after jpeg compression, Fig j: extracted watermark image with jpeg compression, Fig: k: watermarked image after cropping (CR), Fig l: extracted watermark with cropping, Fig: m: watermarked image with histogram equalization(*HE*) , Fig n: extracted watermark with HE, Fig: o: watermarked image with contrast adjustment (CA) , Fig p: extracted watermark with contrast adjustment.

Table second and third shows the Robustness of extracted Watermark (NCC) with different Scale factor against various Image Processing attacks.

Table 2: Robustness of extracted Watermark (NCC)

SF	GN(.01)	RO	JPEG	CR
0.02	0.9292	0.9651	0.9546	0.8846
0.03	0.9465	0.8991	0.9768	0.9459
0.04	0.9575	0.7688	0.9872	0.9526
0.05	0.9666	0.7272	0.9927	0.9692

Table 3: Robustness of extracted Watermark (NCC)

SF	MF	HE	CA	AF
0.02	0.6261	0.9943	1.0000	0.8581
0.03	0.7391	0.9788	1.0000	0.8478
0.04	0.7630	0.9789	1.0000	0.8124
0.05	0.7835	0.9744	1.0000	0.7814

4. CONCLUSION AND FUTURE WORK

In this paper, a hybrid image-watermarking technique based on DWT and SVD has been proposed in which the watermark wavelet coefficient values are embedded on the singular values of the cover image's twice level DWT HL1 sub band. The Experimental results of the proposed technique have shown the significant improvement in both perceptibility and the robustness under various possible watermarking attacks. Further work of integrating the human visual system characteristics into our approach and optimization technique for scale factor is in progress.

5. REFERENCES

[1] Kiyoshi Tanaka, Yasuhiro Nakamura and Kineo Matsui, "Embedding Secret Information into a dithered multi-level image," IEEE, 1990.

[2] S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston, Mass, USA, 2000.

[3] C. I. Podilchuk and E. J. Delp, "Digital watermarking: algorithm and application," IEEE Signal Processing Magazine, vol. 18, no. 4, pp.33– 46, 2001.

[4] Rajendra Acharya U, Deepthi Anand, Subbanna Bhat P, and Niranjan U. C, "Compact Storage of Medical Images with Patients Information," IEEE Transactions on Information Technology Biomedicine, vol. 5, no. 4, December 2001.

[5] Xuan Kong and Rui Feng, "Watermarking Medical Signals for Telemedicine," IEEE Transactions on Information Technology in Biomedicine, vol. 5, no. 3, September 2001.

[6] 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.

[7] Ahmed Salama, Randa Atta, Rawya Rizk and Fayez Wanes "A Robust Digital Image Watermarking Technique Based on Wavelet Transform"

[8] Poonkuntran, R.S.Rajesh 2011. "A Messy Watermarking for Medical Image Authentication." 2011 IEEE

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

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

[11] V.Santhi and Dr. Arunkumar Thangavelu 2009. 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.

[12] Satendra Kumar, Ashwini Kumar Saini, papendra Kumar, "SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform" International Journal of Computer Applications (0975 – 8887) Volume 45– No.10, May 2012.

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

[14] Jen-Sheng Tsai, Win-Bin Huang, and Yau-Hwang Kuo, "On the Selection of Optimal Feature Region Set for Robust Digital Image Watermarking" IEEE Transactions On Image Processing, Vol. 20, No. 3, March 2011

[15] Dan Kalman, "A Singularly Valuable Decomposition: The SVD of a Matrix", The American University Washington 2002.