

Digital Image Watermarking Techniques Using Transform Domain

Ms.Pallavi patil₁, Dr. D.S. Bormane₂,

Department of Electronics and Telecommunication Engineering, Pune.

_{1,2}Rajarshi Shahu College of Engineering, University of Pune.

Abstract: Nowadays, in every field there is enormous use of digital contents. Information handled on internet and multimedia network system is in digital form. Digital watermarking is nothing but the technology in which there is embedding of various information in digital content, which we have to protect from illegal copying. Digital image watermarking is hiding information in any form (text, image, audio and video) in original image without degrading its perceptual quality. In case of Discrete Wavelet Transform (DWT), decomposition of the original image is done to embed the watermark and in case of hybrid technique (DWT-SVD) firstly image is decomposed according to DWT and then watermark is embedded in singular values obtained by applying Singular Value Decomposition (SVD). DWT & SVD are used together to improve the quality of watermarking. Here, the techniques are compared on the basis of Peak Signal to Noise Ratio (PSNR) value at different values of scaling factor; high value of PSNR is desired as it shows good imperceptibility of the technique.

Keywords—DWT, Hybrid DWT-SVD, PSNR, MSE, NC

I. INTRODUCTION

In the recent few years, there is a serious problem about unauthorized and illegal access and manipulation of multimedia files over internet. Everybody can obtain copies of copyrighted multimedia openly. So we need to generate a robust method in order to protect the copy rights of media. Digital watermarking provides copyright protection of data. Watermarking is a technique in which the original image also known as cover image is modified according to a watermark image. Certain characteristics of the cover image are altered in order to hide the data used for the identification of the owner of the original content [5]. Watermarking can be described by two basic modules, one is to hide the message in data which is called watermark embedder and the other module is detection of watermark named as watermark detector or Extractor. In many cases there is an additional data item necessary for embedding or detection, such as a secret key[11]. The kind of detection result depends on the watermarking application. In some cases the presence of a known watermark pattern is detected, in others a message of some kind (text, or even multimedia contents like images, audio etc.) is read.

There are two types of methods used for watermarking. First one is spatial domain method another one is transform domain method. In the spatial domain, the secret messages are embedded in the image pixels directly. The most common methods are histogram-based and least-significant bit (LSB) techniques in the spatial domain. Spatial domain based watermarking techniques are rarely preferred over transform domain based watermarking techniques because the watermark placed by them can be easily destroyed and modified by the attackers. While in the transform-domain the watermark is embedded by changing the magnitude of coefficients in a transform domain with the help of discrete cosine transform, discrete wavelet transform (DWT), discrete Fourier transform and singular value decomposition (SVD) techniques [10].

The paper is structured as follows. Introduction is given Section I. A review of related work is in Section II. Section III presents the proposed system. Experimental Result is discussed in Section IV. Section V describes the Conclusion of the paper.

II. RELATED WORK

A. Discrete Wavelet Transform (DWT)

DWT involves decomposition of image into frequency channel of constant bandwidth. The DWT decomposes input image into four components namely LL, LH, HL, and HH where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns. The lowest resolution level LL consists of the approximation part of the original image. The remaining three resolution levels consist of the detail parts and give the vertical high (LH), horizontal high (HL) and high (HH) frequencies. In the proposed algorithm, watermark is embedded into the cover image by modifying the coefficients of high-frequency bands i.e. HH sub bands [1]. This decomposition can continue until the desired level of decomposition is achieved for the application.

B. Singular Value Decomposition (SVD)

Singular Value Decomposition transform is a linear algebra transform which is used for factorization of a real or complex matrix with numerous applications in various fields of image processing [10]. As a digital image can be represented in a matrix form with its entries giving the intensity value of each pixel in the image, SVD of an image M with dimensions $m \times m$ is given by: $M = USVT$ Where, U and V are orthogonal matrices and S known as singular matrix is a diagonal matrix carrying non-negative singular values of matrix M . The columns of U and V are called left and right singular vectors of M , respectively [12]. They basically specify the geometry details of the original image. Left singular matrix i.e., U represents the horizontal details and right singular matrix i.e., V represents the vertical details of the original image. In Digital watermarking schemes, SVD is used due to its main properties: 1) Small variations in singular values does not affect the quality of image and, 2). Singular values of an image have high stability so; they do not change after various attacks.

Several methods have been proposed in literature. Hui-Yu Huang[1] proposed technique lossless data-hiding method for a DWT. Using the quantization factors for DWT, our proposed approach can offer high hiding capacity and preserve the image quality of stego-images. The original image can be recovered losslessly when the secret data had been extracted from stego-images. Cui-ling JIANG et al., [2] have presented the cover image is divided into non-overlapping blocks of 16×16 pixels instead of traditional dividing cover-image into 8×8 blocks and the DCT is used to transform each block. The DCT coefficients are quantized and embedded these secret messages. The method has the larger Steganography capacity and better stego-image quality than the other methods.

Hui-Yu Huang et al., [5] have proposed a lossless data-hiding method for a DWT-based technique. Using the quantization factors for DWT, our proposed approach can offer high hiding capacity and preserve the image quality of stego-images. The original image can be recovered losslessly when the secret data had been extracted from stego-images.

SatyanarayanaMurty et al. [10] proposed method (DWT-DCT-SVD) is highly robust and can resist many image processing attacks. The quality of the watermarked image is good in terms of perceptibility and PSNR (42db). The proposed algorithm is shown to be robust to all the attacks mentioned earlier except for JPEG 2000. The singular values in each quadrant are then modified by the singular values of the DWT-DCT transformed visual watermark. We show that embedding data in lowest frequencies is resistant to most of the attacks and some attacks are resistant to other frequency bands.

Vishal Verma et al., [11] we presented a detailed survey of existing image watermarking techniques. We classify the techniques based on different domains in which data is embedded. In This paper we have discussed different type of

techniques of embedding watermark and as per result shown our proposed method based on SVD DWT hybrid Technique have higher PSNR of Extracted watermark image. For the further work for watermarking in digital image we can embed watermark using new wavelet transform like Lifted wavelets and stationary wavelets, S-transform etc.

Prachi Chaudhary et al., [12] described two most recent techniques used in digital image watermarking; they are DWT and hybrid DWT-SVD. Both these techniques are very much robust and imperceptible. In case of DWT, decomposition of the original image is done to embed the watermark and in case of hybrid DWT-SVD firstly image is decomposed according to DWT and then watermark is embedded in singular values obtained by applying SVD. As at every value of scaling factor, value of peak signal to noise ratio is more in case of the hybrid technique. Less the value of PSNR more will be the degradation in the quality of the original image

From literature review digital data hiding in cover image using DWT_SVD techniques gives the good results as compared to others methods.

III. PROPOSED ALGORITHM USING DWT TECHNIQUES

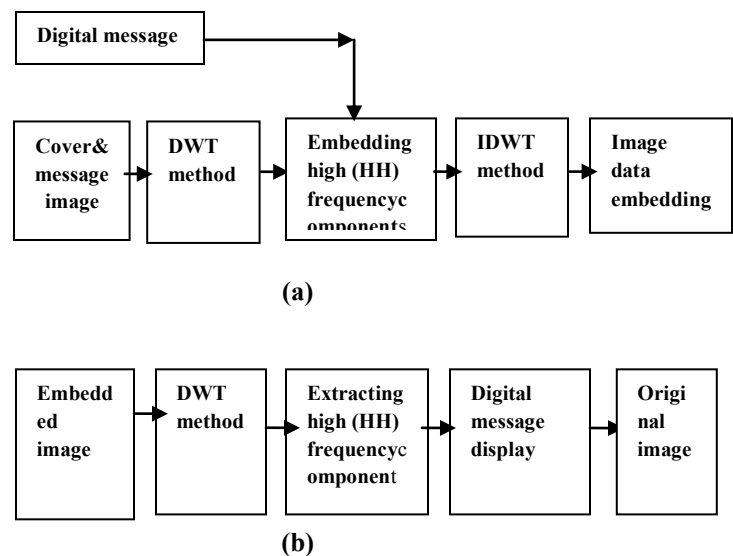


Fig.1 The proposed watermarking technique (a)- Embedding process (b)-Extracting process

The proposed watermarking technique is shown in fig.1 the proposed method embeds secret message or logo into DWT coefficients in medium high frequency components and restores the original image coefficients after the secret messages have been extracted. Wavelet transform is used to convert an image from spatial domain to frequency domain. Decomposition of digital image will be

pair of waveform with high frequency corresponds to detailed parts of an image and low frequency to smooth parts of image. The digital message will be embedding in high frequency components and the image will be reconstructed to get cover image with digital message hidden. Embedded image decomposed into inverse discrete wavelet transform. Inverse wavelet transform is used to convert frequency domain to spatial domain. Hence it is frequency-time representation. Embedded image will be extracted in to sub-band frequencies using dwt method. The digital data will be taken from the medium high frequency components and the extracted digital data will be compared with original message. This system includes the procedures of embedding and extraction.

A. Embedding Algorithm of DWT

1. Read cover image and resize to 512×512.
2. Read watermark logo and resize to 512×512.
3. Cover image decomposed into 1st level decomposition.
4. Apply dwt on message image.
5. Enter scale factor.
6. Now modified HH sub band and component.
 $HH_Mod = HH + k * WL_HH$
7. Apply inverse dwt with modified HH sub band.
8. Obtain watermarked image.
9. Apply noise on watermarked image.

B. Extracting Algorithm of DWT

1. To apply dwt on watermarked image.
2. To find difference
 $HH_Ext = (HH_WL - HH)/k$
3. To Apply idwt 2 using extracted HH sub band component.
4. To obtain the extracted message and original image.
5. To calculate PSNR, MSE & NC.

C. Embedding Algorithm of DWT_SVD

1. Read cover image and resize to 512x512.
2. Read watermark logo and resize to 256x256.
3. Apply haar wavelet and decompose cover image into 4 sub bands.
4. Apply SVD on HH sub band: U_HH, S_HH, V_HH
5. Apply SVD on watermark logo.
6. Enter scale factor.
7. Now modify S component, from svd, of HH band
8. $S_HH_Mod = S_HH + k * S_WM$;
9. Apply inverse svd on modified HH component.
10. Apply inverse dwt with modified HH band to obtain watermarked image.
11. Apply noise on watermarked image.

D. Extracting process Algorithm of DWT_SVD

1. Apply haar wavelet to watermarked image
2. Apply svd to HH band.
3. $D = (S_WMI - S_HH)/k$;
4. Extract s component of watermark logo
5. Apply inverse svd
6. Obtain watermark logo.
7. calculate PSNR ,MSE & NC.

IV. RESULTS AND DISCUSSION

To evaluate the robustness of the proposed approach, the watermarked image was tested against four kinds of attacks. To evaluate and compare the performance of two techniques i.e., DWT and DWT-SVD two parameters are taken into consideration. These parameters are given by

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{[I(i,j) - I'(i,j)]^2}{M \times N} \quad (1)$$

where, MSE is mean square error, M x N is the dimension of the images, I(i, j) is the original image, I' (i, j) is the watermarked image. Using the value of mean square error, Peak Signal to Noise Ratio (PSNR) for the images is calculated which gives the ratio of required signal to the noise content in the watermarked image. PSNR is calculated by the formula:

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

For the comparison of similarities between the original and extracted watermarks, the Normalize correlation coefficient is calculated by the formula:

$$NC = \frac{\sum_{i=1}^N W_i W_i'}{\sqrt{\sum_{i=1}^N W_i} \sqrt{\sum_{i=1}^N W_i'}} \quad (3)$$

Following fig.2 represents the gray-level image of size 512×512 Shown in fig.2(a) is used as the cover image and the gray-level image of size 512×512 Shown in fig.2 (b) is used as the watermark. fig.2(c) shows the watermarked image and fig.2 (d) extracted logo. Embedding and extraction results using 2D Haar DWT the watermarked image after embedding and the extracted image is shown in figure.2

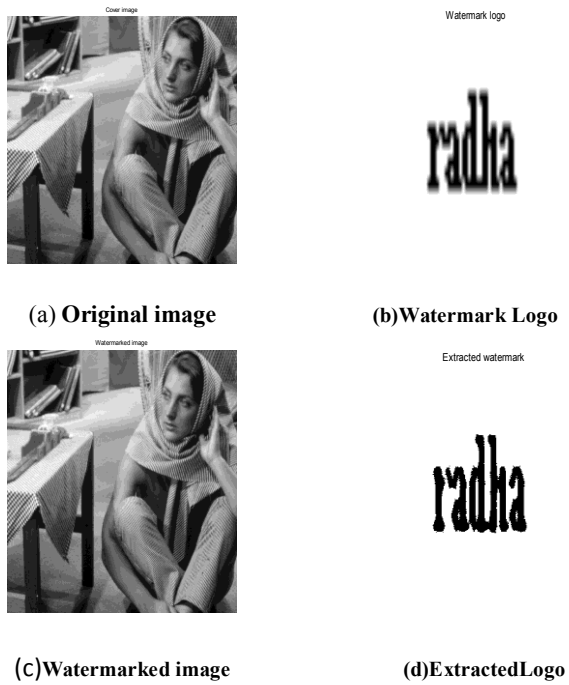


Fig.2 Matlab simulation results for single level DWT based watermarking

Table -1 Comparison Between the PSNR(db) of others & proposed method

Value of scaling factor (C)	PSNR(db) for others method DWT	PSNR(db) for others method DWT_SVD	PSNR (db)for proposed method DWT	PSNR (db)for proposed method DWT_SVD
0.01	43.63	76.2096	63.06	90.626
0.02	37.58	60.8586	62.38	88.687
0.03	34.08	52.6066	61.73	89.6802
0.04	31.57	49.4157	60.23	82.6802
0.05	29.64	45.9157	59.83	81.3097
0.06	28.04	43.1116	58.92	79.3083
0.07	26.71	40.8654	30.25	78.626

In table-1 the PSNR value of watermarked image in DWT is 63.06 & DWT_SVD is 90.626 which indicates that DWT-SVD is much better than DWT technique. We are adding the scale factor for security for purses. In proposed method, the values of the scale factors are carried out with constant range from 0.01 to 0.07 the results are shown in Tables 1. It can be seen that the larger the scale factor, the robustness is maintained. In contrast, the smaller the scale factor, the image watermarked quality is better.

The robustness of the proposed watermarking scheme is evaluated against several attacks including adding salt & pepper noise, Speckle noise, Gaussian low pass filter and Local variance noise. Table 2 shows PSNR & MSE of distorted watermarked images under above distortions. Applying attack on watermarked image using DWT technique the PSNR is less as compared to hybrid technique (DWT-SVD).

Table -2 Comparison between the PSNR & MSE of watermarked image under different attacks of proposed method

Cover images	Attacks	Control parameters	DWT	DWT_SVD
baboon	Gaussian	PSNR(db)	49.453	80.5003
		MSE	0.73758	0.000579
	Local variance	PSNR(db)	52.1913	80.6246
		MSE	0.3926	0.000563
	Speckle	PSNR(db)	49.2497	79.5309
		MSE	1.9417	0.000724
Pepper & salt	PSNR(db)	53.0809	79.0287	
	MSE	0.31988	0.00081	
hill	Gaussian	PSNR(db)	49.4551	80.5002
		MSE	0.7324	0.000579
	Local variance	PSNR(db)	52.2667	80.8899
		MSE	0.38812	0.000529
	Speckle	PSNR(db)	46.0854	79.6322
		MSE	0.72202	0.000708
	Pepper & salt	PSNR(db)	58.7061	79.1815
		MSE	0.13279	0.000785

Table-3 The PSNR (db)& NC of Watermarked noisy image on different logo using DWT_SVD method

Salt & pepper noisy image	Extracted Logo	PSNR	NC
		78.9504	0.9964
		78.939	0.9975
		79.64	0.9957
		78.8503	0.9867

The simulation result is shown in tables-3. Salt and pepper noisy different images, we embedded the different

logos using hybrid technique the simulation result is shown in tables-3. DWT and SVD are used together to improve the quality of the watermarking fusion makes a very attractive technique.

V. CONCLUSION

On comparing the values of PSNR at different values of scaling factor C , it is concluded that the hybrid technique DWT-SVD is much better than DWT technique. We have tested DWT-SVD hybrid method, the scale factor decreases as the PSNR increases. Less the value of PSNR more will be the degradation in the quality of the original image. Hybrid technique used together to improve the quality of watermarking. In proposed method, the difference from traditional scheme is that the watermarking is embedded in high frequency components and gives good performance in a variety of image application.

REFERENCES

- [1] Hui-Yu Huang & Shih-Hsu Chang "A lossless data hiding based on discrete Haar wavelet transform", 10th IEEE International Conference on Computer and Information Technology, 2010
- [2] Cui-ling JIANG "A Steganographic Method based on the JPEG Digital images" Institute of Information, East China University of Science and Technology, 2011
- [3] Anjali A. Shejul & Prof. U.L Kulkarni "A DWT based Approach for Steganography Using Biometrics", International Conference on Data Storage and Data Engineering, 2010
- [4] Souvik Bhattacharyya and Gautam Sanyal "Data Hiding in Images in Discrete Wavelet Domain Using PMM", World Academy of Science, Engineering and Technology, 2010.
- [5] Mohammad Reza Soheili "A Robust Digital image Watermarking Scheme Based on DWT" Journal of Advances in Computer Research, m2(2010) 75-82.1
- [6] Qingzhong Li, Chen Yu and Dongsheng Chu "A Robust Image Hiding Method Based on Sign Embedding and Fuzzy Classification", Proceedings of the 6th World Congress on Intelligent Control and Automation, 2006

- [7] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", IEEE International Journal of Applied Science and Engineering, 2006
- [8] Guorong Xuan, Yun Q. Shi & Chengyun Yang "Lossless Data Hiding Using Integer Wavelet Transform and Threshold Embedding Technique" 0-7803-9332-5/05/\$20.00 ©2005 IEEE
- [9] Y. K. Lee and L.-H. Chen, "High capacity image steganographic model", Vision, Image and Signal Processing, IEEE Proceedings, 2000
- [10] Satyanarayana Murty & 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
- [11] Vishal Verma & Mrs. Jyotsna Singh "Digital Image Watermarking Techniques: A Comparative Study" International Journal of Advances in Electrical and Electronics Engineering ISSN: 2319-1112 /V2N1:173-184, 2013.
- [12] Nidhi Bisla, Prachi Chaudhary "Comparative Study of DWT and DWT-SVD Image Watermarking Techniques" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013 ISSN: 2277 128X

Ms. Pallavi Patil has done B.E (Electronic & Telecommunication) from North Maharashtra University, also pursuing M.E (Digital System) from JSPM's RSCOE, Pune University. Have published one paper in IEEE National Conference & one paper in international journal of engineering & technology.



Dr. D. S. Bormaneis is working as Principal and Professor in JSPM's RSCOE, Pune. He has completed his PhD in Engineering (EC & CSE) from S.R.T.M.U., Nanded in 2003 in area of 'Noise Filtering From Images Using Wavelet Based Techniques'. He is the chairman for Board of Studies (Electronics & E & TC) at University of Pune. He has published more than 25 papers in International Journals, more than 10 papers in IEEE Computer society, 24 in International conferences and 14 in National conferences. His Areas of interests are Digital Signal Processing Image & Speech Processing. He is a life member of societies like – ISTE, ISCEE, IETE etc.