

A Semi-Blind Reference Watermarking Scheme Using DWT-SVD for Copyright Protection

Satyanarayana Murty . P¹, M.Uday Bhaskar², P.Nanna Babu³, P. Rajesh Kumar⁴

¹Sr.Associate Professor , Department of ECE, GIITS, Vishakapatnam,India
murty_pattisapu@yahoo.co.in

²PG Student, Department of CSE,Sri Sai Aditya Institute Of Science & Technology,AndhraPradesh,India
mangipudiuday@gmail.com

³Sr.Asst.Professor Department of CSE,Sri Sai Aditya Institute Of Science & Technology,AndhraPradesh,India

⁴Associate Professor, Department of ECE, AU college of Engineering, Vishakapatnam, India

ABSTRACT

In this paper we propose a semi-blind watermarking scheme using Discrete Wavelet Transform and Singular Value Decomposition for copyright protection. We used a gray scale image as a watermark to hide in another gray scale image as a cover image. The cover image is modified (Zig-Zag) and divided to number of blocks of size $n \times n$. We find the spatial frequency of each block and kept a threshold on this spatial frequency to form a reference image. Then the reference image is transformed into wavelet domain. We hide the watermark into reference image by modifying the singular values of reference image with the singular values of watermark. The proposed algorithm provides a good imperceptibility and robust for various attacks.

KEYWORDS

Spatial frequency, DWT, SVD, Zig_Zag ,Reference image.

1. INTRODUCTION

Digital watermarking is the process of hiding information into an image. The hiding information (a still image, Audio or Video) is called the watermark. The image, which is having hiding information, is called watermarked image. That can identify where the image came from or who has rights on it. In some watermarking schemes, a Watermarked image has a logo or some other information hindered into the image so that it is readily visible. However, these watermarks can be easily corrupted or removed using simple image processing techniques. Other schemes use invisible watermarking, in which the information is virtually invisible after it is embedded. Watermark embedding can be achieved in a number of different ways. Some techniques embed a binary pattern into the spatial domain of an image. Usually, the information can be embedded while taking into account which areas of the original image can hold more information while remaining undetectable [1,2]. The watermark is embedded by directly modifying pixel values in the spatial domain. Correlation based approach [3,4] is another spatial domain technique in which

the watermark is converted to a PN sequence which is then weighted and added to the host image with a gain factor k . For detection, the watermark image is correlated with the watermark image. Watermarking in transform domain is secure and robust to various attacks. The Fractional Fourier Transform (FrFt) can be used for digital watermarking [5,6,7,8]. Digital Image watermarking algorithms using Discrete Wavelet Transform (DWT) [10,11], Singular Value Decomposition (SVD) [12,13,14] are available in the literature. It is possible to have hybrid domains and transforms available in the literature. Some of those were DCT – SVD [17], [DWT-SVD [18] , DWT-DCT[19]. The basic philosophy in majority of the transform domain watermarking schemes is to modify transform coefficients based on the bits in watermark image. Watermarking schemes usually focus on watermarking black and white or gray scale images.

There was an existing reference water marking schemes.

Liu et al proposed [20] a watermark scheme, in this the original watermark is transformed in to one level DWT and then all high frequency bands(detailed) made to zero. Then they made the inverse transform. After that they compared the original and transformed images and found the location to embed the watermark. The watermark was a random sequence generated by seed point.

In another reference watermarking [21], the original image decomposed into three levels by using a DWT. The authors select one sub-band and it was decomposed for one level by using DWT. The authors set a threshold on directive contrast. Then they find the directive contrast between approximate band with other detail bands. By comparing the calculated directive contrast with the threshold value they set the detail bands to zero. They used the image (logo) as a watermark instead of a random sequence.

In this paper we proposed a semi-blind reference watermarking scheme using DWT-SVD technique. This technique is provided a good imperceptibility and high robustness to various imaging processing attacks. The rest of the paper is organized as follows: Section 2 contains our proposed watermark embedding and extraction algorithms, section 3 experimental results followed by conclusions in Section 4.

Spatial Frequency

Spatial frequency measures the overall activity level in an image [9]. For an image block I_1 of size $M \times N$, the spatial frequency is defined as:

$$SF = \sqrt{RF^2 + CF^2} \quad (1)$$

Where RF and CF are the row and column frequencies and are defined as:

$$RF = \sqrt{\frac{1}{M_1 N_1} \sum_{m=1}^{M_1} \sum_{n=2}^{N_1} [I(m, n) - I(m, n - 1)]^2}$$

$$CF = \sqrt{\frac{1}{M_1 N_1} \sum_{n=1}^{N_1} \sum_{m=2}^{M_1} [I(m, n) - I(m - 1, n)]^2}$$

2. PROPOSEDALGORITHM

2.1 Watermark Embedding

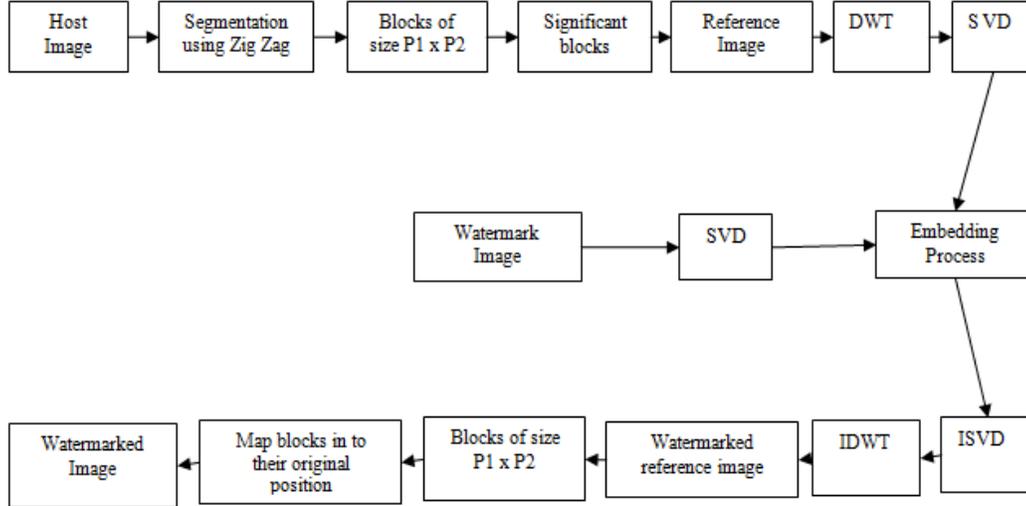


Figure 1(a)

The Watermark Embedding Procedure as Shown in Figure 1(a)

First, the original image is segmented into blocks of size $p_1 \times p_2$ via ZIG_ZAG sequence denoted by F^l , where l is the number of blocks.

Step1: Find out the spatial frequency in each block, denoted by SF_{Fl} .

Step2: Spatial frequencies of each block are stored in descending order. Then make a threshold on spatial frequency. Those blocks, which have spatial frequency less than or equal to threshold, are considered as significant blocks and are used for making reference image, F_{ref} which is a size of $m \times n$.

Step3: Perform DWT on the reference image, which is denoted by f_{ref} .

Step4: Consider f_{ref} HL band and Perform SVD transform as shown in equation (2).

$$f_{ref} = U_{f_{ref}} * S_{f_{ref}} * V_{f_{ref}}^T \quad (2)$$

Step5: Perform SVD on watermark image as shown in equation (3).

$$W = U_W * S_W * V_W^T \quad (3)$$

Step6: Modify the single values of reference image with the singular values of watermark as

$$(\sigma_{f_{ref}})^* = \sigma_{f_{ref}} + \beta * \sigma_W$$

Where β gives the watermark depth.

Step7: Perform inverse SVD,

$$f_{ref}^* = U_{f_{ref}} * S_{f_{ref}}^* * V_{f_{ref}}^T \quad (4)$$

Step8: Perform inverse DWT to construct the modified reference image, denoted by f_{ref}^* . Again f_{ref}^* is segmented into blocks of size $p_1 \times p_2$ and mapped onto their original positions for constructing the watermarked image.

We save the positions of the significant blocks and reference image for the extraction process.

2.2 Watermark Extraction

The Watermark Extraction Procedure as Shown in Figure 1(b)

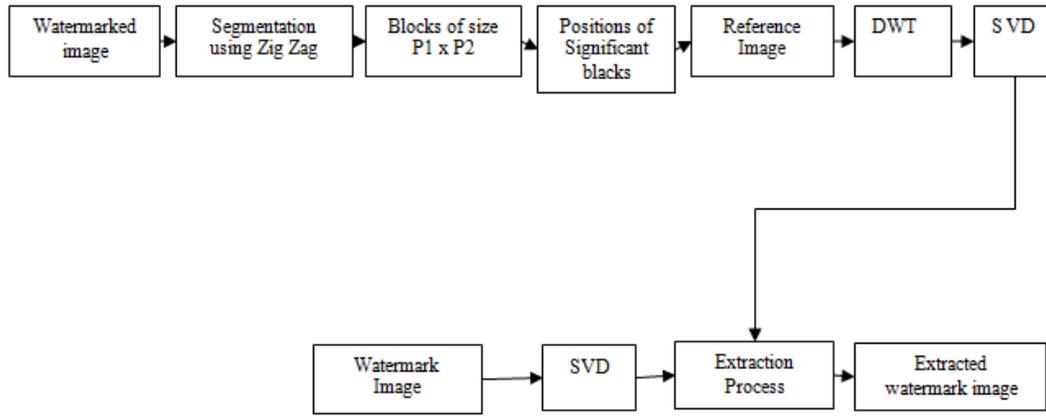


Figure 1(b)

The objective of the watermark extraction is to obtain the estimate of the watermark. For watermark extraction, original reference and watermarked images, left and right singular vectors must be available at the receiver end.

Step1: Using the positions of significant blocks, make the reference image from the watermarked image, denoted by F_{ref}^W .

Step2: Perform DWT on both F_{ref}^W and original reference image, which is denoted by f_{ref}^W and f_{ref} .

Step3: Perform SVD transform on both f_{ref} and f_{ref}^W .

$$f_{ref} = U_{f_{ref}} * S_{f_{ref}} * V_{f_{ref}}^T \quad (5)$$

$$f_{ref}^W = U_{f_{ref}^W} * S_{f_{ref}^W} * V_{f_{ref}^W}^T \quad (6)$$

Step4: Extract the singular values of the watermark.

$$\sigma_W^{ext} = \frac{\sigma_{f_{ref}^W} - \sigma_{f_{ref}}}{\beta} \quad (7)$$

Step5: Obtain the extracted watermark as:

$$W^{ext} = U_W * S_W^{ext} * V_W^T \quad (8)$$

3. RESULT ANALYSIS

The algorithms discussed in the above section have been implemented in MATLAB for the gray scale Boat, Mandrill, Lena and Peppers images of size 512×512 . For watermark, copyright gray scale image of size 128×128 was used. In our experiment, the size of blocks is taken to be 8×8 . The Peak Signal to Noise Ratio (PSNR) is the metric for imperceptibility.

$$PSNR = 20 \log \frac{255}{rms} db$$

rms is root mean square value between the original cover image and watermarked image. 255 is the height gray level value.

The normalized cross correlation is the metric for robustness. The test images, watermarked images and the corresponding PSNR values are showed in table -1. The original watermark and the extracted watermark (without applying attacks) images and normalized cross correlation values are shown in table 2. We investigate the robustness of the algorithm by considering Average filtering, Median filtering, Compression, Cropping, Gaussian noise, Histogram Equalization, Resize, Rotate, Pixilation, Sharpening, wrapping and motion blur attacks. After these attacks on the watermarked image, we have compared the extracted watermarks with the original one. The most common manipulation in digital image is filtering. The watermark is extracted after applying 13×13 averaging filtering and median filtering are shown in figure-2 and figure-3 respectively. To verify the robustness of the watermarking scheme, another measure is noise addition. In real life, the degradation and distortion of the image come from noise addition. In our experiment, we have added 75% additive Gaussian noise in the watermarked image. The extracted watermark is shown in figure-4. In real life applications, storage and transmission of digital data, a lossy coding operation is often performed on the data to reduce the memory and increase efficiency. Hence we have also tested our algorithms for the JPEG compression (80:1) and the extracted watermark is shown in figure-5. We have also tested our algorithms for rotation, cropping, and resizing attacks. Cropping is very frequently used action on images, and result for cropping is shown in figure-6. For resizing, first we reduce the size of image to 128×128 and again carried back to original size 512×512 . The result is shown in figure-7. For rotation, result for 50° is shown in figure-8. Pixilation (mosaic) is another disturbing operation on watermarked image to eliminate or destroying the watermark. The corresponding result of pixilation-3 is shown in figure-9. For wrapping is a 3D- effect on watermarked image and the result is shown in figure-10. Simultaneously histogram equalization, sharpening and contrast adjustment attacks are performed. The watermarked image is exposed for histogram equalization attack and the result is shown in figure-11. Motion blur is another attack on watermarked image and the result is shown in figure-12. For sharpening we increase the sharpness of watermarked image by a factor 100. The result is shown in figure-13. To verify the presence of watermark the correlation coefficient between original and extracted watermarks is given by below equation. The corresponding attacked images and extracted watermark images with NCC values as shown in table-3 and table-4 repectively.

$$\rho = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A})^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2)}}$$

Where, ρ is the normalized cross correlation. 'A' is the original watermark image. B is the extracted watermark image. \bar{A} Is the mean of original watermark and \bar{B} is the mean of the extracted watermark image.

Table – 1: Original cover images and watermarked images

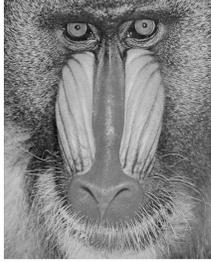
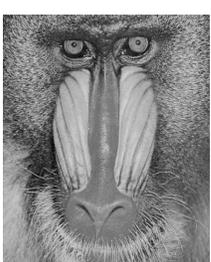
			
Original cover images			
			
PSNR = 43.88	PSNR = 44.30	PSNR = 45.35	PSNR = 44.45
watermarked images			

Table – 2 : Extracted watermarks from Boat, Lena, Mandrill and Peppers
(Without attacks)

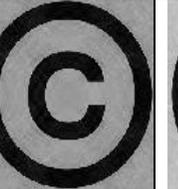
				
Watermark image	NCC = 0.9981	NCC = 0.9970	NCC = 0.9951	NCC = 0.9966

Table -3: showing various attacks on watermarked image

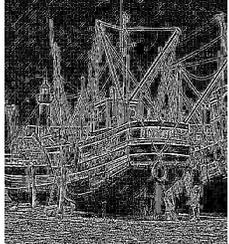
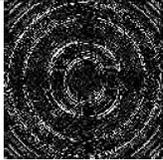
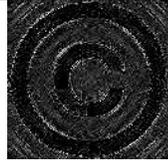
			
Figure-2 Average Filtering	Figure-3 Median Filtering	Figure-4 Additive Gaussian noise	Figure-5 JPEG compression
			
Figure-6 Cropping	Figure-7 Resizing	Figure-8 Rotation	Figure-9 Pixilation 3
			
Figure-10 Wrapping	Figure-11 Histogram equalization	Figure-12 Motion blur	Figure-13 Sharpening

Table -4: Extracted watermarks from various attacks with NCC values

					
Average Filtering 0.1198	Median Filtering - 0.0852	Additive Gaussian noise 0.6749	JPEG compression 0.9751	Cropping 0.8810	Resizing 0.2570

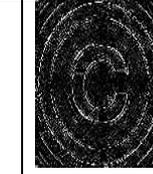
					
Rotation 0.8846	Pixilation 0.0871	Wrapping 0.7299	Histogram equalization 0.9182	Motion blur -0.1854	Sharpening 0.7240

Table -5: Comparison of Normalized Cross Correlation values with existing method

Attacks	Normalized cross correlation values (ρ)			
	Existing method		Proposed Method	
	Boat	mandrill	Boat	Mandrill
Average Filtering (13 x 3)	-0.3163	-0.1281	0.1198	-0.2473
Median Filtering (13 x 13)	-0.3158	-0.1016	-0.0852	-0.1556
Additive Gaussian Noise (75%)	0.1833	0.1656	0.6749	0.6956
JPEG compression (80:1)	0.8929	0.7865	0.9751	0.9471
Cropping (25% area remaining)	-0.1232	-0.1704	0.8810	0.8641
Resizing (512 -> 128 -> 512)	0.4897	0.0560	0.2570	0.4715
Rotation (50°)	-0.5470	-0.3626	0.8846	0.8964
Pixilation 3	-----	-----	0.0871	-0.2375
Wrapping	0.2385	0.5486	0.7299	0.7573
Histogram equalization	0.6009	0.7032	0.9182	0.8846
Motion blur	-----	-----	-0.1854	-0.3363
Sharpening (100)	0.1607	0.1881	0.7240	0.7013

4. CONCLUSIONS

In this paper we proposed a self-reference image watermarking by using the technique DWT-SVD. The watermark is visually meaningful gray scale image instead of a noise type Gaussian sequence. The proposed method is highly robust and can survive the watermark in any of attacks. The quality of the watermarked image is good in terms of perceptibility. The PSNR value for a boat image was 43.88db and the PSNR value for a mandrill image was 45.35 db. Our proposed method was superior than the existing method [22] for average filtering, median filtering, additive Gaussian noise, cropping, rotation, pixilation, wrapping, motion blur, histogram equalization and sharpening .The existing method was superior to our method in resizing attack. In our observations, no one can extract watermark without knowing the value of embedding depth.

REFERENCES

- [1] P.S. Huang, C.-S. Chiang, C.-P. Chang, and T.-M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," *IEEE Proc.-Vis. Image Signal Process.*, vol. 152, no. 5, October 2005.
- [2] C.-T. Hsu and J.-L. Wu, "Hidden Digital Watermarks in Images," *IEEE Trans. On Image Processing*, vol. 8, no. 1, January 1999
- [3] S.S. Bedi and S. Verma, A Design of Secure Watermarking Scheme for Images in Spatial Domain. IEEE 2006.
- [4] R. Bangaleea and H.C.S. Rughooputh. Performance improvement of spread spectrum spatial-domain watermarking scheme through diversity and attack characterization. IEEE Africon 2002.
- [5] A.C McBride , F.H.Kerr, On Namias, Fractional Fourier Transforms, *IMA Journal of Application Mathematics*,39:159-175,1987.
- [6] H.M.Ozaktas, Z Zalevsky ,M Kutay.The Fractional Fourier Transform,John Wiley and Sons,2001.
- [7] C .Chandan, M.Kutay,H.M.Ozaktas.The Discrete Fractional Fourier Transform, *IEEE Transactiona on Signa, processing*,48(5):1329-1337,2000.
- [8] S.C.Pei, M.H.Yeh.Two Dimensional Discrete Fractional Fourier Transform,*Signal processing*,67:99-108,1998.
- [9] A.M. Eskicioglu, P.S.Fisher.Image Quantity Measures and their Performance. *IEEE Transaction on Communication*,43(12):2959-2965,1995.
- [10] M.Barni, M., Bartolini, F., V., Piva, A., Improved wavelet based watermarking through pixel-wise masking. *IEEE Trans Image Processing* 10, 783- 791, 2001.
- [11] Y. Wang, J.F.Doherty and R.E.Van Dyck, A wavelet based watermarking algorithm for ownership verification of digital images, *IEEE Transactions on Image Processing*, Volume 11, No.2, pp.77-88, February 2002.
- [12] Chin-Chen Chang, Piyu Tsai and Chia-Chen Lin, 2005 SVD based digital image watermarking scheme. *Pattern Recognition Letters* 26, 1577-1586, 2005.
- [13] R.Liu, T.Tan, An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans. Multimedia*, vol.4, no.1, pp, 121-128, 2002.
- [14] D. V. S. Chandra, Digital Image Watermarking Using Singular Value Decomposition, *Proceedings of 45th IEEE Midwest Symposium on Circuits and Systems*, Tulsa, OK, pp. 264-267, 2002.
- [15] Sun, R., Sun, H., Yao, T., A SVD and quantization based semi-fragile watermarking technique for age authentication. *Proc. IEEE International Conf. Signal Process.* 2. 1592-95, 2002.
- [16] Y. Yongdong Wu. On the Security of an SVD based Ownership Watermarking *IEEE transactions on Multimedia*, Vol 7. No.4, August, 2005
- [17] Alexander Sverdllov, 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.
- [18] E.Ganic and A.M. Eskiciogulu et.al., Robust embedding of Visual Watermarks using DWT-SVD *Journal of Electronic Imaging*, October-December, 2005.
- [19] Ali Al-Haj, Combined DWT-DCT Digital Image Watermarking, *Journal of Computer Science* 3 (9): 740-746, 2007, ISSN 1549-3636, © 2007 Science Publications

- [20] J.L. Liu, D.C. Lou, M.C. Chang, H.K. Tso, A robust watermarking scheme using selfreference image, *Computer Standards and Interfaces* 28 (2006) 356–367.
- [21] Gaurav Bhatnagar , Balasubramanian Raman. A new robust reference watermarking scheme based on DWT-SVD, *Computer Standards & Interfaces* xxx (2009) xxx–xxx
- [22] Gaurav Bhatnagar and Balasubramanian Raman”Reference watermarking scheme in fractiona fourier transform domain using SVD”*International journal of information processing*,2(4),88-97,2008.