www.ijraset.com
IC Value: 45.98

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Robust Lossless Image Watermarking in Integer Wavelet Domain Using SVD

Shreyash Shantam[1]
[1]School of Information Technology, Vellore Institute of Technology Vellore, India

Abstract: The aim of digital watermarking is to hide some secret information or logo into the multimedia content for protecting the content from unauthorized access or illegal use .A robust and secure technique is required to protect multimedia data as it can be easily produced as illegal copies. Digital watermarking is used for Intellectual Property Rights protection and authentication. In this paper, a watermarking scheme based on Integer wavelet transform (IWT) and singular value decomposition (SVD) is implemented. The watermark image is embedded on the elements of singular values of the low-low (LL) Sub band of original image. The watermark image is extracted which is highly correlated with the original watermark image. The proposed algorithm is robust and authenticated under different attacks.

Keywords -Digital Watermarking, IWT, SVD

I. INTRODUCTION

Digital watermarking is a technique for inserting data (the watermark image) into an image, which can be extracted later for identification and authentication purposes. Digital watermarking technology is a method of protecting copyrights in digital images. It is realized by embedding data into an host image that is invisible to the human visual system. An effective watermarking scheme should satisfy the following basic requirements.

A. Imperceptibility

The difference between the original image and the watermarked image should be unknown to the human observer.

B. Trustworthiness

A watermarking scheme should guarantee that it is impossible to generate counterfeit watermarks and should provide trustworthy evidence to protect the rightful ownership.

C. Robustnes

Watermarks should be robust to common signal processing and intentional attacks. The watermarks should still be extracted from the attacked watermarked image.

II. IWT AND SVD

A. IWT

IWT is used for lossless compression. The transform coefficients are represented by finite precision numbers, and this allows for truly lossless coding. IWT is much faster than the DWT because the floating point wavelet transform demands for longer data length than the integer wavelet transform. Reversibility is another benefit of integer transform. Therefore, the image can be reconstructed without any loss because all the coefficients are integers and can be stored without rounding off errors. Its main advantage with respect to filter bank structure lies in its better computational efficiency and in fact, it enables a new method for filter design.

B. SVD

From the discernment of image processing, an image can be viewed as a matrix with nonnegative scalar entries. SVD is an effective numerical analysis tool from linear algebra to decompose a rectangular matrix "A" into an orthogonal matrix U, diagonal matrix S, and the transpose of an orthogonal matrix V. SVD decomposes a given image A of size M×N as $A = USV_T$ Where, U and V are orthogonal matrices of size MxM and NxN, respectively. S is a diagonal matrix of size MxN having singular values .

III. ALGORITHM

A. The Watermark embedding algorithm :

1) Apply Integer Wavelet Transform and decompose cover image into four sub-bands : LL, HL, LH and HH.
2) Perform Singular Value Decomposition on (HL,LH,HH) , as follows:

$$A_i = U_i * S_i * V_i$$

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Modify the singular values (S_i) of three sub_bands (HL, LH, HH) by embedding the watermark directly into eachsingular value. Then, apply SVD to the altered sub-bands.

$S_i + \alpha W = Uw_i * Sw_i * Vw_i^t$ where i indicates the sub-bands.

Apply SVD on watermark logo, as follows:

$$W = U * S * V$$

3) Apply signature generation procedure on the U and V matrix of the watermark logo.
4) New modified IWT cofficient are calculated as follows:

$Anew_i = U_i * Sw_i * V_i$ where i indicates the subbands.

5) Now apply inverse IWT to get the watermarked image.
6) Finally, embed the signature in the watermarked image.

B. The Watermark extracting algorithm :

1) Apply Integer Wavelet Transform and decompose watermarked image into four sub-bands : LL, HL, LH and HH.
2) Perform Singular Value Decomposition on (HL,LH,HH) , as follows:

$$A_i = U_i * Sd_i * V_i$$

3) Compute

$$D_i = Uw_i * Sd_i * Vw_i^t$$

where i indicates the sub-bands and Uw_i, Vw_i^t are from the watermark embedding process.

Extract the watermark using the following formula i.e.

$$W_i = (D_i - S_i) / \alpha$$

where i indicates the sub-bands and S_i is from the watermark embedding process.

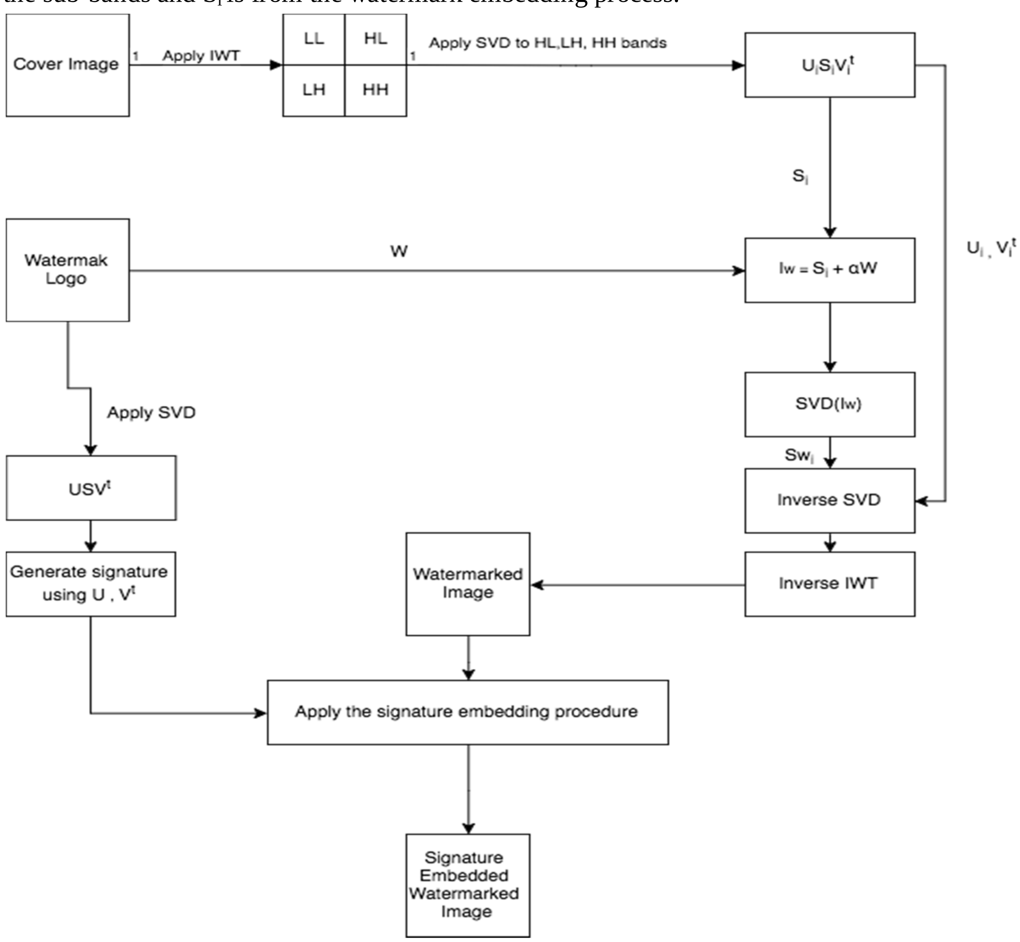

Fig.1 Watermark Embedding Procedure

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

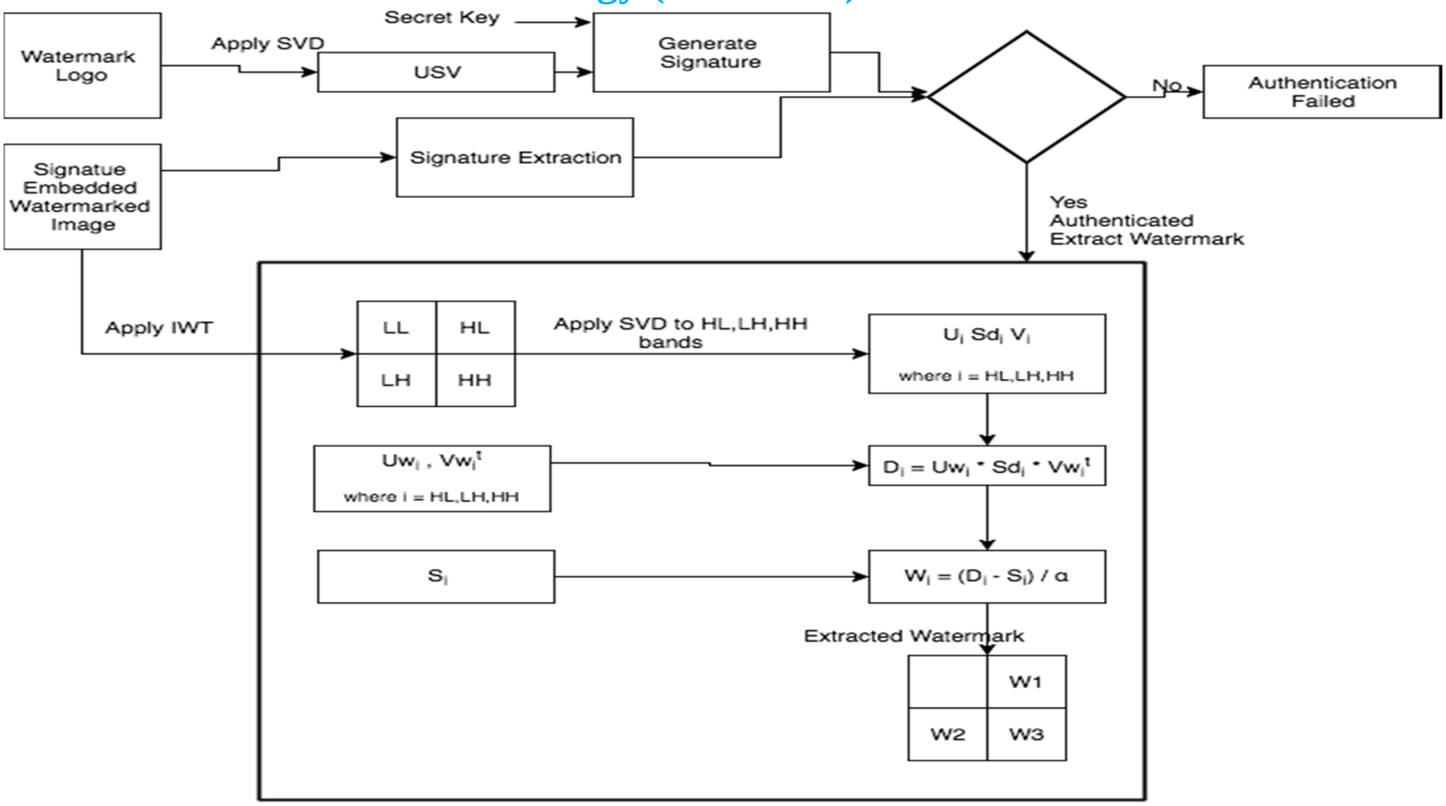

Fig 2 Watermark Extraction Procedure

C. Signature Generation Algorithm

1) Transform the 2-D orthogonal matrices(U and V) to 1-D arrays(by adding the columns of the matrices).
2) Convert the array into corresponding binary values, based on the threshold values (which is the median of the array) and then do XORing between them, named R1.
3) Using the secret key, generate a pseudo-random binary sequence of length R1 and store the result in R2.
4) By XORing R1 and R2, the signature is generated for authenticated purpose.

D. Signature Embedding Algorithm

1) Using DWT, decompose the watermarked image into 4 sub-bands : LL, LH, HL, HH. And then decompose the LL band upto 4th level.
2) Create 1-D array by concatenating the coefficient of LL4 and HH4 bands.(reshape LL4 and HH4)
3) Keep record of the index of negative coefficients and seperate the integer from the decimal fraction.
4) If the integer part is even and the signature bits equal one, or the integer part is odd and the signature bit equals zero, increase the integer part by one. Otherwise keep integer part unchanged.
5) Reconstruct original array by adding integer part and fraction part and then put back the negative signs.
6) Reshape the modified LL4 and HH4 bands and apply inverse DWT (four times)
7) Perform Inverse DWT.

E. Signature Extracting Algorithm

1) Using DWT, decompose the signature embedded watermarked image(possibly distorted) into four sub-bands: LL, LH, HL, HH. And then decompose the LL band upto 4th level.
2) Create 1-D array by concatenating the coefficient of LL4 and HH4 bands.(reshape LL4 and HH4)
3) Keep record of the index of negative coefficients and seperate the integer from the decimal fraction.
4) Extract the signature, based on the condition: if integer part is even then the signature bit is one, otherwise zero.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. SIMULATION RESULTS

A. Cover Image

Fig.3. Lena Cover image.

B. Watermark Image

Fig.4. Camerman as Watermark image

Figure 3 shows the original cover image whereas in Figure. 4 the cameraman as watermark image has been taken for embedding of watermark in the cover image

Figure.5 , Figure.6 , Figure.7 are the results of the above Images .Figure.7 is the watermarked Image which Is formed by embedding watermark logo into cover Image.

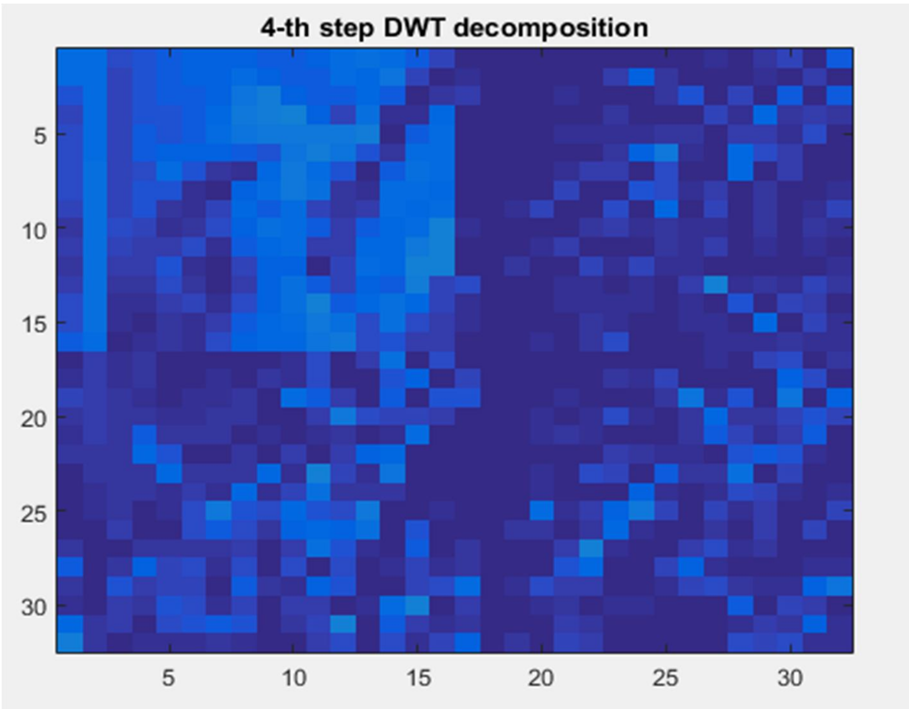

Fig.5 Fourth Step Decomposition

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

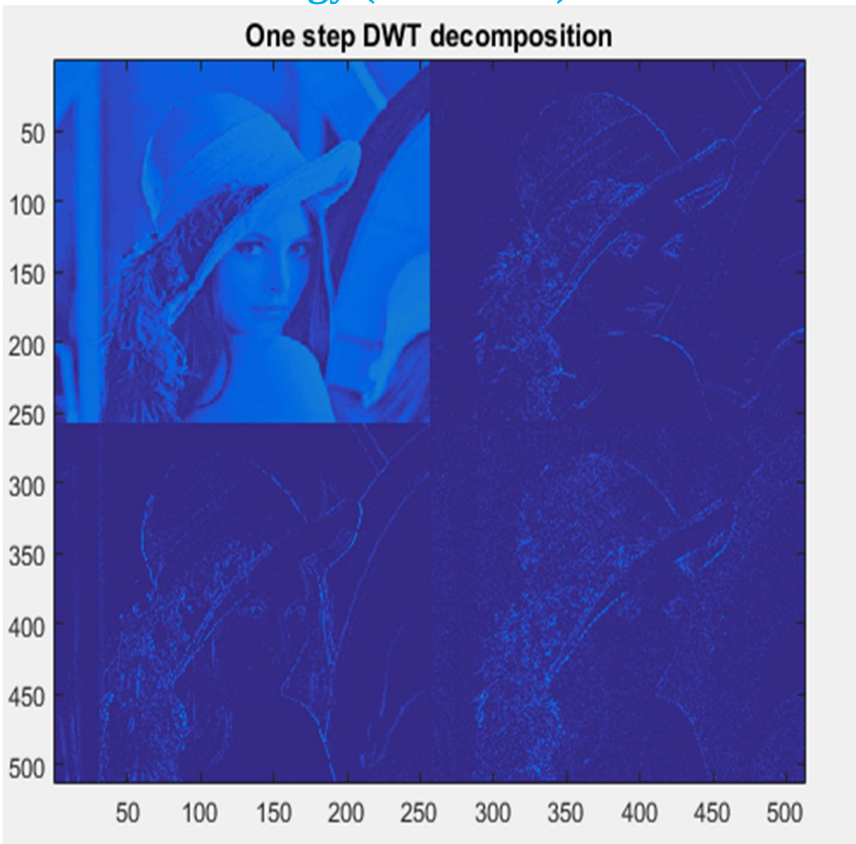

Fig.6 One Step Decomposition.

Fig. 7. Watermarked Image

V. PERFORMANCE MEASUREMENT

To check the quality of the watermarked image w.r.t the original image, PSNR (Peak Signal to Noise Ratio) is used. It can be calculated as:

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

$$PSNR = 10\log_{10}\frac{N \times N}{MSE} \qquad (1)$$

Where, NxN is the size of the image, and MSE is the Mean Square Error between the original A (i, j) and the watermarked image A' (i, j), can be written as:

$$MSE = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\frac{(A(i,j) - A'(i,j))^2}{N \times N} \qquad (2)$$

To find out the similarity between the original and extracted watermark, normalized correlation coefficient (NCC) is calculated. Its formula is:

$$NCC = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\frac{(W(i,j) \times W'(i,j))}{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(W(i,j) \times W(i,j))} \qquad (3)$$

Where, W (i, j), W' (i, j) are the original watermark image and the extracted watermark image respectively. NCC is a value between 0 and 1. The larger the NCC value, the higher the watermark robustness.

VI. CONCLUSION

A non-blind watermarking scheme based on IWT and SVD was implemented. Modifying Singular Values of the host image in IWT domain provides high robustness against the common attacks. High PSNR of watermarked image is another benefit of the algorithm as the result of IWT implementation .The proposed algorithm takes the advantages of the Wavelet Transform and SVD methods. The extracted watermarks are more robust against all mentioned attacks. IWT is useful for medical imaging and remote sensing applications because it produces lossless image. In future, this watermarking scheme can be extended to blind watermarking.

REFERENCES

[1] A.A. Mohammad, A. Alhaj, S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership", Signal Processing 88 (9) (2008) 2158–2180.
[2] C.-C. Chang, P. Tsai, C.-C. Lin," SVD-based digital image watermarking scheme", Pattern Recognition Letters 26 (10) (2005) 1577– 1586
[3] Chesta Jain, Vijay Chaudhary," Performance Analysis of Integer Wavelet Transform for Image Compression " IEEE conference 2011.
[4] Chin-Chin Lai ,"Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Transaction on Instrumentation and measurement Vol.59, No 11, November 2010
[5] S. Lingamgunta, V. K. Vakulabaranam, and S. Thotakura, "Reversible watermarking for image authentication using IWT.," International Journal of Signal Processing, Image Processing & Pattern Recognition, vol. 6, no. 1, 2013, pp. 145-156.
[6] I. J. Cox, J. J. Kilian, and T. G. Shamoon, Secure spread spectrum watermarking for multimedia data. Google Patents, 1999.
[7] I. J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking applications and their properties.," in itcc, 2000, pp. 6–10.
[8] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding",IBM System Journal, Vol. 35, NOS 3&4, pp. 313-336, 1996.
[9] E. T. Lin and E. J. Delp, "A Review of Data Hiding in Digital Images ",Proc. of the Image Processing, Image Quality, Image Capture Systems Conf. (PICS' 99), pp. 274-278, 1999
[10] P. H. W. Wong, O. C. Au and G. Y. M. Yeung, "A Novel Blind Multiple Watermarking Technique for Images", IEEE Transactions on Circuits and Systems for Video.