

Hybrid Image Watermarking using Second Level IWT-SVD

Manoj Kumar¹, Mahendra Kumar Pandey², Chetan Pathak³

¹Research Scholar, Dept. of Electronics and Communication Engineering, RJIT, Gwalior, INDIA

^{2,3} Assistant Professor, Dept. of Electronics and Communication Engineering, RJIT, Gwalior, INDIA

Abstract— with the widespread distribution of digital information over internet, the protection of intellectual property rights has become increasingly important. Digital Image Watermarking is one such technology that has been developed to protect digital images from illegal manipulations. This paper deals with watermarking technique based on Integer Wavelet Transform (IWT) and Singular Value Decomposition (SVD). In this proposed work, the cover image is decomposed at second level into four sub-bands (LL, LH, HL and HH) using IWT and thereafter SVD is applied to LL sub band. The singular values of cover image are embedded with singular values of watermark by making use of scaling factor. Performance of proposed work under with and without attacks has been analyzed. Experimental results demonstrated that IWT-SVD based watermarking technique is imperceptible and robust against most of the applied attacks such as; noise addition, resizing and filtering.

Keywords— Digital Image Watermarking, IWT, SVD, Attacks.

I. INTRODUCTION

Digital watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video [1-3]. The ease with which digital content can be exchanged over the internet has created copyright infringement issues. Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents.

Generally, the image watermarking can be done in spatial domain or in transform domain [4]. Compared to spatial domain techniques frequency-domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms [6-8]. Commonly used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) and IWT. However, DWT has been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system, but it has problem of down-sampling. Hence to overcome this problem here we use IWT (Integer Wavelet Transform) with SVD. IWT has better computational efficiency than DWT [9-12]. Also IWT performs lossless decomposition and hence it can be used for lossless data hiding. SVD is then performed on the transformed image, as SVD is more robust against attacks than traditional methods. It has the unique property that even large variations in the singular values do not affect the signal energy a lot [13-16].

Rest of the paper is organized as follows. Section 2 Describes methodology used in this paper. The proposed method is presented in Section 3. Section 4 describes experimental results and analysis with discussion. Section 5

describes the robustness analysis. Finally, Section 6 concludes the paper.

II. METHODOLOGY

A. Integer Wavelet Transform (IWT)

Integer Wavelet Transform is a flexible watermarking technique given by Sweldens [5]. Integer or Lifting wavelets are second generation wavelets that have distinctive advantages over first generation wavelets. IWT stores the multimedia content in integer value instead of floating value hence it reduces the computation time. Hence IWT is much faster than other transforms. The other property of IWT is less memory requirements because all computations for lifting wavelets are performed in integer domain unlike traditional wavelets (DWT) [17-18].

Applying IWT will help in increasing the robustness of watermark.

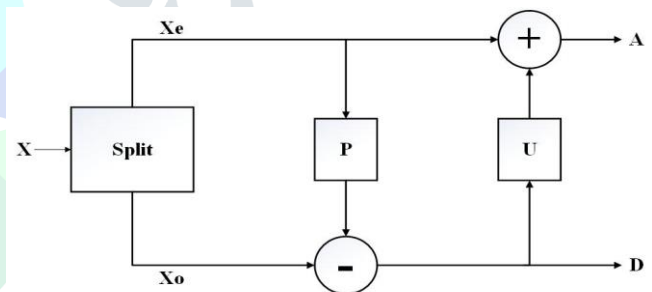


Fig. 1. One lifting Step Illustration

Figure 1 illustrates the single lifting step described by three basic operations: *Split*, *Predict (P)* and *Update (U)*.

Split: The signals are split into two subsets: the even sample set X_e and the odd sample set X_o , then modifying these values using alternating prediction and updating steps.

Predict (P): In this step, the odd sample X_o is replaced by the difference between the odd component and the predicted value.

Update (U): The update step is also known as primal lifting step.

B. Singular Value Decomposition (SVD)

In SVD transformation, a matrix can be decomposed into a multiplication of three matrices that are left singular vectors, set of singular values and right singular vectors.

SVD of an image M with dimensions $n \times n$ is given by:

$$M = USV^T \quad (1)$$

The columns of U are known as left singular vector and columns of V are known as right singular vectors of M . U and

V basically describe the geometry details of the original image. Horizontal and vertical details of the original image are represented by U and V, respectively. S is known as a diagonal matrix having positive singular values of matrix M. When minor variations in singular values of an image occur, it does not produce any noticeable change in the original image. Hence these value are more robust against various attacks.

III. WATERMARKING TECHNIQUE

The proposed algorithm is divided into two parts, watermark embedding and watermark extraction.

A. Embedding Process

The embedding process has following step as described below as following:

Step 1: Input the images; Cover and Watermark.

Step 2: Decomposition of both the images at second level into four sub-bands with IWT.

Step 3: After IWT, apply SVD on lower band of both the images, respectively.

Step 4: Compute new singular matrix using scaling factor and both singular matrix obtained from SVD.

$$S_{wm} = S_c + (\alpha * S_w);$$

$$new_LL = U_c * S_{wm} * V_c';$$

where,

S_{wm} = singular matrix of Watermarked Image,

S_c = singular matrix of Cover Image,

S_w = singular matrix of Watermark,

new_LL = lower band of Watermarked Image,

α = scaling factor.

Step 5: New LL band is computed with inverse SVD by using new computed singular matrix.

Step 6: After following the above steps, **Watermarked** image obtained by applying inverse IWT using new_LL band and remaining sub bands of Cover image.

B. Extraction Process

The watermark embedding process is described below:

Step 1: Input the obtained **Watermarked** image.

Step 2: Split the image up to second level into four quadrants by applying IWT.

Step 3: after performing IWT, apply SVD on low sub band .

Step 4: Compute new singular matrix using scaling factor work as key in watermark embedding process.

$$S_{w_n} = (S_{wm} - S_c) / \alpha$$

Step 5: Extract singular matrices with orthogonal matrices for final extracted watermark is calculated by formula:

$$W = U_w * S_{w_m} * V_w'$$

Step 5: Therefore, extracted watermark image obtained by performing inverse IWT on sub-bands .

IV. SIMULATION RESULTS

In simulation, proposed watermarking algorithm is applied on test image; Lena (size of 512×512) and Cameraman used as watermark image (size of 512×512). To evaluate the performance of the proposed IWT-SVD method, PSNR (Peak

Signal to Noise Ratio) and NCC (Normalized Correlation coefficient) values have been calculated.



(a) Lena (512x512) as Cover (b) Cameraman (512x512) as Watermark

Fig. 2. Input Images for Simulation

Evaluation Fidelity Parameter

❖ Peak signal-to-noise ratio (PSNR) :-

For measurement of imperceptibility, PSNR in dB is given by:

$$MSE = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (f_c(i, j) - f_{wm}(i, j))^2 \quad (2)$$

$$PSNR = 10 \log_{10} \frac{f_c^2(i, j)}{MSE} \quad (3)$$

where, $f_c^2(i, j)$ indicates the peak value of pixel and f_c, f_{wm} represent the host and watermarked images, respectively.

To evaluate the imperceptible capability, we can also use structural similarity(SSIM) index to measure the similarity between the original and the watermarked image with traditional method PSNR.

❖ Normalized Correlation Coefficient (NCC):-

To check the robustness and image quality, the value of Normalized Correlation Coefficient (NCC) is measured by:

$$NCC = \frac{\sum_{i=1}^N \sum_{j=1}^M g_w(i, j) * g'_w(i, j)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^M g_w^2(i, j)} \sqrt{\sum_{i=1}^N \sum_{j=1}^M g_w'^2(i, j)}} \quad (4)$$

where, g_w and g'_w are the original watermark and extracted watermark, respectively [11].

❖ Simulated Experimental Results

Simulated results on MATLAB platform using proposed work has been presented by considering Lena as a cover & cameraman as a watermark image.

Table I shows the fidelity parameters

Scaling Factor (S.F.)	IWT-SVD (Second Level)
-----------------------	--------------------------

Scaling Factor (S.F.)	Watermarked image	Recovered image
0.01		
0.02		
0.025		
0.03		
0.05		
0.1		
1		

α	PSNR (Watermarked Image)	SSIM (Watermarked Image)	NCC (Recovered Watermark)
0.01	48.32	0.9996	0.9761
0.02	41.01	0.9992	0.9942
0.025	38.82	0.9991	0.9968
0.03	37.06	0.9989	0.9968
0.05	32.25	0.9977	0.9963
0.1	25.94	0.9924	0.9998

1	8.92	0.6968	0.9206
---	------	--------	--------

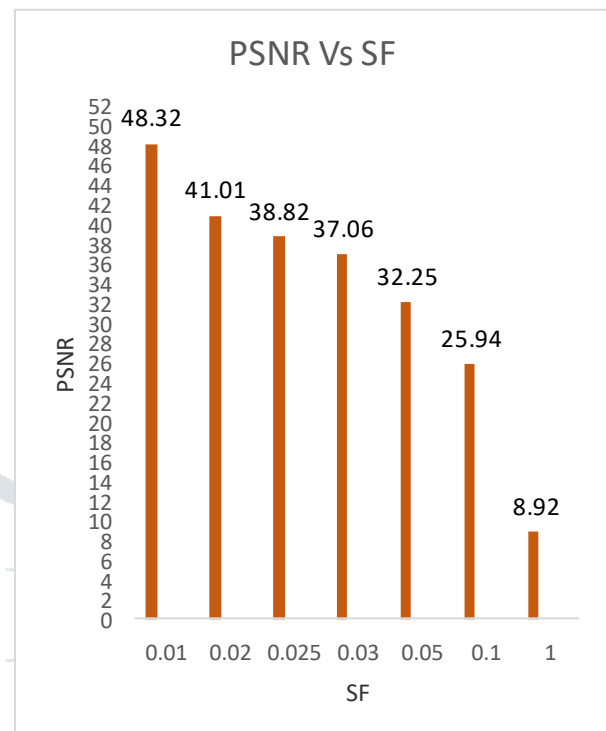


Fig. 3. Bar chart for PSNR at different value of S.F

Table I shows the values of PSNR, SSIM and NCC without applying any attack. The values of scaling factor; α has been varied from 0.01 to 1. Figures 4 show the watermarked and recovered watermark images at different value of scaling factor. From the simulated results it has been observed that as decrease the value of scaling factor, the value of PSNR increases but the same time the value of NCC decreases.

Fig. 4. shows the watermarked image and recover watermark image at different value of scaling factor

The simulated experimental results also evaluated with visual representation of watermarked and extracted watermark image for human vision system (HVS). Results are clearly seen that the proposed methodology having robust efficiency of watermarking with data hiding ability.

V. ROBUSTNESS ANALYSIS

Robustness is described as the resistance against non-geometrical and geometrical attacks and measured by NCC value. To test the robustness, the proposed watermarking technique has been tested against the various attack as listed in fig.5.

Fig. 5. shows the watermarked image and recover watermark image under various attacks.













From fig.5, it has been observed that the proposed method gives good value of recovered NCC after various attacks applied on watermarked image. This indicates that the proposed method is robust against various attacks.

VI. CONCLUSIONS

In this paper, a hybrid image watermarking technique based on a second level Integer wavelet transform has been presented and implemented. This technique can embed the watermark into salient features of the image using variable scaling factor. Experiment results shows that the quality of the watermarked image and the recovered watermark are dependent only on the scaling factors and also indicate that the 2-level IWT provide better performance. All the results obtained for the recovered images and the watermark are identical to the original images. Results are clearly seen that the proposed methodology having robust efficiency of watermarking with data hiding ability.

References

- [1] 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.
- [2] 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 Conference*, Vol. 299, pp. 274-278, April, 1999.
- [3] R. Liu, and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership", *IEEE Transactions on Multimedia*, Vol. 4, No. 1, pp. 121-128, March, 2002.
- [4] Kundur, Deepa, and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion", *Proc. IEEE International Conference on Image Processing*, Vol. 1, pp. 544-547, October, 1997.
- [5] W. Sweldens, "The lifting scheme: A construction of second generation wavelets", *SIAM J. Math. Anal.*, Vol. 29, No. 2, pp. 511-546, 1998.
- [6] Z. Zhou, B Tang, and X. Liu, "A Block-SVD based image watermarking method", *IEEE The Sixth World Congress on Intelligent Control and Automation*, Vol. 2, pp. 10347-10351, June, 2006.
- [7] A. Miyazaki, and F. Uchiyama, "An image watermarking method using the lifting wavelet transform", *IEEE International Symposium on Intelligent Signal Processing and Communications*, pp. 155-158, December, 2006.
- [8] Lee, Sunil, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform", *IEEE Transactions on Information Forensics and Security* 2.3, pp. 321-330, September, 2007.
- [9] Loukhaoukha, and J. Y. Chouinard, "Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification", *IEEE, 11th Canadian Workshop on Information Theory, CWIT 2009*, pp. 177-182, May, 2009.
- [10] L. Hu, and F. Wan, "Analysis on wavelet coefficient for image watermarking", *IEEE International Conference on Multimedia Information Networking and Security (MINES)*, pp. 630-634, 2010.
- [11] S. Lagzian, M. Soryani, and M. Fathy, "A new robust watermarking scheme based on RDWT-SVD", *International Journal Of Intelligent Information Processing*, Vol. 2, No. 1, March, 2011.
- [12] M. Thapa, Dr S. K. Sood, and A. P. M. Sharma, "Digital image watermarking technique based on different attacks", *International Journal of Advanced Computer Science and Applications*, Vol. 2, 2011.
- [13] Kashyap, Nikita, and G. R. Sinha, "Image watermarking using 2-level DWT", *Advances in Computational Research* 4.1, pp. 42-45, 2012.
- [14] 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, 2013.
- [15] A. Kala, and K. Thaiyalnayaki, "Robust lossless image watermarking in integer wavelet domain using SVD", *International Journal of Computer Science Engineering*, pp. 30-35, 2013.
- [16] Makbol, Nasrin, and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition", *Digital Signal Processing* 33, pp. 134-147, October, 2014.
- [17] Purna Gupta and G.Parmar, "Image watermarking using IWT-SVD and its comparative analysis with DWT-SVD", *Proc. IEEE International Conference on Computer, Communications and Electronics (COMPTLIX-2017)*, pp. 527-531, July, 2017.
- [18] N.Chawla, Mahendra Kumar Pandey " Lifting scheme based non-blind hybrid image watermarking technique using low frequency band", *7th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, (2017).

Attacks	NCC	Attacked Image	Image attacked
Salt & Pepper Noise at 0.001 density	0.9962		
Poisson Noise	0.9630		
Gaussian Noise at 0.001 Variance	0.9815		
Speckle Noise at 0.001 Variance	0.9939		
Resize attack 50%	0.9968		
Median filtering [3x3]	0.9277		
Rotate 1 degree	0.4748	