A ROBUST IMAGE WATERMARKING USING BWT-SVD

Sumalatha Muthyala[1], Sivadanam Bharath Kumar[2], Prof. B. SubbaReddy[3]
N.B.K.R. Institute of Science & Technology, Vidyanagar.
Email: [1]Sumalatha495@gmail.com, [2]sivadyanams@gmail.com , [3]subbareddy.bellapu@gmail.com

Abstract: **The digital world has many advantages in making the information available to every one without any discrepancy. With the internet connection any one can access everything whichever is available in the World Wide Web. At the same time, accessing unauthorised content or information theft is also made possible. The security of the information has become a challenge. One of the many solutions for the information security copy right protection is watermarking. In this present work, Biorthogonal Wavelet Transformation in combination with Singular Value Decomposition is used to embed the authentication data, sometimes also called logo, i.e., the watermark, into the host image, which improves the robustness compared to many other watermarking methods proposed till now. The watermark is embedded in the host image by modifying the coefficients of the middle frequency coefficients of the BWT filter so that the quality of the host image will not get disturbed or the disturbance will not be found with naked eye, at the same time the watermark cannot be removed by standard attacking methods. Its robustness has been compared with discrete cosine transform, discrete wavelet transform and stationary wavelet transformation. The simulation results shows that among these four methods, biorthogonal method has more robustness against standard attacks. The standard Lena image is used for simulation purpose.**

Keywords: **watermark, host, robustness, biorthogonal wavelet transform, SVD, DWT, SWT, DCT, copyright protection.**

1. INTRODUCTION

According to DailyMail News Journal, Every minute hundreds of terabytes of data is being uploaded into the World Wide Web in different digital forms like text, images, videos and audio[1]. This digital media is very easy to copy and transmit and even to store. It also includes the many issues like copy right protection, piracy and content authentication or proof of ownership. This digital information, whatever may the form, can be easily manipulated with the available sophisticated digital signal processing tools and algorithms. Such manipulations raise serious questions about the integrity and authentication of information. Watermarking is one among so many authentication techniques. Watermarking is a method of embedding authentication information directly into digital content either perceptibly or imperceptibly. If authentication is visible to naked eye it is known as visible watermarking and in other case it is known as invisible watermarking. Below images are the examples for visible and invisible watermarking techniques, with N.B.K.R.I.S.T. logo as watermark.


Fig-1: Visible Watermarking Fig-2: Invisible Watermarking

Watermark in images can be embedded either in spatial domain or in frequency domain. Spatial techniques are simple and efficient but not robust, sometimes spatial watermarking disturbs the quality of the host image. Frequency domain watermarking is complex and also robust and effective than spatial watermarking.

Among many types of techniques wavelets gained many advantages in watermarking, like invisibility and its robustness [2]. Wavelets also gives very good compression with less loss or lossless over high resolution images [3],[4],[5]. DCT, DWT are the mostly used frequency domain watermarking techniques. Discrete wavelet transform have higher de-correlation and frequency, thereby high resolution images can be represented efficiently with few number of coefficients. The watermark is inserted into wavelet coefficients of the host image and its amplitudes are controlled by wavelet coefficients [6]. Many researchers have performed wavelet decomposition at two level, three level and four level by using haar, 7/9-biorthogonal, daubechies 16 etc. wavelet transformations [7],[8],[9],[10][11]. In this present paper, biorthogonal wavelet and singular value decomposition are used and its robustness is verified. Compared to the robustness with SWT-SVD[15], the present technique has got better robustness except without any attacks.

2. OVERVIEW OF BWT

The wavelet transforms have gained widespread acceptance in signal and image processing techniques. Because of their inherent multi-resolution nature, wavelet-coding schemes are especially suitable for applications where scalability and tolerable degradation are important, especially in image compression techniques. The elementary idea of wavelets is using the same function by expanding and shifting to approach the original signal. The wavelets can maintain the fine structure of the original signal or image in various resolutions.

A biorthogonal wavelet is a wavelet where the associated wavelet transform is invertible but not necessarily orthogonal. Designing biorthogonal wavelets allows more degrees of freedom than orthogonal wavelets. One additional degree of freedom is the possibility to construct symmetric wavelet functions. In the biorthogonal case, there are two scaling functions, ϕ, $\tilde{\phi}$, which may generate different multi-resolution analyses, and accordingly two different wavelet functions ψ, $\tilde{\psi}$. So the numbers M and N of coefficients in the scaling sequences $a, \tilde{a}$ may differ. The scaling sequences must satisfy the following biorthogonality condition

$$\sum_{n\in \mathbb{Z}} a_n \tilde{a}_{n+2m} = 2 \cdot \delta_{m,0}$$

Then the wavelet sequences can be determined as[11]

$$b_n = (-1)^n \tilde{a}_{M-1-n} \qquad (n = 0,1,\ldots N-1)$$
$$\tilde{b}_n = (-1)^n a_{M-1-n} \qquad (n = 0,1,\ldots N-1)$$

Compared with the orthogonal wavelet, biorthogonal wavelet has gained more superiority in image processing, as it can maintain the orthogonality and symmetry in balanced way. In addition, the reconstructing signal of the biorthogonal wavelet transform is suitable to embed watermark for its balance. Daubechies9/7 wavelet is recommended in JPEG2000. In this paper, ‘9/7’ pair of CDF (Cohen, Daubechies and Feauveau) is used for embedding and retrieval of watermark. The CDF ‘9/7’ pair is obtained by factorizing the length 16 Lagrange Half band Filter which has a large number of zeros at z= -1 that is maximum number of vanishing points.[14].

A digital image is decomposed into three high frequency subbands and one low frequency subband by one level wavelet transform. The Low frequency subband can be decomposed continuously. With the more levels the image is decomposed by wavelet transform. The energy of the watermark is diffused into better, and stronger watermark intensity can be embedded. For better robustness of the watermark embedding, three level decomposition is used in this algorithm. With three level wavelet decomposition, the image will be as shown below. Watermark can't be embedded into either low frequency content or into high frequency content since sharpening or smoothing, respectively, of image will remove the watermark from the host easily. If watermark is embedded in the mid-band region, the watermark can be made more robust and also the quality of the image will be retained.

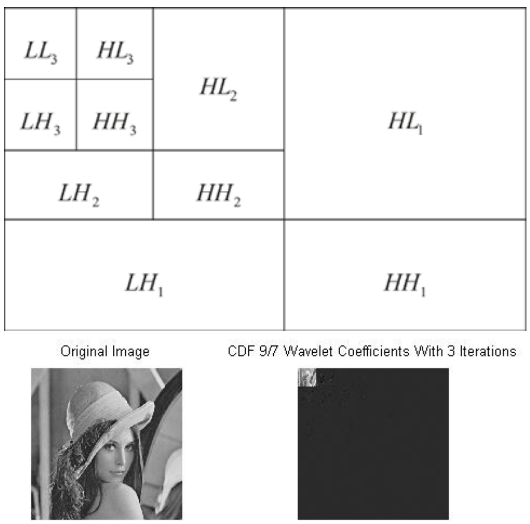


Fig-2: Three level decomposition of Lena image

3. OVERVIEW OF SVD

Singular value decomposition (SVD) is a general linear algebra technique for a variety of applications including solving most linear least-squares problems, computing pseudo-inverse of a matrix and multivariate analysis. SVD can be looked at three mutually compatible points of view. It can also be looked as a method for transforming correlated variables into a set of uncorrelated ones that better expose the various relationships among the original data items. At the same time, SVD is a method for identifying and ordering the dimensions along which data points exhibit the most variations. SVD can be seen as a method for data reduction. This tie into the third way of viewing SVD, which is that once the location where most variation has occurred, it is also possible to find the best approximation of the original data points using fewer dimensions. Hence, SVD can be seen as a method for data reduction [16]. Any M × N (M $\geq$ N) real matrix A, can be written as

$$A = USV^T = \sum_{i=1}^{N} s_i U_i V_i^T \; (1 \le i \le N) \text{ ----(1)}$$

where U and V are orthogonal matrices, and S is an M ×N matrix with the diagonal elements s_i representing the singular values of A. U_i is the i-th column vector of U, V_i is the i-th column vector of V. U_i, V_i are called left and right singular vectors of A respectively. S has the structure of

$S = \begin{pmatrix} S_1 \\ 0 \end{pmatrix}$, where

$$S_1 = \begin{pmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ & & . & \\ 0 & 0 & 0 & s_n \end{pmatrix} \text{----------- (2)}$$

4. PROPOSED ALGORITHM

A. Watermark Embedding

Let A represent the host image of size M×M, W represent the watermark image of size N×N, and we assume M = 2N, then the embedding process can be described as following steps:

1) Use BWT to decompose the host image into four subbands: HL_2, LH_2, and HH_2.

$A \Rightarrow I_s$ $(s \in 2\{HL_2, LH_2, HH_2\})$ -----(3)

Low frequency coefficients are avoided in embedding the watermark as it may disturb the image. In other words, distortion in the image can be observed after watermarking.

2) Apply SVD to each subband image.

$I_s \Rightarrow U_s S_s V_s^T$ -----------(4)

3) Compute the SVD of the watermark image.

$W \Rightarrow U_w S_w V^T_w$ ------(5)

4) Modify singular values of the host image in each subband according to those of the watermark image.

$\hat{I}_s \Leftarrow U_s(S_s + \alpha_s S_w)V_s^T$ ----(6)

5) Apply inverse BWT to four sets of modified BWT coefficients to produce the watermarked image.

$\hat{A} \Leftarrow \hat{I}_s$ ---------------------------(7)

Since the most important singular value is the first one, s_1, so we use s_1 to limit the embedding strength.

B. Watermark Detection

In order to recover the watermark from the watermarked image, reverse process is applied. The watermarked image is decomposed using the biorthogonal wavelet transform. In short, the watermark detection process is just an inverse of equations (3)–(7), and can be represented as below:

1) Use BWT to decompose the watermarked (and possibly attacked) image.

$\hat{A} \Rightarrow \hat{I}_s$ $(s \in \{HL_2, LH_2, HH_2\}$------(8)

2) Apply SVD to each subband of the watermarked image.

$$\hat{I}_s \Rightarrow \hat{U}_s \hat{S}_s \hat{V}_s^T \quad \text{----------- (9)}$$

3) Extract singular values of the watermark image from each subband.

$$\hat{S}_{ws} \Leftarrow \frac{\hat{S}_S - S_S}{\alpha_S} \quad \text{----------(10)}$$

4) Construct four watermark images from four subbands.

$$\hat{W}_s \Leftarrow U_w \hat{S}_{ws} V_w^T \quad \text{---------(11)}$$

The proposed scheme is a non-blind for (8)–(11) need both the host and watermark images.

5. EXPERIMENT RESULTS

The Biorthogonal wavelet transform has got some unique properties. Biorthogonal wavelet transform has perfect reconstruction of the image or signal and it has linear phase properties which make the transform much better and more robust compared to other transforms. Therefore it also produces more accurate results, even against many attacks on the watermarked image. The robustness is evaluated based on the peak signal to noise ratio, PSNR. The proposed algorithm is implemented and tested using the standard test image Lena and NBKRIST college logo as watermark. The results are shown in below figures. The distortion in image is measured using PSNR, one of the best measure for distortion used for images and video coding. PSNR is measured in decibels. The PSNR is the objective criteria used to measure the quality of the watermarked image. Similarly the quality of the extracted watermark is measured by comparing it with the original watermark and is called similarity measure. To compute the PSNR, the mean-squared error is first measured using the formula,

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M \times N} \text{ ---- (12)}$$

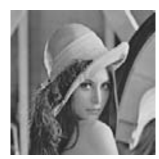
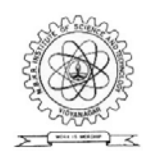
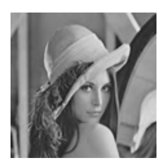
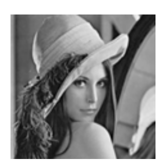
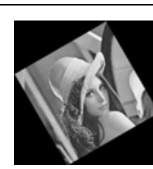
In the equation-(12), M and N are the number of rows and columns of the input image respectively. The PSNR is evaluated using the equation,

$$PSNR = 10\log_{10}\left[\frac{R^2}{MSE}\right] \text{ ----- (13)}$$

In equation-(13), R is the maximum fluctuation in the input image data type. The quality of the watermarked image is measured and tabulated in Table-I.

For computational simplicity during simulation, the Lena image is selected as the host image and college logo is considered as the watermark image. The results were shown in Table-I. Even after many attacks, the watermark/logo has sustained without much quality loss. The same can also be simulated with any other image of our interest.

Table I: Attacked host images and retrieved watermarks

Type of attack	Image	Watermark
Original or No Attack		
Compression		
Cropping		
Rotation		

Salt & Pepper Noise		
Speckle Noise		
Gaussian Noise		

Table II: PSNR values of the retrieved watermarks

Type of attack	PSNR	MSE
Original or No Attack	61.98432	0.0415
Compression	46.54423	1.4523
Cropping	34.37045	23.9571
Rotation	34.187632	24.9872
Salt & Pepper Noise	44.06851	2.5682
Speckle Noise	41.60775	4.5259
Gaussian Noise	45.32027	1.9251

Table – II indicates the respective MSE and PSNR values corresponding to Table-I. The use of biorthogonal wavelets requires a careful selection of scaling vector used to determine the strength of the watermark. Due to the watermark embedding function [13], image artefacts are produced by embedding watermarks that are too large. Likewise using a wavelet of large energy requires a further reduction of the watermark magnitude. Ideally, to achieve a highly robust watermark, a high watermark should be embedded into wavelet coefficients obtained from a low energy filter. Thus, a compromise between the robustness and invisibility of the watermark is required. Sufficiently reducing the strength of the watermark in such cases will remove any artefacts.

6. CONCLUSION

With the above results, it is evident that the biorthogonal wavelets offer sufficient robustness and security to particular watermark attacks. Because BWT is combined with SVD, it is observed that robustness increased further. By adaptively setting the strength of the watermark, better results might be achieved as in this case. This measure also ensures the invisibility of the watermark. In this paper watermarking technique is investigated only over gray-scale images. This can be further extended with colour images. While embedding the watermark in the host image, low frequency coefficients have not been considered, since it will introduce distortion which can be easily noticed. By considering JND, LL_2 can also be taken into consideration for watermarking.

7. REFERENCES

1. http://www.dailymail.co.uk/sciencetech/article-2381188/Revealed-happens-just-ONE-minute-internet-216-000-photos-posted-278-000-Tweets-1-8m-Facebook-likes.html
2. “Comparison of different wavelets for watermarking of colour images”, Achintya Singhal, Rudra Prathap Singh, Monal Tenguria, 3rd International Conference on Electronics Computer Technology, pp: 187-190, Vol-3, 2011.
3. Devore R.A., Jawerth B, Lucier B, “Image compression through wavelet transforms coding”, IEEE transaction on information theory, 38(2), pp:719-746, 1992.
4. Antonini M, Barland M, Mathieu P and Baubechies, “Image coding using the wavelet transform”, IEEE transactions on image processing, vol-1, pp 205-220,(1992,April).
5. Lewis A S and Knowles G, “Image compression using the 2D wavelet transform”, IEEE transactions on image processing, Vol-1, pp:244-250, 1992,April.
6. “Perceptual digital watermarking of images using wavelet transform”, Wei Z H, Qin P and Fu Y Q, IEEE transactions on consumer electronics, vol-44(4), pp: 1267-1272 (1998, November).

7. Xia X, Boncelet C G, and Arce G R, "A multiresolution watermark for digital images", International Conference on Image Processing, ICIP 97, Vol-1, pp: 548-551 (1997, September).
8. Inove H, Miyazaki A, Yamamoto A and Katsura T, " A digital watermark based on the wavelet transform and its robustness on image compression", International Conference on Image Processing Proceedings, ICIP 98, Vol-2, pp:391-395 (1998, October).
9. Wolfgend R B, Podilchuk C I, and Delp E J, "The effect of matching watermark and compression transforms in compressed colour images", ICIP Proceedings, ICIP 98, Vol-1, pp:440-444 (1998, October).
10. "Wavelet based watermarking for tamper proof of still images", International Conference of Image Processing Proceedings, ICIP 2000, pp: 88-91 (2000 October)
11. Wolfgang R B, Podlchuk C I, and Delp E J, "Perceptual watermarks for digital images and videos", Proceedings of IEEE special issue on Identification and Protection of Multimedia Information, Vol-7, pp:1108-1126 (1999, July)
12. "A wavelet tour of signal processing", Academic Press, Stéphan G Mallot, 1999.
13. "Biorthogonal bases of compactly supported wavelets", A Cohen, I Daubechies and J.C.Feauveau, Communications on Pure Applied Mathematics, pp:485-560, 1992.
14. "A study of biorthogonal wavelets in digital watermarking", slaven Marusic, David B H Tay, Guang Deng and marimuthu Palaniswami, Internations Conference on Inage Proceesing Proceedings, ICIP 2003,Vol-2, pp:463-466, September 2003.
15. "Robust SWT SVD based digital image watermarking technique", Sivadanam Bharath Kumar, Dr. Tirumala Ramashri, International Journal of Computer Science Information and Engineering Techmologies, ISSN 2277-4408, Issue 2, Volume 2, Series 1, May 2012.
16. "Singular value decomposition tutorial", Kirk Baker, March 29th,2005(Revised January 14th, 2013).