INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue3)
Available online at www.ijariit.com

A Watermarking Approach in DWT Domain using SYMLET and COIFLET Filters

Akanksha Singh
M.Tech Computer Science
(Software Engineering)
BBDU Lucknow
Akankshasingh9495@gmail.com

Mohd. Saif. Wajid
Assistant Professor
Computer Science and Engineering
BBDU Lucknow
mohdsaif06@gmail.com

Abstract: Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. Watermarking has a number of uses in security, authentication and registration purposes. Image Watermarking is a widely sought after research area and many researchers have done extensive study on various aspects of digital image watermarking. Out of those techniques DWT based techniques are quite popular. In this research work a novel algorithm has been presented for Digital Image Watermarking, which uses the DWT technique to perform Watermark embedding and extraction process. The wavelet filter are of many kinds and erstwhile research have been mostly carried on 'haar' and 'daubechies' wavelet filter. In this research work, 'symlets' and 'coiflet' filters have been used. A comparative study of results in terms of PSNR and MSE with other filters is also available to give a better reasoning and insight.

Keywords: Watermarking, DWT, haar, coiflet, symlet, wavelets.

I. INTRODUCTION

Watermarking has been in use around since ages, in the form of watermarks found initially in plain paper for document authentication and on currency notes to provide fake note detection. .There has been an increase in the research on Digital Watermarking owing to an increase in the digital services like multimedia, telecommunication and internet. With the growing usage of these technologies and the ease with which multimedia data such as image, video, songs etc. can be transferred from one device to other device has also led to a threat of it being copied and forged to appear altogether different using tools which are easily available. In such a scenario it is of utmost importance to have certain mechanism for digital data copyright protection and authentication. Watermarking provides a solution to this problem. Watermarking as has been understood by this research is an act of embedding some form of data inside or over another piece of data or information. For example, the University Documents generally come with a Logo or name watermark in the backdrop of a text document. Thus, its gives an authentication that the particular document has been issued by the University and an authentic data of the University.

Likewise, there are other examples of watermark. Another such example can be an image or video where the watermark data can be hidden inside the original content. Based on the visibility of the watermark, it can be divided into two type's visible watermark or invisible watermark. The example of document watermarking with university logo is an example of visible watermarking. In case of image, video or song, invisible watermarking is used.

Several techniques and methods have been proposed and implemented in the past years to perform digital watermarking in multimedia data. In this research paper, Digital Image Watermarking is of particular interest. There are various techniques like LSB substitution method, Pixel Value Differencing, Quantization index modulation etc., in the spatial domain. In frequency domain there are different methods which use the Discrete Cosine Transform and Discrete Wavelet Transform techniques to achieve the watermarking. In this paper a novel algorithm has been proposed and implemented which uses a DWT based approach to perform Watermark Embedding and Extraction. The Wavelet domain gives a frequency domain analysis of the available signal and divides it ito low frequency and high frequency sub bands. This is performed using wavelet filters. There are a number of filters available in the wavelet domain, the first and foremost being the 'haar' filter. In most of the methods and algorithms used for Digital image Watermarking 'haar' filter or its clone, the 'daubechies1' filter has been used to implement the watermarking. In this research work, we propose a novel method which uses the 'symlets' and coiflet' wavelet filters for performing the Image Watermark embed and extraction.

The next section gives a literature review followed by the proposed implementation framework in Section III. Section IV gives the analysis and result and finally Section V gives the Conclusion.

II. LITERATURE REVIEW

In spatial domain of watermarking, the secret information is directly embedded in pixel values of the image or in other words pixels are directly altered to store secret messages. These techniques are very simple but have greater impact then other techniques on the resultant image reducing visual perceptibility.

Least Significant Bit (LSB) substitution algorithm is one of the simplest form of algorithm in which LSBs of the cover image(the image inside which secret message is to be hidden), is modified according to the secret message. It is simple yet effective technique of embedding secret data into images. The bits in a pixel vary from 8 bits in case of Gray scale images to colored RGB images which use 24 bits to store color information where 8 bits each is used for for Red, Green and Blue components. This method can achieve high embedding capacity but this algorithm is sensitive to image manipulations such as cropping, scaling and rotations, lossy compression and addition of noise.

There are a number of techniques which can be seen as of variation of this algorithm including edge and texture masking of cover image to determine the number of bits of LSBs for data embedding [3], Adaptive LSB algorithm based on brightness, optimized LSB algorithm using cat swarm and genetic algorithm [4,5], image steganography based on histogram modifications [6,7] etc.

Pixel Value Differencing is another technique that sub divides the cover image into non overlapping blocks consisting of two connecting pixels. This technique uses an algorithm where the difference between two connected pixels is altered. High difference in the cover image pixel values, allows more changes. The area in which pixel exists over the whole image is used to decide the hiding capacity of this technique for example if edge area is chosen then the difference is high, between the connecting pixels, where as in normal areas, difference is low. So, ideal choice can be to select edge areas to embed the secret message that has more embedding capacity. Watermarked or stego image obtained by this technique has better quality and has better imperceptibility results [8].

Grey Level Modification technique the data is mapped by applying some modifications to the grey values of the image pixels. This technique doesn't hide or embed data, instead it map the data by using some mathematical functions. Set of pixels are selected for mapping using this mathematical function. It uses the concept of odd and even numbers for mapping the data in cover image. High hiding capacity and low computational complexity are some advantages of this technique [9].

Prediction based Steganography technique pixel values are predicted with the help of predictor. This technique is an improvement over techniques which directly embed the secret data into pixel values and remove their loopholes to a certain extent. This technique uses prediction error values, of the pixels which are altered to hide the secret data. It consists of two steps, the prediction step followed by entropy coding. In prediction step predictors are used to determine the pixel values of a cover image and in the second step entropy coding of prediction error values is done.

Quantization Index Modulation (QIM) is another technique used for spatial domain watermarking in which secret information is embedded in cover image by modulating an index with embedded information and after that quantization process is applied to the host signal with associated quantizers. This technique has a number of advantages such as high embedding capacity and is a highly robust technique.
Transform domain steganography techniques are the most complex way to embed the secret data in the cover image.
An image in digital form is made up of high and low frequency components. Digital image can have smooth and edge (sharp) areas. Smooth areas represent low frequency whereas high frequency is represented by edge or sharp areas of the cover image. Changes done in low frequency areas can easily be visible to human eyes. So it is not possible to embed equal amount of secret information in all the regions. It has number advantages over the spatial domain methods of steganography such as it is more robust against compression, image processing and cropping and these methods are less prone to attacks.

In frequency domain watermarking, the cover data is considered as communication medium. The watermark is considered as a signal that is passed through this medium. In frequency domain watermarking the cover medium is converted to frequency domain before adding the watermark. After the insertion of the watermark, the medium is inversely transformed to get the watermarked medium in the spatial domain. The watermark inserted in the frequency domain ensures high level of security. The watermark is spread in such a way that the position of the watermark in not known. Moreover, watermark destruction brings severe degradation to the watermarked medium.

The most popular methods in this domain are DCT and DWT. Nowadays a number of researchers have focused their research on these two methods. Cox proposed a non-blind watermarking technique. The technique is based on using spread spectrum for inserting a watermark in DCT domain [10]. A Gaussian random sequence is used as a watermark. The watermark is inserted imperceptibly in a spread spectrum-like fashion. The technique proposed was robust to majority of geometric and common signal processing attacks like compression, analog-to digital and digital-to-analog conversion etc. But the major limitation of the technique is that it requires the original image to register it against the transformed watermarked image. Harrak et al. proposed a watermarking technique in [11].

In wavelet based methods an image is decomposed into different sub-bands. A wavelet based watermarking technique is proposed. In this technique every watermark bit is embedded in various frequency bands. The technique spread the watermark information in large spatial regions of the cover medium. The technique is able to survive the frequency based attacks for example removing the high frequency areas through low-pass filter, and the removal of high-pass details in JPEG compression. The technique is also resistant against the time based attacks like rotation and pixel shifting. This technique is not imperceptible because of using a fix watermarking level for the whole image. The technique proposed by Huang is a blind technique in which the original image is not required at the time of detection [12]. In this technique, Hue variance saturation (HVS) values of the cover image are used to insert the watermark in wavelet domain. In this method four adjacent coefficients after conversion to wavelet domain are grouped. Watermark is then added to the average of these four adjacent coefficients.

III. Wavelet Analysis

Wavelet analysis is able to reveal signal aspects that other analysis techniques may miss, such as trends, breakdown points, discontinuities, etc. it is assumed that low frequencies last for the entire duration of the signal, whereas high frequencies appear from time to time as short burst. This is often the case in practical applications. The wavelet analysis calculates the correlation between the signal under consideration and a wavelet function (t). The similarity between the signal and the analyzing wavelet function is computed separately for different time intervals, resulting in a two dimensional representation. The analyzing wavelet function f(t) is also referred to as the mother wavelet.

For the DWT special families of wavelet functions are developed. These wavelets are compactly supported, orthogonal or biorthogonal and are characterized by low-pass and high-pass analysis and synthesis filters. Some generally used families for the DWT are discussed in this section.

The Daubechies familiy is named after Ingrid Daubechies who invented the compactly supported orthonormal wavelet, making wavelet analysis in discrete time possible. The first order Daubechies wavelet is also known as the Haar wavelet, which wavelet function resembles a step function.

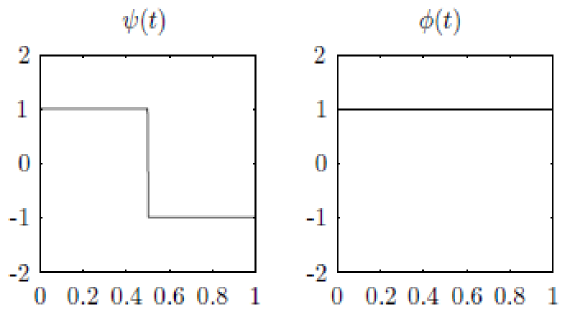

Figure 1: Haar Wavelet (db1)

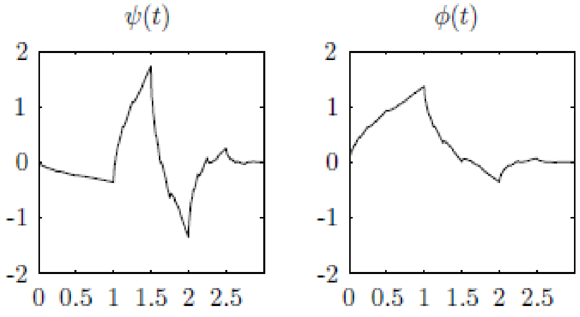

Figure 2: db2 wavelet and scaling function

Coiflets are also build by I. Daubechies on the request of R. Coifman. Coifman wavelets are orthogonal compactly supported wavelets with the highest number of vanishing moments for both the wavelet and scaling function for a given support width. The Coiflet wavelets are more symmetric and have more vanishing moments than the Daubechies wavelets.

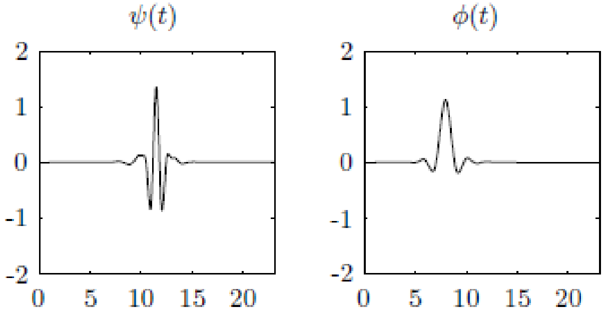

Figure 3: Coiflet wavelet and scaling function

Symlets are also orthogonal and compactly supported wavelets, which are proposed by I. Daubechies as modifications to the db family. Symlets are near to being symmetric and have the least asymmetry. The associated scaling filters are near linear-phase filters. The properties of symlets are nearly the same as those of the db wavelets.

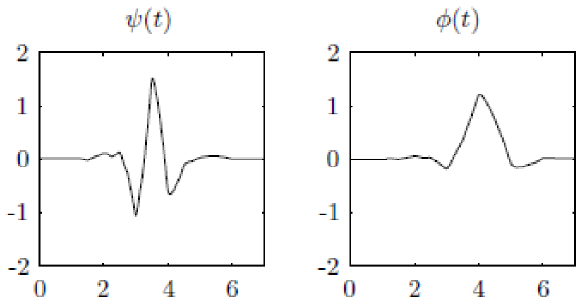

Figure 4: Symlet Wavelet and scaling function

There are a number of wavelet families apart from the above mentioned wavelet families.

IV. PROPOSED WORK

The Discrete Wavelet transform technique has been used to transform images from their original spatial domain to frequency domain. The watermark generated is then inserted into one of the frequency bands in the DWT sub bands. The detailed architecture of the watermark embedding and extraction is shown in the Figure 5.

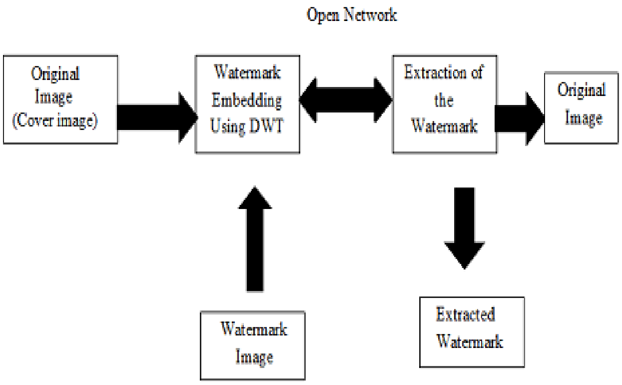

Figure 5: General System Architecture

The detailed algorithm is as shown below.

- Input Cover Image
- Preprocess for type and size
- Apply 2D-DWT using different filters viz. db1, sym1.
- Select subband for Watermarking.
- Find out weight factor S(i,j) for HH subband.
- Generate Watermark Key Image
- Perform Embedding

$$Y = cv + c*abs(cv).*N \quad (1)$$

where cv is the DWT coefficient in which the embedding is done, c is the watermark weight, N is the size of hidden image

- Perform Inverse DWT.
- The watermarked image is obtained
- Extraction:
- Read in the watermarked image.
- Perform DWT.
- Obtain Coefficients of Hidden message, using below equation:

$$cc = abs(cv1./N) \quad (2)$$

Where cc is hidden message, cv1 is the coefficients of DWT and N is watermark size

The haar, symlet and coiflet wavelet filters have been used to perform the Wavelet transform.

V. Results

Extensive experiments have been performed on a number of images to analyse the working of the algorithm. Several standard test images such as boat, baboon, Lena, peppers, couple, cameramen etc are referred to in the present paper for watermark embedding and watermark detection. The technique is not limited to the use these cover images but we have used them as they are standard images widely used by other researchers working on watermarking. They all are gray scale images with size 256x256. All the images are watermarked using the best evolved expression.

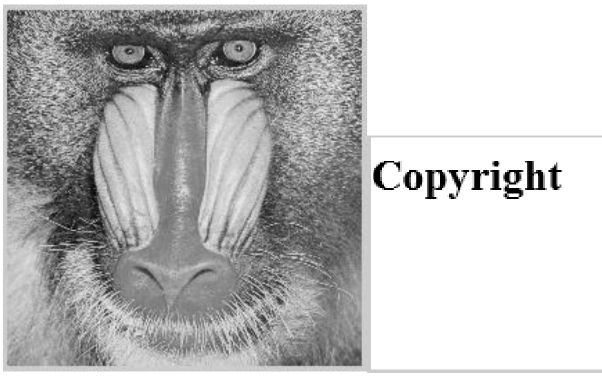

Figure 6: Cover Image(Baboon) and Hidden Image

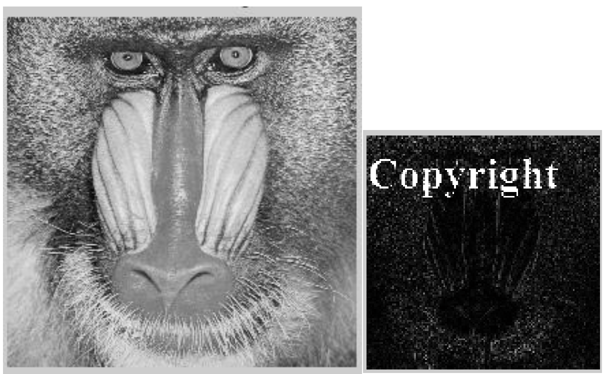

Figure 7: Watermarked Image and Retrieved hidden Image using haar wavelet

Figure 6 shows the original image of baboon and the key image. Figure 7 shows the watermarked image which is watermarked using the best evolved expression the and retrieved watermark under no attacks. There is no perceptual distortion in the watermarked image which shows the high imperceptibility of the proposed technique. It can be observed that the proposed method is able to learn the spatial distribution of the baboon image.

Figure 8: Peppers Image (Original and Watermarked) using symlet filter

Figure 9: Boat Image (Original and Watermarked) using coiflet filter

Figure 8 and figure 9 show the results of symlet and coiflet filters on peppers and boat image respectively.

TABLE I : Comparative Results for Pepper Image

Filter Used	MSE	PSNR
HAAR(DB1)	27.3578	77.7353
SYMLET	25.3977	78.4787
COIFLET	25.3234	78.0580

TABLE II : Comparative Results for Boat Image

Filter Used	MSE	PSNR
HAAR(DB1)	38.9263	74.2086
SYMLET	38.3553	74.3564
COIFLET	38.3842	74.3488

TABLE II : Comparative Results for Baboon Image

Filter Used	MSE	PSNR
HAAR(DB1)	80.7402	66.9129
SYMLET	79.4937	67.0685
COIFLET	80.0438	66.9995

TABLE II : Comparative Results for Lena Image

Filter Used	MSE	PSNR
HAAR(DB1)	26.5616	78.0306
SYMLET	25.2895	78.5214
COIFLET	25.5326	78.4257

The above results show a comparative analysis of results with haar(db1), symlet and coiflet filters in terms of Mean Square Error(MSE) and Peak Signal to Noise Ratio(PSNR). The symlet and coiflet filters based algorithm gives better performance as compared to haar wavelet based algorithm. Out of symlet and coiflet, symlet is seen to give a slightly better results in terms of MSE and PSNR values.

CONCLUSION

The watermarking techniques were discussed extensively to understand the state of the art of Digital image Watermarking. A discussion on Wavelet transform and wavelet filters gives a thorough insight into the wavelet technology which can be greatly useful to better understand the wavelet terminology. A novel method based on 2D-DWT technique was proposed and tested on a number of standard test images and the results show a high level of perceptibility of Watermarked Image and the retrieved hidden image. The method was implemented using haar, symlet and coiflet filters. A comparative analysis of results in terms of MSE and PSNR is shown which gives the conclusion that symlet filter based algorithm is the best in terms of performance.

REFERENCES

[1]. M. Kim, D. Li and S. Hong, "A Robust Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method", International Journal of Multimedia and Ubiquitous Engineering,Vol.9, No.1 (2014), pp.369-378.
[2]. Brijesh B. Mehta, Udai Pratap Rao," A Novel approach as Multi-place Watermarking for Security in Database", Int'l Conf. Security and Management | SAM'11 |.
[3]. Nameer N. EL-Emam," Hiding a Large Amount of Data with High Security Using Steganography Algorithm", Journal of Computer Science 3 (4): 223-232, 2007
[4]. Dipesh Agrawal and Samidha Diwedi Sharma," Analysis of Random Bit Image Steganography Techniques", International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology – 2013.
[5]. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt," Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Volume 90, Issue 3, March 2010, Pages: 727-752\
[6]. Anil Kumar and Rohini Sharma," A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.
[7]. Ramadhan Mstafa and Christian Bach," Information Hiding in Images Using Steganography Techniques", 2013 ASEE Northeast Section Conference, Norwich University, March 14-16, 2013.
[8]. ISO/IEC 14495-1**,** ITU T.87, "Information technology - Lossless and near-lossless compression of Continuous tone still images," 1999.
[9]. M. J. Weinberger, G. Seroussi, and G. Sapiro, "LOCO-I: A low complexity, context-based, lossless image compression algorithm," in *Proc. DCC'SG,* (Snowbird, Utah, USA), pp. 140-149, Mar. 1996.
[10]. I. Ueno and F. Ono. "Prouosed modification of LOCO-I for its improvement of the performance." ISOIIEC JTCl/SC29/WGl doc. N297. Feb. 1996.
[11]. M. 'J. Weinbeiger, G. Seroussi, and G. Sapiro. ISO/IEC JTCl/SC29/WGl docs. N341, N386, N412 (1996).
[12]. M. J. Weinberger, G. Seroussi, G. Sapiro, and E. Ordentlich, "JPEG-LS with limited-length code words." ISO/IEC JTCl/SC29/WGl doc. N538**,** July 1997.
[14] Yu, Y.-H., Chang, C.-C., & Lin, I.-C. "A new steganographic method for color and grayscale image hiding. Computer Vision and Image Understanding", 107(3), 183-194. doi: 10.1016/j.cviu.2006.11.002, 2007
[15]Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727-752,2007
[16] Min-Jen, T., & Jung, L. (2011, 6-9 Nov. 2011). The quality evaluation of image recovery attack for visible watermarking algorithms. Paper presented at the Visual Communications and Image Processing (VCIP), 2011 IEEE.
[17] H.Harrak,T.D. Hien & Y. Nagata, Z.Nakao," DCT Watermarking Optimization by Genetic Programming", Volume 35 of the series Advances in Soft Computing pp 347-351.
[18] Chun-Hsiang Huang, Chih-Hao Shen & Ja-Ling Wu," Fidelity-Controlled Robustness Enhancement of Blind Watermarking Schemes Using Evolutionary Computational Techniques", Volume 3304 of the series Lecture Notes in Computer Science pp 271-282
[19] Min-Jen, T., & Jung, L ,"The quality evaluation of image recovery attack for visible watermarking algorithms", Paper presented at the Visual Communications and Image Processing (VCIP), 2011 IEEE, (2011, 6-9 Nov. 2011).
[20] Akhil Pratap Singh and Agya Mishra," Wavelet Based Watermarking On Digital Image",Indian Journal of Computer Science and Engineering,Vol 1 No 2, 86-91

