Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 393-401, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.393.401

Comparison of Wavelet Filters in Hybrid Domain Watermarking

V. Elamaran, K. Narasimhan, P.V.M. Vijayabhaskar and G. Shiva
Department of Electronics and Communication Engineering, SASTRA University, India

Corresponding Author: V. Elamaran, Department of Electronics and Communication Engineering, SASTRA University, India

ABSTRACT

The rapid growth of the Internet over the last two decades has enormously increased the abundant of computer data such as audio, images and videos to the public. It has greatly facilitated the hacking and unauthorized distribution of those digital media, which become simple and easier due to the adequate technology processing platforms. To enforce the intellectual property rights and digital media from tampering, "digital watermarking" technique can be used. The pixel values of the watermark which is embedded with the asset image are directly modified in spatial domain watermarking technique. Transform domain watermarking embed the watermark in the transform domain like modifying the spectral coefficients of both asset and watermark images. In this paper, we implement watermarking in hybrid domain which modify the image regarding both spatial and spectral coefficients. DWT is applied to both the asset and message which is to be hidden in the asset image. The watermark is embedded spatially with the HL, LH and HH components which has been wavelet transformed using various wavelet filters. The Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are evaluated to test the imperceptibility of the watermark. Watermarked image suffers some different signal attacks like compression, adding salt and pepper noise, image cropping, image rotation and filter which are used to evaluate the robustness of a watermark. Simulation results show the Daubechies 10 wavelet produces better response among all the others, at the cost of more computation.

Key words: Discrete wavelet transform, spatial domain watermarking, subband coding, transform domain watermarking

INTRODUCTION

Digital watermarking is a method for inserting the watermark (information) into an image, which can be later extracted during the dewatermarking process for identification or authentication purposes. This technique does not distort the image but embeds some hidden information, which is like a secret signature that can be accessed by authorized users before copying it or retransmitting it. Other applications of watermarking are transaction tracking, broadcast monitoring, owner identification, copy control and device control, etc.

For the copyright protection, robust watermark is used. The requirements for the robust watermark are the watermark must be permanently intact to the host information, avoiding the watermark will affect the perceptual quality of the signal. For the digital signature or tamper detection, fragile watermark is used. Semi fragile watermark is used for the data authentication. Original information is used to retrieve the hidden data in the non-blind watermarking algorithm.

Semi-blind watermarking algorithm uses the side information and/or the watermark rather than the original signal. The most challenging task is the blind watermarking algorithm which does not use the original signal or any side information.

Present study focus on the combination of spatial domain technique and the transformed domain technique. In the spatial method, the watermark image is embedded by altering directly or comparing the gray-level or color value (Jiansheng *et al*., 2009). The Least Significant Bit (LSB), patchwork method with streak block mapped coding and the district intersect based method are the popular ways to work with spatial domain (Zeki *et al*., 2011a; Nikolaidis and Pitas, 1996). Spread spectrum, DCT transformation method (Zeki *et al*., 2011a, b) and DWT transform (Phadikar *et al*., 2007) method are the main current transformed domain algorithms.

The watermark is mapped with the significant coefficients of the transformed image and the inverse-transformed to retrieve the image representation. In this study, we apply DWT (Shilbayeh and Alshamary, 2010) to the both asset and message images. To decompose the asset and message image, both orthogonal and bi-orthogonal wavelet filters are applied. The Low frequency content of the hidden information i.e., the LL band is embedded in the high frequency content of the asset image i.e., LH or HL band. Further to generate the watermarked image, the Inverse Discrete Wavelet Transform (IDWT) is applied. The recovery process is quite straight forward as well, basically the reverse mapping is performed in the same place where mapping was performed in the first phase.

The robustness of a watermark method (Chen *et al*., 2003) can be evaluated by performing attacks on the watermarked image and evaluating the similarity of the extracted message to the original asset (Naini, 2011). Compression attacks, adding a salt and pepper noise, cropping attacks, image rotation and enhancement attack are evaluated to test the robustness of a watermark and the results are discussed.

The main objective of present study is to incorporate both spatial and transform domain techniques for the purpose of digital watermarking and also to study the behavior and characteristics of different wavelet filters for both watermarking and evaluation of watermarking methods.

WAVELET TRANSFORM

The extension of the wavelet transform to two dimensions is quite straightforward. A two-dimensional scaling function is said to be separable if it can be factored into a product of two one-dimensional scaling functions, i.e., $\Phi(x, y) = \Phi(x)\,\Phi(y)$. For simplicity, only separable wavelets are applied here. Wavelet transform is a time domain localized analysis method with the window's size fixed and form convertible.

A 2-Dimensional DWT is applied to the original gray-scale 512×512 image of baboon and the message gray-scale 128×128 image of girl which is to be hidden. DWT is applied the images on a tile-by-tile basis for subband coding. Different wavelet filters are used to convert image into wavelet coefficients. Although the convolutions in the discrete wavelet transform can still be computed efficiently on blocks of data, no partitioning of the image is required in wavelet coding. The advantage is that the typical blocking artifacts like the ones occurring in Joint Photographic Experts Group (JPEG), are avoided and the computing time is hardly increased.

Wavelet decomposition: The basic idea of DWT in image processing is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district

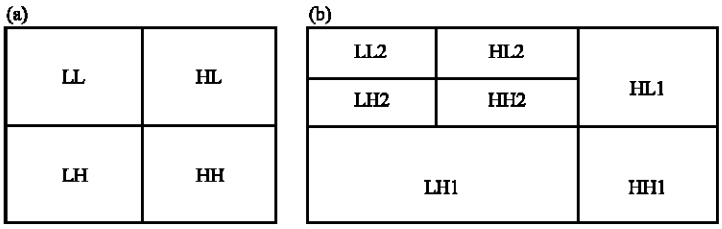

Fig. 1(a-b): The two-dimensional DWT (a) One-level transform and (b) Two-level transform

(Ghouti *et al*., 2006). The low-pass filtered Subband is recursively decomposed in an usual dyadic wavelet decomposition and a logarithmic tree structure representation is used as shown in Fig. 1.

The LL band indicates the lower resolution version of the image and the LH band indicates the horizontal edge data. Vertical edge data and diagonal edge data are represented by HL band and HH band, respectively. The message image which is to be hidden is placed in the HL, LH or HH subbands since modifications to edge data create the least visually perceptible changes. Images with a greater number of edges will hold more watermarking data.

The wavelet packet decomposition offers a number of attractive properties, including (1) Flexibility, from a cost metric approach a best wavelet from a large library of permissible bases can be found, (2) Favorable localization of wavelet packets in both frequency and space and (3) Low computational requirement for wavelet packet decomposition, because each decomposition can be computed in the order of N log N using fast filter banks (Chu, 2003).

PROPOSED DIGITAL WATERMARKING

An image watermarking scheme should at least meet the following requirements, since digital watermarking is a technique that allows for the secret embedding of information in host data (Qidwai and Chen, 2010):

- **Transparency:** The embedded watermark should be perceptually invisible
- **Robustness:** The embedded watermark should not be erased by any attack that maintains an acceptable host image quality

One of the most important issues in image watermarking is the trade-off between transparency and robustness. Watermarking algorithms are broadly classified into two groups in terms of the embedding domain: spatial domain methods, in which the data is embedded by altering the pixel values of the original image directly and transform domain methods, in which the data is embedded by modulating the transform domain coefficients.

Discrete Fourier Transform (DFT), DCT and DWT are the frequently applied transforms for digital watermarking. Computing performance is well in spatial domain methods, where in transform domain methods high robustness can be achieved. In terms of the extracting scheme, watermarking algorithms are also divided into two groups: blind and non-blind watermarking. The original image must be needed for the watermark extraction in non-blind watermarking, whereas in blind watermarking, the original image is not necessary for watermark extraction (Qidwai and Chen, 2010).

Proposed watermarking strategy in hybrid domain: Watermarking in hybrid domain means modifying the image regarding both spatial and spectral coefficients as shown in Fig. 2.

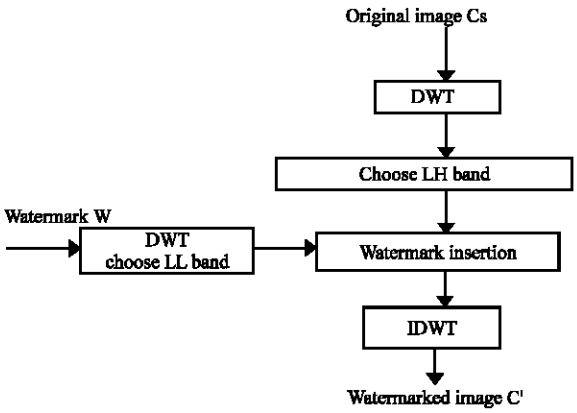

Fig. 2: Watermarking process

The LL band of message image is embedded in the LH band of the asset image according to the Eq. 1 as follows:

$$a_i' = ai+\alpha w_i \quad (1)$$

where, a_i' and w_i represent the DWT coefficients (LH/HL or HH) of the asset and watermark message (LL) image respectively and the ai' indicates the watermarked DWT coefficients of the original asset. The α decides the embedding depth of the watermarking.

In this study, during the second level wavelet decomposition, we implement the embedding portion of message image in to the LH, HL and HH subbands of the asset image. Standard wavelet filters are used to obtain DWT coefficients of both asset and message subband images. But to produce Inverse DWT for the purpose generating a final watermark image, we propose the method that our own defined synthesis filters can be used instead of standard wavelet filters. Results are obtained and compared with all the possibilities of watermark depth and various wavelet filters.

Analysis and synthesis filters: Wavelet filters like orthogonal and biorthogonal are used for the purpose of decomposition and reconstruction. This can be among the filter families of Daubechies, Coiflets, Symlets, Discrete Meyer, Biorthogonal and Reverse Biorthogonal. The option is also provided that we can use our own defined filters which are used in this paper to produce simulation results.

A lowpass decomposition and reconstruction filter Lo_D = Lo_R = [-1 2 6 2-1]/8 and a highpass decomposition and reconstruction filter Hi_D = Hi_R = [1 2-6 2 1]/8 are used in our simulations.

Lowpass and highpass synthesis filters are applied here to the DWT coefficients of the subband images to produce the final watermark image.

Attacks on watermarks: Trickier attacks involve warping, rotations of the image and scaling of the image. Cropping attack, which removes rows and columns from the image to form a new shape is also possible. It affects the synchronization of the image is the difficulty of this attack. There needs to be some form of comparison of the signal against a benchmark in order to detect a

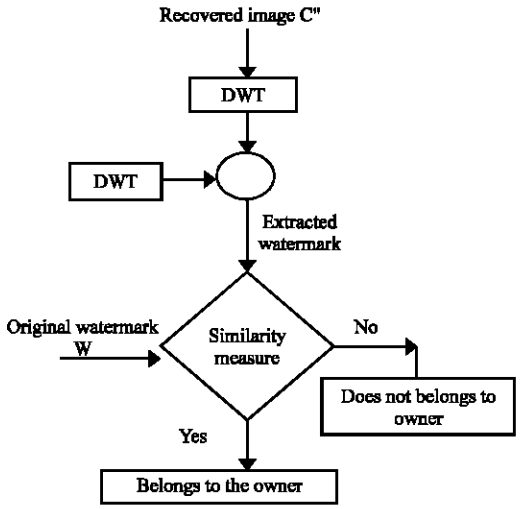

Fig. 3: Dewatermarking process

watermark. The watermark is detected if the signal is close enough to the expected form. The watermark will not be detected if the synchronization is lost, however. Most of the above attacks are considered here and the results are discussed.

Attacks on watermarking: Trickier attacks involve warping, rotations of the image and scaling of the image. Cropping attack, which removes rows and columns from the image to form a new shape is also possible. It affects the synchronization of the image is the difficulty of this attack. There needs to be some form of comparison of the signal against a benchmark in order to detect a watermark. The watermark is detected if the signal is close enough to the expected form. The watermark will not be detected if the synchronization is lost, however. Most of the above attacks are considered here and the results are discussed.

Dewatermarking strategy: To detect a watermark, the reverse mapping is performed in the same place where mapping was performed in the first phase i.e., during watermark insertion process. The watermark extraction process is shown in Fig. 3 and the inverse mapping is done based on the following Eq. 2.

$$\alpha w_i = a_i' - a_i \tag{2}$$

Evaluation of watermarking methods: Mean Square Error (MSE) is one of the earliest tests that were performed to test if watermarked image with the original asset image. A function could be simply written according to the following Eq. 3:

$$MSE = \frac{1}{N_1 N_2} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} (x[n_1, n_2] - x'[n_1, n_2])^2 \tag{3}$$

where, $x[n_1, n_2]$ is the original asset image, $x'[n_1, n_2]$ is the watermarked image and N_1 and N_2 are the dimensions of the image.

Peak Signal-to-Noise Ratio (PSNR) takes the signal strength into consideration (not only the error), is a better test here. It is written according to the following Eq. 4:

$$PSNR = 10 \log_{10}\{255^2/MSE\} \quad (4)$$

SIMULATION RESULTS

To test the performance of the proposed algorithm, the experiments are simulated with the Matlab software. A 512×512 baboon asset image and a 128×128 girl message images are used in these experiments which are shown in Fig. 4. The LL subband of watermark image is spatially embedded in the LH subband of asset image and the result is shown in Fig. 5. The final watermarked image after IDWT is shown in Fig. 6. It is very difficult to recognize the transformed image. The PSNR evaluated as a comparison of the watermarked image versus original asset image is 52.0244 dB, which is better than the PSNR of Cox algorithm (Cox and Linnartz, 1998).

Also the correlation coefficient is evaluated using different wavelet filters and the result is obtained in Table 1. Results show that the db2 has 0.8215 and Sym2 has 0.8215 as a correlation coefficient which indicates that the watermarked and asset images look more similar. But db10 and

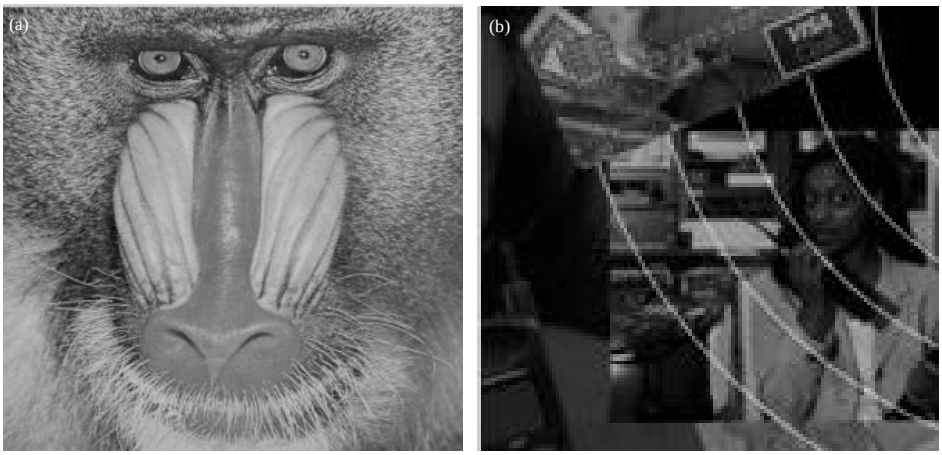

Fig. 4(a-b): (a) Asset image 512×512 and (b) Watermark image 128×128

Table 1: Correlation Coefficient between the watermarked and the original asset image

Wavelet filters used	Correlation coefficient
Bior1.1	0.5768
Bior1.4	0.5180
Dmey	0.1001
Coif1	0.7963
Sym2	0.8215
Haar	0.5768
Db2	0.8215
Db4	0.5208
Db6	0.4583
Db8	0.3992
Db10	0.3593

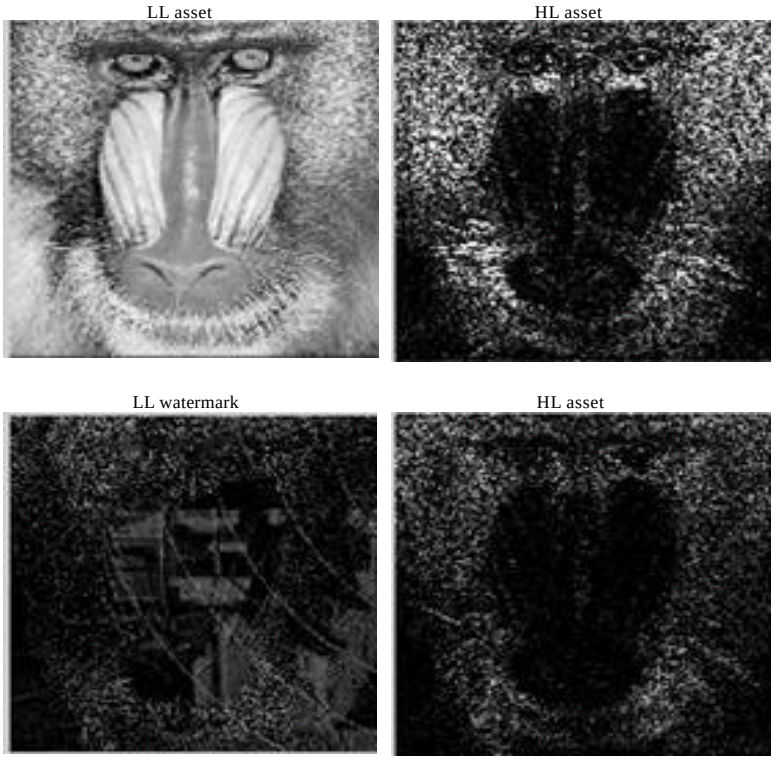

Fig. 5: LL watermark embeded in LH asset

Fig. 6(a-b): (a) Watermarked and (b) Dewater marked images

Dmey wavelet filters have the correlation coefficient 0.3593 and 0.1001 respectively. This shows that the watermarked and asset images look differently. Table 2 and 3 shows that the PSNR parameter which is compared with the dewater marked image and the original watermark image with the various filters by suffering different attacks to the watermarked image. Here the db10

Table 2: PSNR values of attacked watermarked image

	Wavelet filters used				
Attacks	Bior 1.1	Bior 1.4	Dmey	Coif1	Sym2
Compression	44.51	45.70	45.70	46.58	46.58
Salt and pepper noise	55.57	55.57	55.56	55.58	55.57
Cropping	55.53	55.53	55.53	55.53	55.53
Rotation	45.07	45.32	46.99	46.53	46.40
2×2 median filter	36.60	36.80	36.78	37.00	36.80

Table 3: PSNR values of attacked watermarked image with Haar and Daubechies family

	Wavelet filters used				
Attacks	Haar	Db2	Db4	Db8	Db10
Compression	44.51	46.58	46.33	46.21	45.18
Salt and pepper noise	55.57	55.57	55.50	55.57	55.57
Cropping	55.53	55.53	55.53	55.53	55.53
Rotation	45.07	46.40	45.86	47.37	49.02
2×2 median filter	36.60	36.80	37.00	37.20	38.16

wavelet filter has comparatively a better PSNR value while the attacks are salt and pepper noise, cropping, rotation and 2×2 median filter as 55.57, 55.53, 49.02 and 38.16, respectively. The watermarked and the distilled watermark images are shown in Fig. 6.

CONCLUSION

Results indicate that the db10 wavelet filter produce better results but at the cost of more computation. Also it indicates that 2×2 mean filter attack response is bad for all kind of wavelet filters.

Robustness can be further achieved in the watermarked images through multiple watermarks, redundant watermarks and mapping the watermarks using transformed binary images rather than the image itself. To make more difficult for an attacker to isolate the watermark, nonlinear mapping can be utilized rather than linear or affine mapping.

REFERENCES

Chen, T.H., G. Horng and S.H. Wang, 2003. A robust wavelet-based watermarking scheme using quantization and human visual system model. Inform. Technol. J., 2: 213-230.

Chu, W.C., 2003. DCT-Based image watermarking using sub sampling. IEEE Trans. Multimedia, 5: 34-38.

Cox, I.J. and J.P.M.G. Linnartz, 1998. Some general methods for tampering with watermarks. IEEE J. Selected Areas Communi., 16: 587-593.

Ghouti, L., A. Bouridane and M.K. Ibrahim, 2006. Digital image watermarking using balanced multiwavelets. IEEE Trans. Signal Process., 54: 1519-1536.

Jiansheng, M., L. Sukang and T. Xiaomei, 2009. A digital watermarking algorithm based on DCT and DWT. Proceedings of the International Symposium on Web Information Systems and Applications, May 22-24, 2009, China, pp: 104-107.

Naini, P.M., 2011. Digital Watermarking using MATLAB. In: Engineering Education and Research Using MATLAB, Assi, A.H. (Ed.). Chapter 20, InTech Publisher, India, ISBN: 978-953-307-656-0, pp: 465-480.

Nikolaidis, N. and I. Pitas, 1996. Copyright protection of images using robust digital signatures. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, May. 7-10, IEEE Xplore Press, USA., pp: 2168-2171.

Phadikar, A., B. Verma and S. Jain, 2007. Region splitting approach to robust color image watermarking scheme in wavelet domain. Asian J. Inform. Manage., 1: 27-42.

Qidwai, U. and C.H. Chen, 2010. Digital Image Processing: An Algorithmic Approach with Matlab. 2nd Edn., CRC Press, UK., ISBN: 9781420079500.

Shilbayeh, N.F. and A. Alshamary, 2010. Digital watermarking system based on cascading haar wavelet transform and discrete wavelet transform. J. Applied Sci., 10: 2168-2186.

Zeki, A.M., A.A. Manaf and S.S. Mahmod, 2011a. High watermarking capacity based on spatial domain technique. Inform. Technol. J., 10: 1367-1373.

Zeki, A.M., A.A. Manaf, A.A. Ibrahim and M. Zamani, 2011b. A robust watermark embedding in smooth areas. Res. J. Inform. Technol., 3: 123-131.