An Efficient Watermarking Algorithm Based on DWT and FFT Approach

S.Manikanda prabu
Assistant Professor,
Department of CSE,
Tamilnadu College of Engineering, Coimbatore, India
smaniprabume@gmail.com

Dr.S.Ayyasamy
Professor and Head, Department of Information Technology,
Tamilnadu College of Engineering
Coimbatore, India

***ABSTRACT*-Multimedia and Internet have become our daily needs. It has become a common practice to create copy, transmit and spread digital data .It leads to unauthorized duplication problem. Digital image watermarking provides a powerful solution for this problem. Watermarking is the process of embedding a cover image in such a way that the resulting watermarked image is robust to certain distortion caused by either standard data processing in a friendly environment or malevolent attacks in an unfriendly environment . This paper presents a digital image watermarking based on two dimensional Fast Fourier Transform (FFT) and Discrete Wavelet Transform (DWT). The generalized algorithms are presented for FFT, DWT-FFT combined approach. Peak signal to noise ratio and normalized cross-correlation coefficient are computed to measure image quality for each transform. Comparative results of image watermarking using FFT and DWT-FFT are presented. Experimental results demonstrate that the proposed scheme is imperceptible and has good robustness for some common image processing operations and some attacks. The paper recommends DWT-FFT based techniques for achieving secure image watermarking.**

Keywords: Discrete Wavelet Transform (DWT), Fast Fourier Transform (FFT) and watermarking.

I.INTRODUCTION

The advent of multimedia and the rapid development of network technology have caused digital information, such as digital images, digital audio and digital video to be easily distributed, copied and used either legally or illegally. This has made the protection of the intellectual property of digital products a warm issue which requires conducting laborious research. Digital watermarking is considered one of the powerful approaches to protect the intellectual property rights of digital media from illegal manipulations .Digital image watermarking has attracted the attention of several researchers in the past decades. The main idea behind the work in this area is the desire to achieve information security, information hiding and authentication. There are several approaches have been proposed for digital image watermarking.

Digital watermark is an invisible signature or an image embedded inside an image to show authenticity and ownership. An effective digital watermark should be perceptually invisible to avert obstruction of the original image. It should be statistically invisible to prevent detection and also be robust to many image manipulations like filtering, additive noise, and compression. Digital Watermarking is the process of hiding information into digital multimedia content such that the information can be extracted later or detected for a variety of purposes including copy prevention and control. Digital watermarking has been proposed as a new and an alternative method to enforce the intellectual property rights and protect digital media from tampering. The significant requirements to be satisfied by any digital watermarking scheme are as follows.

1. **Robustness:** Robust is a measure of immunity of watermark against attempts to image modification and manipulation such as noise attacks, compression, filtering, rotation, scaling, collision attacks, resizing, cropping etc. Watermark should be difficult to remove.
2. **Imperceptibility:** It means quality of host image should not be destroyed by presence of watermark.
3. **Capacity:** From a quantitative view, it means that the amount of information that can be stored into cover data depends on the application. On the other hand, from a qualitative perspective, it refers to the type of information that can be used as a watermark. Thus, the effective watermarking system must have the ability to embed the majority of information.
4. **Security:** It means that the ability of the watermark to resist attempts by attacker to destroy it without modifying the cover data itself so that unauthorized users cannot detect, read or modify the embedded watermark.

5. **Effectiveness:** It means that the watermark extraction process should be simple and fast.

In this paper, we introduce a robust image watermarking algorithm in the frequency domains using Fast Fourier Transform (FFT) and Discrete Wavelet Transform (DWT). Watermarking image will be discrete Cosine transformed at first. The cover image is decomposed through DWT transform, then choose the appreciate wavelet modulus in the high frequency level. Selected sub band is fourier transformed. The watermarking information is embedding into the corresponding position. Make the whole image Inverse FFT (IFFT) and Inverse DWT (IDWT) transformed and get the watermarked image. The watermark extraction is quite the contrary.

The rest of the paper is organized as follows: Section 2 presents some related work. Section 3 discusses the preliminaries required for this work. Section 4 describes in detail about the proposed watermarking algorithm. Section 5 includes the experimental results and discussion. Section 6 concludes this paper followed by relevant references.

II.RESEARCH BACKGROUND

A number of studies have been conducted for watermarking in spatial and frequency domains. In this section, we will briefly review some of the previous work in this area.

Spatial domain techniques [1][2] are simple to implement and often require a lower computational cost, although they can be less robust against tampering than methods which place the watermark in the most perceptually significant components of a transform domain (Fourier, Wavelet, Cosine) [4][5][8]. ElGamal et al. [3] presents the hybrid image watermarking algorithm for color images based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform. The cover image is converted from RGB color space into YCbCr color space, and then the luminance component is selected and partitioned into non-overlapping blocks of pixels according to the number of bits of the original watermark. DCT conversion is performed for each block separately. After DCT transformation, the DWT is performed and vertical component, LH is taken out for embedding the watermark. Mei Jiansheng et al. [7] have developed a method for watermarking based on Discrete Cosine Transform and Discrete Wavelet Transform. The information of watermarking which has been discrete Cosine transformed, is put into the high frequency band of the image which has been wavelet transformed. Then extract the digital watermarking with the help of the original image and the watermarking image.

III. PRELIMINARIES

A. FAST FOURIER TRANSFORM

Fast Fourier Transform (FFT) is a transformation algorithm that converts images from spatial domain to frequency domain. The Fast Fourier Transform is an important image processing tool which is used to decompose an image into its sine and cosine components. The output of the transformation represents the image in the frequency domain, while the input image is the spatial domain equivalent. In the frequency domain image, each point represents a particular frequency contained in the spatial domain image. The FFT is used in a wide range of applications, such as image filtering, image reconstruction, image compression, image analysis and image watermarking. 2D transform of a 2K by 2K image requires 4K 1D transforms. This follows directly from the definition of the fourier transform of a continuous variable or the discrete fourier transform of a discrete model. The 2-D FFT is a direct extension of the 1-D case and is given by

$$F(u,v) = \frac{1}{MN}\sum_{x=0}^{M}\sum_{y=0}^{N} f(x,y)e^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \quad (1)$$

The inverse transform is defined as

$$f(x,y) = \sum_{u=0}^{M}\sum_{v=0}^{N} F(u,v)e^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \quad (2)$$

B. DISCRETE WAVELET TRANSFORM

Discrete wavelet transform (DWT) is another powerful transformation algorithm for digital image watermarking in frequency domain. The DWT finds a great popularity in the field of watermarking as it is able to decompose the available images into sub-bands, in which watermarks can be embedded; selectively .DWT is also a mathematical tool for decomposing an image hierarchically. It decompose the original image into four sub-bands which are lower approximation image (LL), horizontal (HL), vertical (LH) and diagonal (HH) sub-bands. This process of division can be repeated several times to compute multi-level wavelet decomposition.LL sub-band is not suitable for the watermark embedding based on HVS model, because it contains significant information about the image and causes image distortion. In addition, embedding a watermark in the HH sub-band is not suitable, because this sub-band is less robust against image processing operations such as compression. Thus, the suitable areas for watermark embedding are the mid-frequency sub-bands LH and HL, where acceptable performance of imperceptibility and robustness could be achieved. Figure.1 illustrates the sub-band decomposition of an image using 2D wavelet transform after 3 levels of decomposition. Where, L represents low-pass filter, H represents high-pass filter. An original image can be decomposed of frequency districts of HL1, LH1, and HH1. The low-frequency region information also can be decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for *n* level wavelet transformation.

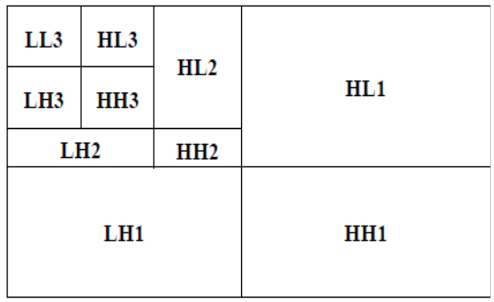

Fig.1. Sketch Map of Image DWT Decomposed

DWT is currently used in a wide variety of signal processing applications, like data compression, image recognition, denoising and speech synthesis, etc, because it has a number of advantages over other transforms.

IV. PROPOSED WATERMARKING ALGORITHM

Frequency domains are better for the watermarking than spatial domain for both reasons of robustness under conventional attacks as well as visual impact. This section introduces a novel image watermarking algorithm in the frequency domain using FFT and DWT-FFT combined approach.

A. WATERMARKING ALGORITHM USING FFT

1. The original image I and the watermark image W are reading.
2. The watermark image resize if necessary to make it size the same of original image.
3. The FFT coefficients for original image and watermark image are found out.
4. The value of scaling factor defined to be suitable for invisible watermarking.
5. The FFT coefficient of the original image and watermark image is modified using the following equation. The IFFT of modified coefficients give the watermarked image.

$$\mathrm{I_w(i,j) = I(i,j) + \beta W(i,j)} \qquad \mathrm{i,j} = 1,\dots,n \tag{3}$$

6. Watermark is extracted by applying the following equation:

$$\mathrm{W(i,j)} = \frac{\mathrm{I_w(i,j) - I(i,j)}}{\beta} \qquad \mathrm{i,j = 1,2,3 \dots n} \tag{4}$$

Where,
I-Original image
W-Watermark image
Iw-watermarked image and
β-Embedding factor

B. WATERMARKING ALGORITHM USING DWT-FFT

The original image is decomposed up to n levels. Then, the vertical component LH is taken out for inserting the watermark, because embedding the watermark in vertical regions increases the watermark robustness on image quality. The concrete embedding and extracting procedure can be summarized as follows:

1. Apply DWT to decompose the original image to the required level.
2. Select vertical sub band (LH) for embedding.
3. The watermark image resized if necessary to make it size the same of selected sub band.
4. The FFT coefficients for selected sub band and watermark image are found out.
5. The value of scaling factor defined to be suitable for invisible watermarking.
6. Modify the coefficients of the LH band by adding watermark coefficients:

$$\mathrm{LH_{w\,i,j} = LH_{i,j}} + \alpha \mathrm{w_{ij}}, \mathrm{i,j = 1,\dots,n} \tag{5}$$

7. Apply IFFT and IDWT to obtain the watermarked cover Image, *Iw*.
8. Using two-dimensional DWT decompose the watermarked image (and possibly attacked) to the required level.

9. Select vertical sub band and find the fourier coefficients.
10. Extract the invisible watermark from the LH band by using equation :

$$w_{ij} = (LH_{w,ij} - LH_{ij})/\alpha \quad (6)$$

Where, LH is the selected sub band, LH_w represents the watermarked image, w denotes the watermark and α is the embedding factor.

11. The IFFT of the coefficients give the watermark image.

V. EXPERIMENTAL RESULTS AND DISCUSSION

To evaluate the performance of the proposed algorithm, MATLAB simulations are performed by using a variety of popular cover images .The measurement criteria are required to assess the performance of the method used in terms of imperceptibility and robustness. The First criterion is the peak signal to noise ratio (PSNR) given by Eq. (7) which is used to measure the quality of watermarked image. The second criterion is the Normalized Cross-Coefficient (NC) given by Eq. (9) which is used to measure the similarity and difference between the original and extracted watermarks under various attacks.

$$PSNR = 10log_{10}\frac{P*P}{MSE} \quad (7)$$

Where P=256, MSE is the mean square error, which is defined as:

$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{[I(i,j)-I'(i,j)]^2}{M*N} \quad (8)$$

Where I is the original image and I' is the watermarked image. PSNR is measured in decibels (db) and the bigger the PSNR value is, the better the watermark conceals.

$$NC = \frac{\sum_{i=1}^{M1}\sum_{j=1}^{M2} W(i,j).W'(i,j)}{\sqrt{\sum_{i=1}^{M1}\sum_{j=1}^{M2}[W(i,j)]^2}\sqrt{\sum_{i=1}^{M1}\sum_{j=1}^{Mdv2}[W'(i,j)]^2}} \quad (9)$$

Where W is the original watermark image and W' is the extracted watermarked image. The value of NC is between 0 and 1. And the bigger the value is, the better the watermark robustness. In this paper the simulation process is implemented in MATLAB using different types of cover and watermark images. The example of opted original and watermark images are as follows:

Fig.2. original images

Fig.3. Watermark images

For robustness inspection of the proposed scheme the watermarked image was tested against several types of attacks namely JPEG compression, Salt & Pepper noise, Gaussian noise, Speckle noise, Rotation and Resizing. The numerical evaluation metrics for all schemes in the absence and presence of attacks are tabulated in Tables (I) to (III).

TABLE.I. COMPARISON OF PSNR VALUE BETWEEN FFT & (DWT-FFT) WITHOUT ATTACK

WATERMARKING METHOD	PSNR	NC
FFT	42.2393	1.0000
DWT +FFT	48.0339	0.9969

TABLE II: COMPARISON OF PSNR VALUE BETWEEN FFT & (DWT-FFT) FOR DIFFERENT TYPES OF ATTACK

IMAGE TYPE	FFT	DWT-FFT
COMPRESSION	42.0533	47.8515
SALT & PEPPER	41.5790	47.8283
GAUSSION	41.8829	47.9064
SPECKLE	40.3193	47.7374
SCALING	42.3476	48.0913
ROTATION	49.1754	48.0339

TABLE III: COMPARISON OF NC VALUE BETWEEN FFT & (DWT+FFT) FOR DIFFERENT TYPES OF ATTACK

IMAGE TYPE	FFT	DWT-FFT
COMPRESSION	0.9709	0.9212
SALT & PEPPER	0.9461	0.9213
GAUSSION	0.9604	0.9234
SPECKLE	0.8702	0.9178
SCALING	1.0000	0.9336
ROTATION	1.0000	0.9403

From Table I, we notice that the FFT and DWT -FFT based watermarking scheme achieves the lowest distortion in the watermarked images in the absence of attacks. From Tables (II) and (III), we found that the proposed watermarking scheme based on DWT -FFT has a better performance than FFT watermarking for most of the attacks. The simulation results, including the watermarked image and extracted watermark under different kinds of signal attack, are shown in Fig.4 and Fig.5.

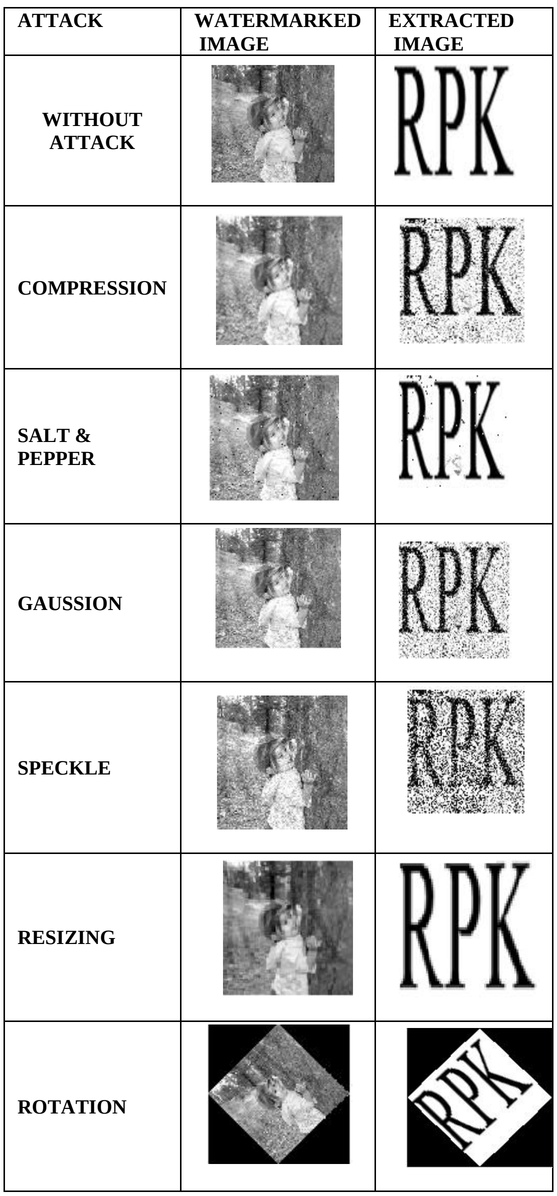

Fig.4.Performance of the FFT based watermarking against various types of attacks

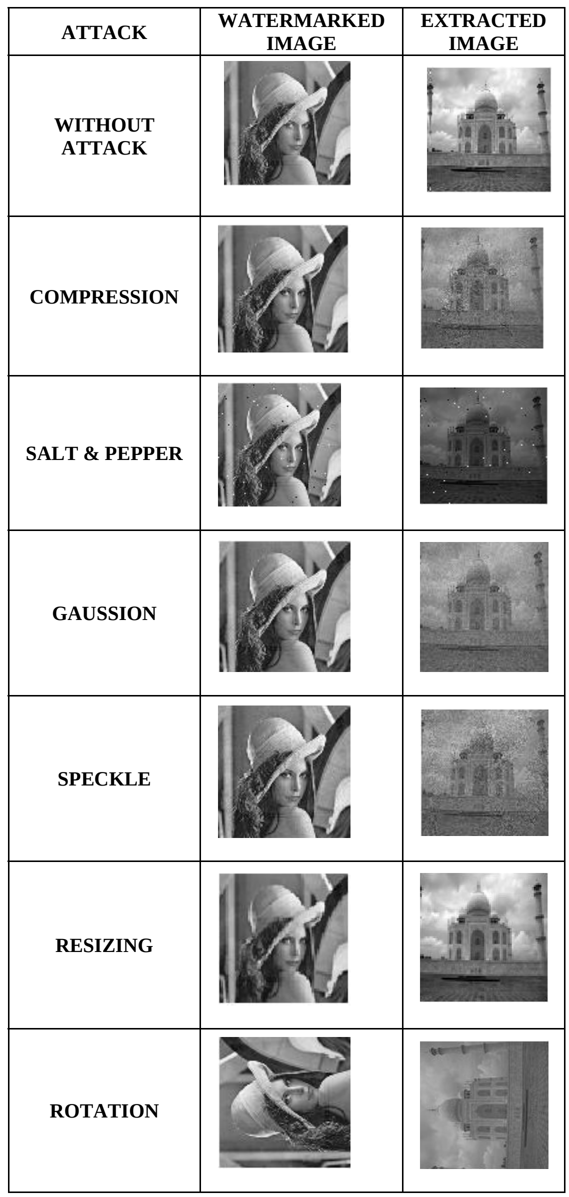

Fig.5. Performance of the DWT- FFT based watermarking against various types of attacks

VI. CONCLUSION

This paper presents a new technique for embedding a watermark into host image using discrete wavelet transform and fast fourier transform. Watermark signal is embedded into the fourier transformed vertical sub band of wavelet coefficient. Before embedding, this watermark image has been fourier transformed in order to improve its robustness. By applying this algorithm, the experimental results have demonstrated that the proposed algorithm is imperceptible, because the average PSNR for all test images is 48.033dB. Moreover, the proposed watermarking system is more robust, because it can keep the image quality well and achieves optimal NC values against many common image processing operations like adding various noises, image compression, and image rotation and so on. It also shows that the proposed method has strong capability of embedding image and anti-attack.

REFERENCES

[1] F. M. Boland, J. J. K. O Ruanaidh and W. J. Dowling. "Watermarking digital images for copyright protection". In IEEE Proceedings on Vision, Signal and Image Processing, vol.143,n.4,pp.250-256,1996.

[2] G. Caronni. "Assuring ownership rights for digital images". In Proceedings Reliable IT System, VIS'95. Vieweg Publishing Company, pp. 251-263, 1995.

[3] A.F.ElGamal, N.A.Mosa and W.K.ElSaid." Block-based Watermarking for Color Images using DCT and DWT", International Journal of Computer Applications (0975 – 8887) Vol. 66, No.15,pp.33-39, 2013.

[4] E. Koch and J. Zhao. "Towards robust and hidden image copyright labaleing". In Proc. of IEEE Workshop of Nonlinear Signal and Image Processing, Halkidiki, Greece, 1995.

[5] D Kundur and D Hatzinakos. " Digital watermarking using multiresolution wavelet decomposition". In International Conference on Acoustic, Speech and Signal Processing(ICASP), Seattle, USA, Vol. 5, pp. 2969-2972, 1998.

[6] Mei Jiansheng1, Li Sukang1 and Tan Xiaomei," A Digital Watermarking Algorithm Based On DCT and DWT", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, pp. 104-107,2009.

[7] W. Bender, D. Gruhl, N. Morimoto. "Techniques for data hiding". In Proceedings of SPIE, vol. 2420, pp. 40, 1995.

[8] I.Pitas. "A method for signature casting on digital images". In Proc. of the International Conference on Image Processing, Vol.. 3, pp 215 - 218, 1996.

[9] Cox, I.J., M.L. Miller and J.A. Bloom (2001). Digital Watermarking. Morgan Kaufmann publisher.

[10] Neil, F.J., D.C. Zoran and J. Sushil (2000). Information Hiding: Steganography and Watermarking – Attacks and Countermeasures. Kluwer Academic Publishers.

About the Authors

Mr.S.Manikanda prabu completed his B.E. (Computer Science and Engineering) in 2003 from Madurai Kamaraj University, Madurai and M.E. (Computer Science and Engineering) in 2008 from Sathyabama University, Chennai Currently he is pursuing PhD degree. He is working as an Assistant Professor, Department of Computer Science and Engineering at Tamilnadu College of Engineering, Coimbatore. His research areas include Pattern Recognition, Signal and Image processing and Neural Networks and having 8 years of teaching experience in Engineering Colleges.

Dr.S.Ayyasamy completed his B.E.(Electronics and Communication Engineering) in 1999 from Maharaja Engineering College and M.E. (Computer Science and Engineering) in 2002 from PSG College of Technology, both under Bharathiar University. He is working as a Professor and HOD, Department of Information Technology at Tamilnadu College of Engineering, Coimbatore. He is a member of CSI. His research areas include P2P networks, Overlay Networks, Cloud computing and Quality of Services and having 12 years of teaching experience in Engineering Colleges.