Comparison of Invisible Digital Watermarking Techniques for its Robustness

Meghana M[1], Dr. P. A. Vijaya[2], Anuradha J P[3]

[1]PG Student, VLSI & Embedded Systems, Dept. of ECE, B.N.M Institute of Technology, Bangalore, India
[2]Professor and Head, Dept. of ECE, B.N.M Institute of Technology, Bangalore, India
[3]Assistant Professor, Dept. of ECE, B.N.M Institute of Technology, Bangalore, India

---

Abstract - *An invisible digital watermarking is a process where an image or a video is embedded with some information in the form of a text or an image called as watermark which is not visible to human eye. In this paper, two invisible digital watermarking techniques based on Discrete Cosine Transforms (DCT) and Discrete Wavelet Transforms (DWT) are implemented in MATLAB and are compared for its robustness using correlation coefficient parameter. The measure of this parameter is done after performing all types of attacks and degradation on the images. The end results show that invisible image watermarking based on DWT is more robust to all sort of attacks and degradation as compared to DCT.*

Key Words: **Digital Invisible Watermarking, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Robustness, Co-efficient Correlation, MATLAB.**

1. INTRODUCTION

Due to the wide expansion of internet over years, availability of data on digital platform has increased very rapidly. One of the major problem is to protect the multimedia information available and so as the rightful owner of the information are concerned about their work being illegally duplicated. So in order to maintain the balance of multimedia being available and also being protected of illegal use, out of many approaches digital watermarking is the one which has gained a lot of interest in the industry.

The main idea of robustness of images in watermarking is to embed the watermark within the original image which is not visible for human eye and also protects the images from image processing attacks and degradations. In other words, the major aim is to develop an image visible exactly as same as the original image, but still allows identification of the hidden watermark when compared with the key given by the owner whenever necessary.

This paper is divided into six sections: section 1 gives the introduction of the paper, section 2 deals with the basics on digital watermarking, section 3 talks about implementation of the whole watermarking process, section 4 talks about implementation of DCT method, section 5 gives an idea about implementation of DWT method, section 6 describes the results of the work done and section 7 is the conclusion of the work done.

2. BASICS ON DIGITAL IMAGE WATERMARKING

The rapid increase in the usage of digital multimedia applications has created a great necessity to given copyright protection to those data. Generally watermarking is a type of marker which is embedded in a digital image which is used to identify the ownership of the image. Digital watermarking are of two types. 1. Spatial domain method where, in an image space, a change in the position of X direction, will projects the change of position in space. 2. Transform domain method, where the image is transformed into frequency domain using different transformations and then watermarking is done.

A watermark indeed can be described as a unique identification code visible or invisible which is embedded into the image permanently. Watermarks are of four different types. 1. Visible watermark: watermarks are visible on the image. 2. Invisible watermark: watermarks are hidden in the image and not visible by naked eyes. 3. Public watermarks: Not so secure watermarks that can be understood and anyone can modify using certain algorithms. 4. Fragile watermark: watermarks that can be destroyed by manipulating the data.

3. IMPLEMENTATION

Digital Watermarking has three phases in its life cycle. 1. Embed: here a digital image is embedded with a watermark image. 2. Attack: Once the original image is changed, it is more prone to threats and this is known as attack to the system. 3. Protection: it is the detection of the watermark from a noise which might have altered the original image.

Considering the life cycle of the watermarking process, Fig -1 shows the flow of the watermarking process implemented in this work. The original which has to be marked must be a grayscale image, but incase if a color image is selected, it is converted into a grayscale image before proceeding further.

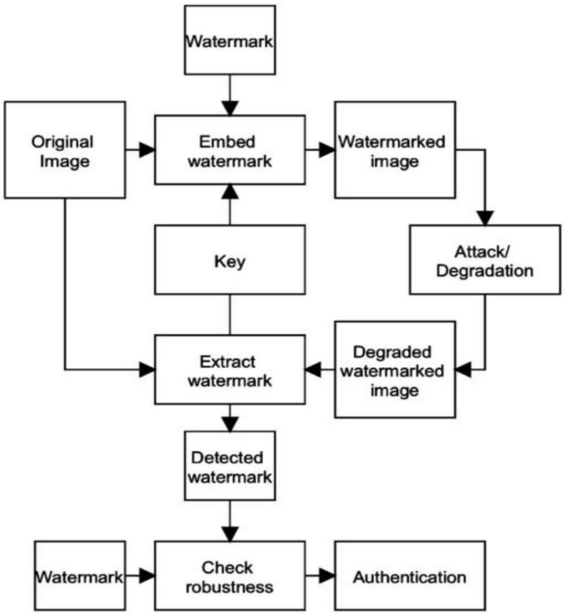

Fig -1: Flow chart for watermarking

The original image used here is an X-ray of a human hand with dimensions of 512x512 pixels as shown in Fig -2. The watermark image used here is a binary image of size 64x64 pixels as shown in Fig -3. When embedding and extracting the watermark, the user is asked to enter a cryptographic key as a password. The two transform domain methods used for digital invisible watermarking are DCT and DWT.

Fig -2: Original Image

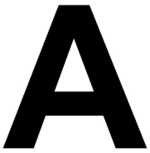

Fig -3: Watermark Image

4. DISCRETE COSINE TRANSFORM

The DCT permits to break the image into bands of different frequency, which makes it much easy to embed the watermark into the middle frequency bands of the image as shown in figure 4. These middle bands are selected as they don't represent the most important visual part of the images.

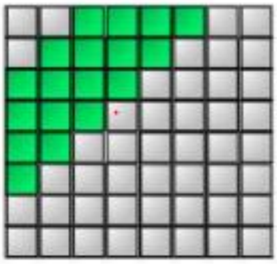

Fig -4: 8x8 Coefficients to be modified

4.1 Embedding DCT Watermark

Figure 5 shows the embedding flowchart for DCT. Here one pixel of the image is hidden in every 8x8 block of image by performing 2-D DCT. Then the coefficients combination for DCT are modified and inverse DCT is performed to obtain the watermarked image.

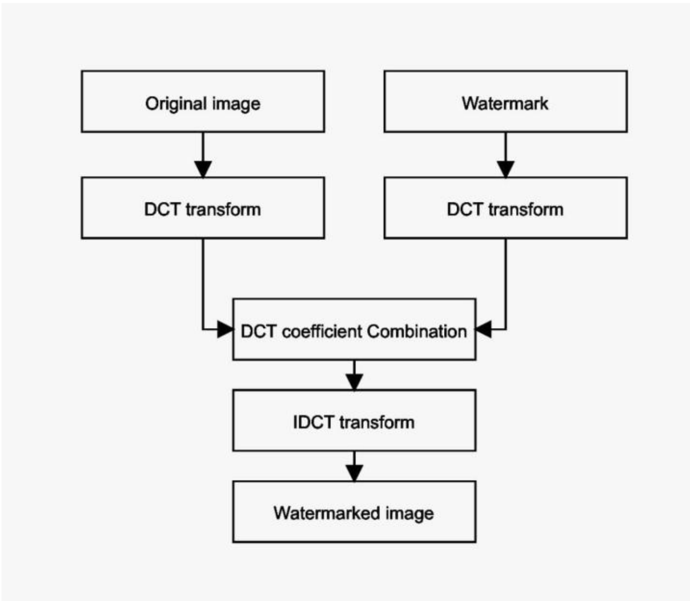

Fig -5: Embedding Flowchart

4.2 Extracting DCT watermark

Figure 6 shows the extracting flowchart for DCT. Here DCT coefficients of the corresponding blocks of an original image are subtracted from the DCT coefficients of the watermarked image block. If the sum of differences between these two are greater than 0, the value of the bit detected is considered 1 else 0.

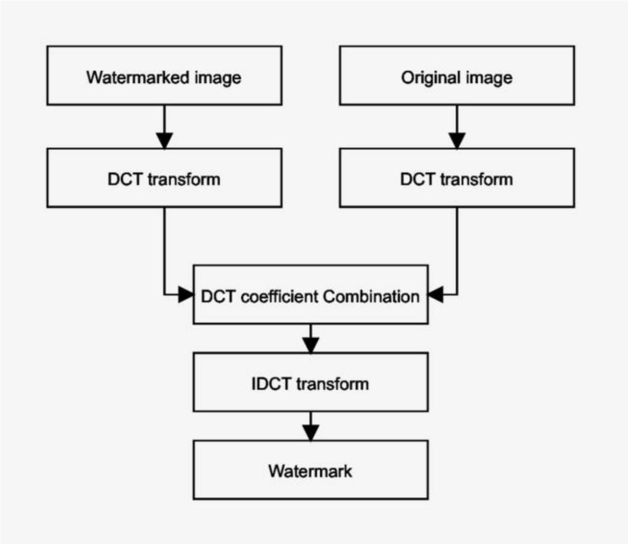

Fig -6: Extracting Flowchart

5. DISCRETE WAVELET TRANSFORM

DWT is a wavelet transform method where the wavelets are sampled discretely. The wavelet transform methods gives the frequency and spatial description of an image. DWT divides the image into low and high frequency parts, where higher frequency parts contain information of edge components of the image, while the lower frequency parts are again split into higher and lower frequency bands. The higher frequency bands are most widely used for digital invisible watermarking as they are less visible to human eye when edges are changed.

The 3 level decomposition of DWT is as shown in Fig -7.

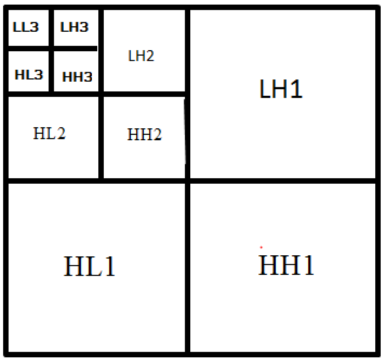

Fig -7: 3 level decomposition of DWT

5.1 Embedding DWT watermark

Fig -8 shows the embedding flowchart for DWT. After performing 3 level decomposition on both original and watermark images, the coefficients of the horizontal, diagonal and vertical details and modified at levels 2 and 3 to embed the watermark. Later which an inverse 3 level DWT decomposition is performed to obtain the watermarked image.

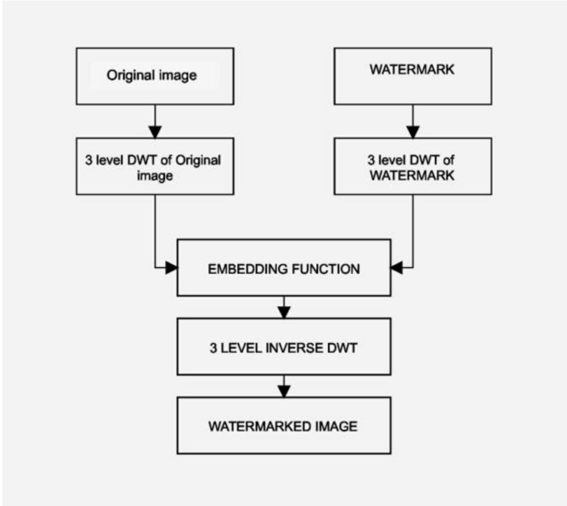

Fig -8: Embedding Flowchart

5.2 Extracting DWT watermark

Fig -9 shows the extracting flowchart for DWT. Here, DWT coefficients of levels 2 and 3 of the original image are subtracted from every DWT coefficient of levels 2 and 3 of the watermarked image. The differences are added and if their sum's differences is greater than 0, the value of the detected bit is considered to be 1, else 0

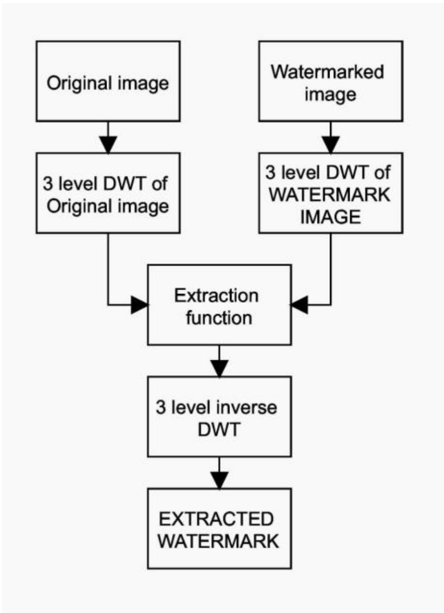

Fig -9: Extracting Flowchart

6. RESULTS

In this work, both the watermarking methods use the original non marked image for the detection of the watermark thus making the system a private invisible digital watermarking system. Also in this paper, the correlation coefficient which is the similarity measure between the original watermark and extracted watermark is calculated using MATLAB function "corr2". As this correlation coefficient approaches close to 1, it is determined that both the original and extracted watermarks are almost matching.

To test the quality of the detected watermark which is called the robustness of the watermarking system, there are a series of attacks performed: JPEG compression, cropping, contrast modification, brightness modification, filtering and adding noise. After every attack, a watermark is extracted and is compared with the original watermark using correlation coefficient.

When the watermarked images are not prone to any attacks, the DCT and DWT techniques yield a good correlation coefficient value as shown in Table -1.

Table -1: Correlation coefficient of original and detected watermark without attacks

DCT	DWT
0. 987946	1

The JPEG compression attacks are performed for 10 qualities and the correlation coefficient values are as listed in Table -2. It shows that the values in case of the DWT methods are higher than 0.5 which is up to 20% of JPEG compression quality. Hence DWT method is more robust.

Table -2: Correlation coefficient of original and detected watermark after JPEG Compression attack

Quality	DCT	DWT
10	0.163426	0.318756
20	0.295148	0.587610
30	0.332688	0.610387
40	0.387562	0.725036
50	0.421597	0.836497
60	0.503624	0.803412
70	0.586931	0.901479
80	0.690752	0.966587
90	0.706981	0.975905
100	0.996308	1

Brightness implies the indication of more gray level in an image. This attack is done over 10 different levels and the correlation coefficient values are as listed in Table -3. It is observed that on a majority DCT method is more robust than DWT.

Table -3: Correlation coefficient of original and detected watermark after brightness attack

Level	DCT	DWT
0.1	0.962381	1
-0.1	0.967857	0.994860
0.2	0.93785	0.971269
-0.2	0.882490	0.921475
0.3	0.819575	0.849625
-0.3	0.726942	0.612589
0.4	0.652369	0.603470
-0.4	0.606777	0.325871
0.5	0.456297	0.409787
-0.5	0.425778	0.214085

Contrast is the ratio of minimum and maximum values of the gray level in the images. While histogram is the distribution of the gray level over the image. Correlation coefficient values for original and detected watermark with histogram equalization contrast attack is listed in Table -4. It is seen that both methods show approximately same values for this attack.

Table -4: Correlation coefficient of original and detected watermark after contrast attack

Level	DCT	DWT
0.5	0.152364	0.251268
0.6	0.180369	0.278569
0.7	0.236187	0.284156
0.9	0.279641	0.281456
1.1	0.286147	0.278945
1.4	0.291025	0.271025
1.5	0.296947	0.276301
1.6	0.300156	0.269785
1.7	0.314789	0.268941
1.8	0.297510	0.087456

Cropping is altering the image by removing some part of it, while the removed part are padded with 0s. Different levels of cropping is done and their correlation coefficient values are listed below in Table -5. It is seen that both methods perform well even after half of the pixels are replaced by zeros.

Table -5: Correlation coefficient of original and detected watermark after cropping attack

Level	DCT	DWT
1.1	0.164259	0.065148
1.2	0.275630	0.154783
1.4	0.469512	0.289641
1.6	0.584102	0.423271
1.8	0.650326	0.539245
2	0.720159	0.674715
4	0.926314	0.970364
8	0.985201	0.983014
16	0.980236	0.995214

Image filtering is performed by convolution of image and the impulse response of the filter. Averaging (LF filtering) and Sharpening (HF filtering) are also performed on the image and their values are listed in Table -6. It is concluded that on a majority basis DWT is more robust than DCT as it doesn't tolerate averaging.

Table -6: Correlation coefficient of original and detected watermark after filtering attack

Type	DCT	DWT
Average	0.186485	0.465120
Gaussian	0.762014	0.920365
Laplace	0.624596	0.892145
Log	0.542360	0.810265
Median	0.317526	0.69785
Unsharp	0.564523	0.804526

Noise is an unwanted pixel that doesn't belong to the original picture. Gaussian noise, impulse noise (Salt & pepper) which is characterized by pixels that deviate from their surroundings, and Speckle noise, which is a multiplicative noise are the different types of noise attacks that are performed on the watermark. Their values are listed in Table -7. It is seen that DWT is more robust except for salt & pepper noise attacks, where the situation is unresolved.

Table -7: Correlation coefficient of original and detected watermark after noise attack

Type	DCT	DWT
Gaussian	0.275630	0.569085
Salt & Pepper	0.542697	0.510697
Speckle	0.302689	0.536478

7. CONCLUSION

In this paper, two different types of invisible digital image watermarking methods using DCT and DWT techniques are implemented. Their Robustness is compared after different types of attacks and degradation. The correlation coefficient which is the similarity measure of the original and extracted watermark are taken as a measure for Robustness.

Considering the obtained results, it is concluded that invisible digital image watermarking based on DWT technique is more robust than the image watermarking based on DCT technique.

REFERENCES

[1] Cox, IJ, Miller, ML & Bloom, JA 2002, "Digital Watermarking", Morgan Kaufmann Publisher, San Francisco, CA, USA 2002

[2] Christine I. Podilchuk, Edward J. Delp, —"Digital watermarking: Algorithms and application", IEEE Signal processing Magazine, July 2001.

[3] Sumedh P. Ingale, Dr.C.A.Dhote,"A Survey Of Digital Watermarking Techniques"

[4] Vinita Gupta,Mr.Atul Barve ,"A Review on Image Watermarking and Its Techniques"

[5] Manpreet Kaur, Sonika Jindal, Sunny Behal," A STUDY OF DIGITAL IMAGE WATERMARKING"

[6] Lalit Kumar Saini, Vishal Shrivastava " A Survey of Digital Watermarking Techniques and its Applications"

[7] G. Rosline Nesa Kumari, B. Vijaya Kumar, L.Sumalatha, and Dr V. V. Krishna," Secure and Robust Digital Watermarking on Grey Level Images", International Journal of Advanced Science and Technology, 2009

[8] Baisa L. Gunjal, R.R. Manthalkar, "An overview of transform domain robust digital image watermarking algorithms", Journal of Emerging Trends in Computing and Information Sciences, 2010

[9] W. Hong and M. Hang, "Robust Digital Watermarking Scheme for Copy Right Protection," IEEE Trans. Signal Process, 2006.

[10] D.S. Bormane, Pallavi Patil, “DWT Based Invisible Watermarking Technique for Digital Images”, International Journal of Engineering and Advanced Technology (IJEAT) , April 2013, ISSN: 2249 – 8958, Volume-2, Issue-4

[11] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, “Lsb Based Digital Image Watermarking For Gray Scale Image” IOSR Journal of Computer Engineering (IOSRJCE)

[12] Qing Liu,Jun Ying(2012),”Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis”

[13] Mohamed Sathik, SS Sujatha, “A novel DWT based Invisible Watermarking Technique for Digital Images”, International Arab Journal of e-Technology, Jan 2, Vol.2, No.3

[14] Li Sukang, Mei Jiansheng, and Tan Xiaomei, “Digital Watermarking Algorithm Based On DCT and DWT”, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA’09), China, May 22-24, 2009, pp. 104-107

[15] Ikpyo Hong, Intaek Kim, Seung-So0 Han, “A Blind Watermarking Technique Using Wavelet Transform”, ISIE 2001, Pusan, KOREA, 07803-70~9-2/01, IEEE

[16] Pravin M. Pithiya, H.L.Desai, “DCT Based Digital Image Watermarking, Dewatermarking & Authentication”, International Journal of Latest Trends in Engineering and Technology (IJLTET) , Issue 3 May 2013, Vol. 2

[17] Shahin Shaikh, Manjusha Deshmukh, “Digital Image Watermarking In DCT Domain, International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April 2013

[18] Sharma, Janki Ballabh et al. “Comparison of Bit Error Rate Performance Measure of Robust Watermarking Scheme Based On Self-Fractional Fourier Functions , Empirical Mode Decomposition and Cyclic Encoding.” (2013).