ISSN:0975-9646

A Study Combined DWT-DCT Digital Image Hiding Information

Jyoti sahu
Department of Electronics & Telecommunication Engineering,
Shri Shankaracharya Technical Campus Bhilai, India

Dolley shukla
Sr. Associate Professor (IT) Professor and Associate Director,
Faculty of Engineering & Tech, Shri Shankaracharya Technical campus Bhilai,India

Abstract- Digital Hiding information has emerged as a new area of research in an attempt to prevent illegal copying and duplication. In this paper, represent both method i.e. DCT&DWT based algorithm for watermarking in digital image .In order to compare the imperceptibility &robustness of both the algorithms make use of simple attacks such as resizing rotation& copping.

Index Terms- Digital watermarking, discrete cosine transform (DCT),discrete wavelet transforms(DWT), Peak signal to noise ratio (PSNR),Mean squared error (MSE).

1. INTRODUCTION

Hiding information is a technique used to hide data or identifying information within digital multimedia. Our discussion will focus primarily on the watermarking of digital images, though digital video, audio, and documents are also routinely watermarked. Digital Hiding information is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information. Because of this use, watermarking techniques are often evaluated based on their invisibility, recoverability, and robustness. Our goal was to implement two different watermarking methods and evaluate their susceptibility to attack by various image processing techniques. Additionally, we wanted to create a GUI that would allow users unfamiliar with Matlab to add and extract watermarks, as well as evaluate their respective robustness based on a few morphological image attack.[1]

It is desirable to develop analytical statemen about water [7]

2.4. Key restrictions:

An important distinguishing characteristic is the level of restriction placed on the ability to read a watermark.

As explained in earlier sections, we describe watermarks in which the key is available to a very large number of detectors as “unrestricted-key” watermarks, and those in which keys are kept secret by one or a small number of detectors as “restricted-key” watermarks.[7]

2.5. Modification and multiple watermarks:

In some circumstances, it is desirable to alter the watermark after insertion. For example, in the case of digital videodiscs, a disc may be watermarked to allow only a single copy.

Once this copy has been made, it is then necessary to alter the watermark on the original disc to prohibit further copies. [7]

2. PROPERTIES OF DIGITAL WATERMARK:

There are a number of important characteristics that a watermark can exhibit. The characteristics are discussed in more detail next.

2.1. Fidelity:

The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content.

In earlier work, we had used the term imperceptible”, and this is certainly the ideal.[7]

2.2. Robustness:

Music, images and video signals may undergo many types of distortions. Lossy compression has already been mentioned, but many other signal transformations are also common. For example, an image might be contrast enhanced and colors might be altered somewhat, or an audio signal might have its bass frequencies amp lied.

In general, a watermark must be robust to transformations that include common signal distortions as well as digital-to-analog and analog-to-digital conversion and lossy compression.[7]

processing that is solely intended to remove them, in addition to being robust against the

2.3. Tamper-resistance Watermarks are often required to be resistant to signal signal distortions that occur in normal processing. We refer to this property as tamper-resistance

2.6. Data payload:

Fundamentally, the data payload of a watermark is the amount of information it contains. As with any method of storing data, this can be expressed as a number of bits, which indicates the number of distinct watermarks that might be inserted into a signal.

If the watermark carries N bits, then there are 2N different possible watermarks. It should be noted, however, that there are actually 2N + 1 possible values returned by a watermark detector, since there is always the possibility that no watermark is present[7]

2.7. Computational cost:

As with any technology intended for commercial use, the computational costs of inserting and detecting watermarks are important. This is particularly true when watermarks need to be inserted or detected in real-time video or audio.[7]

3. TYPES OF WATERMARKING

3.1 **Division Based On HumanPerceptoin**

This is sub-divided into visible watermarks and invisible watermarks.

3.1.1 Visible Watermarks

These watermarks can be seen clearly by the viewer and can also identify the logo or the owner. Visible watermarking technique changes the original signal The watermarked signal is different f rom the original signal [http://en.wikipedia.org/wiki].Visible watermark embedding algorithms are less computationally complex.[2]

3.1.2 Invisible Watermarks

These watermarks cannot be seen by the viewer. The output signal does not change much when compared to the original signal. The watermarked signal is almost similar to the original signal [http://en.wikipedia.org/wiki]. As the watermark is invisible, the imposter cannot crop the watermark as in visible watermarking. Invisible watermarking is more robust to signal processing attacks when compared to visible watermarking. As the quality of the image does not suffer much, it can be used in almost all the applications [2].

3.2 Division Based On Applacation

Based on application watermarks are sub-divided into fragile, semi-fragile and robust watermarks.

3.2.1 Fragile Watermarks

These watermarks are very sensitive. They can be destroyed easily with slight modifications in the watermarked signal .

3.2.2 Semi- fragile Watermarks

These watermarks are broken if the modifications to the watermarked signal exceed a pre-defined user threshold. If the threshold is set to zero, then it operates as a fragile watermark.[3]

3.2.3 Robust Watermarks

These watermarks cannot be broken easily as they withstand many signal processing attacks. Robust watermark should remain intact permanently in the embedded signal such that attempts to remove or destroy the robust watermark will degrade or even may destroy the quality of the image.[3]

3.3 Division Based On Level Of Information Required To Detect The Embedded Data [6]

3.3.1 Blind Watermarks

These watermarks detect the embedded information without the use of original signal. They are less robust to any attacks on the signal.

3.3.2 Semi-blind watermarks

These watermarks require some special information to detect the embedded data in the watermarked signal.

3.3.3 Non Blind watemarking

These watermarks require the original signal to detect the embedded information in the watermarked signal. They are more robust to any attacks on the signal when compared to blind watermarks.

3.4 Based On User's Authorization To Detect The Watermark [6]

This is sub-divided into public watermarks and private watermarks.

3.4.1 Public Watermarks

In this watermarking, the user is authorized to detect the watermark embedded in the original signal.

3.4.2 Private Watermarks

In this watermarking, the user is not authorized to detect the watermark embedded in the original signal.

4 MAIN ALGORITHMS OF DIGITAL WATERMARKING

In recent years, the study of digital watermarking technology makes great progress. There are a lot of good algorithms which can be divided into spatial domain algorithm and transform domain algorithm.

4.1 Spatial domain algorithms

Spatial domain digital watermarking algorithms directly load the raw data into the original image.

4.1.1 Last significant bit algorithm

The algorithm embeds the information with the form of the least significant bits selected randomly which can ensure the embedded watermark is invisible. But the algorithm has poor robustness, and watermark information can easily be destroyed by filtering, image quantization, and geometric distortion.

4.1.2 Patchwork algorithm

Based on the statistics, the algorithm uses the statistical characteristics of pixels to embed the information into the brightness values of pixel. It can resist lossy compression coding and malicious attacks. However, the amount of embedded information is limited, in order to embed more watermark information; we can segment the image, and then implement the embedding operation each image block.

4.1.3 Texture mapping coding method

It hides the watermark in the texture part of the original image. The algorithm has strong resistance ability to attacks for a variety of deformation, but only suitable for areas with a large number of arbitrary texture images, and cannot be done automatically.

4.2 TRANSFROM DOMAIN DIGITAL WATERMARKING ALGORITHM

Transform domain algorithm is a method of hiding data similar to spread-spectrum communication technology. Firstly, it does a kind of orthogonal transformation forimage, and then embed watermark information in the transform domain of image, finally use the inverse transform to recovery the image in spatial domain, the detection an extraction of the watermark are also realized in transform domain. There are several common used transform domain methods,

4.2.1 Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies [8]. For an input image, X, of size N x N the DCT coefficients for the transformed output image, Y, are computed according to (1). X (i, j) is the intensity of the pixel in row i and column j of the image, and Y (u, v) is the DCT coefficient in row u and column v of the DCT matrix.

$$Y(u,v) =$$
$$C_u C_v \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{Cos((2j+1)y\pi)}{2N} \frac{Cos((2i+1)x\pi)}{2N}$$

Where,

$$C_u C_v = \sqrt{\frac{1}{N}} \text{ for u, v=0 and}$$

$$C_u C_v = \sqrt{\frac{2}{N}} \text{ for u ,v = 1,2.- - - - - -(N-1)}$$

Where,
for u, v=0 and
for u ,v = 1,2.- - - - - -(N-1)

Performing DCT of an image gives rise to three different frequency coefficient tsets:lowfrequency, mid frequency and high frequency coefficient sets as The DCT has a special property that most of the visually significant information of the image is concentrated in just a few coefficients of the DCT [1]-[3].

4.2.2 Discrete Wavelet Transform (DWT)

Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error [8]-[9]. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub bands, a lower resolution approximation image (LL1), horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components. The process can be repeated to obtain multiple scale wavelet decomposition.

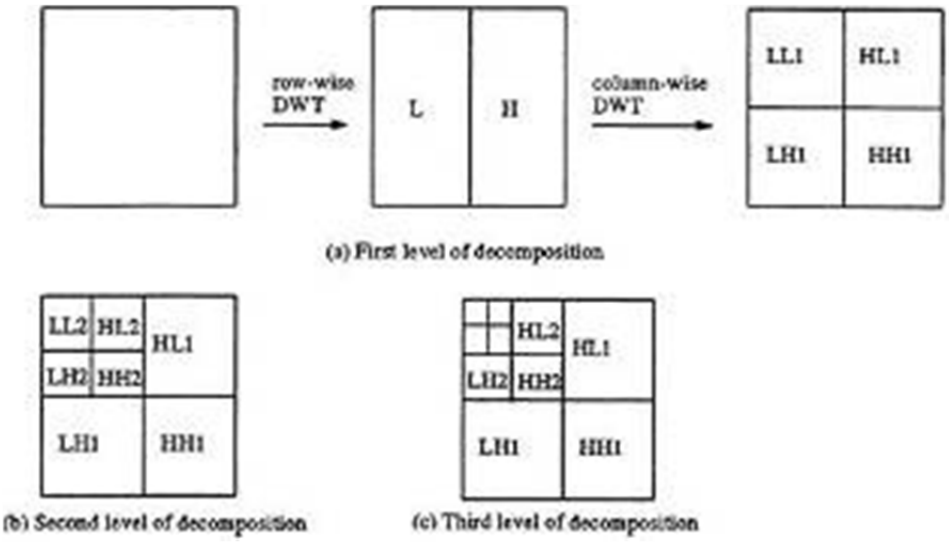
One of the advantages of DWT over DCT is that it can more accurately model the aspects of the compared to DCT [8]-[9]. In general most of the image energy is concentrated at the LL sub band and hence embedding watermarks in this sub band may degrade the image quality, but embedding watermark in this subband can provide higher robustness. On the other hand, the detail sub bands LH, HL and HH include the edges and textures of the image and the human eye is generally not much sensitive to changes in these sub bands. Hence embedding watermarks in these sub bands can provide higher imperceptibility, without being perceived by human eye. But the noise attacks and lossy compression results in data loss at high frequencies and hence the robustness may suffer for the watermarks embedded in the HH sub band. Hence many of the watermark embedding schemes opts for the LH or HL sub band for embedding the watermark in order to provide both imperceptibility and robustness [10].

The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges [14].

In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1 . for each successive level of decomposition, the LL sub-band of the previous level is used as the input . To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub –

To perform third decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-band –LL3, LH3 HL3, HH3. This results in 10 sub-band per component. LH1, HL1, and HH1 contain the highest frequency band. The three-level DWT decomposition is shown in Fig.1 are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, The Wavelet Transform suits many applications very well.

DWT is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution [8].



(a) First level of decomposition

(b) Second level of decomposition

(c) Third level of decomposition

Fig:- 1 Three level DWT decompositio

5. COMPARSION TABLE FOR VARIOUS WATERMARKING SCHEMES

S.NO	Year of publication	Name of journal	Title	Method	Result
DCT based watermarking schemes					
1	2004	IEEE	A novel DCT-based for secure colour image watermarking	Modifies the middle coefficient of dct of original image to embed the watermark. Threemethodareimplemented (HVS,2D periodic torus perprocessing algorithm) to improve robustness and security.	High quality watermarked image is obtained with PSNR=57.9db After attack NC=1 is reduced to NC=0.8 i.e Less degradation of image.
2	2007	IEEE	Embedding image watermarking in dct componentes	Quantitative analysis on the magnitudes of DCT components of host images based on HVS.	When attack is applied average PSNR value = 43 dB is reduced as low as 13dB.
3	2010	IEEE	Improving the robustness of DCT based image watermarking	Pseudorandom permutation FDCT, middle frequency coefficient of DCT	When attack is applied average PSNR value = 40.83 dB is reduced as low as 31.27 dB. Image resampling and image rotation, are still challenging to our current work,
4	1999	IEEE	Hidden digital watermarks in image processing	Based on concept of mathematical remainder by modifying the low frequency coefficient of DCT.	Suitable for highly JPEG compressed image
5	2001	IEEE	Improved wavelet-based watermarking through pixel-wise masking	Operate in the wavelet domain; masking is accomplished – pixel by pixel by taking into account the texture and luminance contents of all the subbands.	Average PSNR=36 dB After attack by image cropping result was surprisingly high.
6	1998	IEEE	Wavelet transform based watermark for digital image	Pseudo random codes are added to the large coefficients at the high and middle frequency bands of the DWT (haar wavelet) of an image.	Result show that DWT is better than DCT by using EZW and halftoning
7	2012	ACR	Image watermarking using 2-level DWT	2-level DWT and alpha bending technique	Best result obtain at k=0.98 Shows that 2 level DWT is better than1 level DWT.
8	2012	IJMEC	Image watermarking using 3 level DWT	3-level DWT by alpha bending embedding technique.	3 level DWT is better than 2 level DWT
DCT Vs DWT					
9	2010	IJAEA	Discrete cosine transform vs discrete wavelet transform:	DCT with scalar quantization and Huffman coding based JPEG encoder. DWT-3level wavelet with SPIHT	In DWT method , when attack is introduced PSNR vary from 38.36 to 30.13 whereas in case of DCT its value vary by 38.04 to 28.50. in terms of variations Thus DWT is better
10	2011	IJIEA	Comparative analysis between DCT&DWT Techniques of image compression	DCT-Quantization DWT-Analysis is computed by filter bank HPF (detail part), LPF (approximation part) and downsampling	DWT technique is much efficient than DCT technique in quality and efficiency wise but in performance time wise DCT is better than DWT
Joint DCT-DWT based watermarking scheme					
11	2007	JCS	Combined DWT-DCT Digital Image watermarking.	Combined DWT and DCT using pn sequence. DWT-2-level subband (HL2,HH2) DCT-middle frequency	Comparison of DWT and DCT-DWT is analyzed. Psnr value obtained by DWT (HL2/HH2) is 80 dB/77 dB where as in case of joint DCT-DWT it is 97 dB. After attack NC value in DWT reduces to 0.447 from 1 where as its value in DCT-DWT reduces only to 0.968.
12	2012	ITEEE	Image watermarking in DCT-DWT domain	Two different methods of image watermarking are described, using combined DCT-DWT transform. In the first approach, the two smaller sub bands of the HL sub band LH2 and HL2 are used to embed the watermark and in the second approach all the four smaller sub bands of the HL sub band are used to embed the watermark.	The imperceptibility and robustness of the four sub band method psnr=43 dB is comparatively higher than the two sub band method i.e. 40 dB. But for rotation attack psnr is as low as 8.63.
13	2012	IEEE	A joint DWT-DCT based watermarking technique	Joint DCT-DWT technique based on low frequency watermarking with weighted correction.	Results show that the proposed algorithm apparently preserves superior image quality and robustness under various attacks.
14	2008	IEEE	A New robust digital image watermarking technique based on joint DWT-DCT transfromation	Embed the watermark in the special middle frequency of3 DCT in the sub bands of 3levelsDWTtransformed of a host image.	Results show that the imperceptibility of the watermarked image is acceptable but for rotation attack psnr is reduced from 37.67 dB to 8.63. Further studies are needed on improving the robustnes

CONCLUSION

It is concluded from the above discussion that a lot of work going on in the field of combined DWT-DCT digital watermarking. Various digital watermarking models in DCT based ,DWT based and joint DWT-DCT based domain are explored to minimize the mean square error and hence improving the PSNR.

REFERENCES

[1] I.J.Cox,M.L.Miller and J.A.Bloom “Watermarking application and their properties” proc.intern.Conf.on Information Technology2000,Las vegas 2000

[2] Latha, M.M., Pillai, G.K. and Sheela, K.A. (2007), “Watermarking based content Security and Multimedia Indexing in digital Libraries”, International Conference on Semantic Web and Digital Libraries (ICSD). ARD Prasad & D. P. Madalli (Eds.).

[3] Bender, W., Gruhi, D., Morimota, N. and Lu, A. (1996), “Techniques for Data Hiding”, IBM Systems Journal, Vol. 35, No. 3 & 4.

[5] Lee, J. and Jung, S. (2001), “A survey of watermarking techniques applied to multimedia”, Proceedings IEEE International Symposium on Industrial Electronics (ISIE), Vol. 1, pp. 272-277.

[6] Kamaldeep (2012)” Classification of Watermarking Based upon Various Parameters” International Journal of Computer Applications & Information Technology Vol. I, Issue II, September 2012 (ISSN: 2278-7720)

[7] Prabhishek Singh, R S Chadha” A Survey of Digital Watermarking Techniques, Applications and Attacks International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013

[8] Voloshynovskiy, Sviatolsav, Shelby Pereira, Thierry Pun, Joachim J. Eggers, and Jonathan K. Su. "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks." Communications Magazine, IEEE 39, no. 8 (2001): 118-126.

[9] Radharani, S., and M. L. Valarmathi. "A study on watermarking schemes for image authentication." International Journal of Computer Applications 2, no. 4 (2010): 24-32

[10] Hsu, Chiou-Ting, and Ja-Ling Wu. "Hidden digital watermarks in images." Image Processing, IEEE Transactions on 8, no.

[11] Huang, Jiwu, Yun Q. Shi, and Yi Shi. "Embedding image watermarks in DC components." Circuits and Systems for Video Technology, IEEE Transactions on 10, no. 6 (2000): 974-979.

[12] Ahmidi, Narges, and Reza Safabakhsh. "A novel DCT-based approach for secure color image watermarking." In Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on, vol. 2, pp. 709-713. IEEE, 2004.

[13] Lin, Shinfeng D., Shih-Chieh Shie, and Jim Yi Guo. "Improving the robustness of DCT-based image watermarking against JPEG compression."Elsev Computer Stand