International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 5 (June 2013), PP. 104-109

DWT Based Digital Image Watermarking, De-Watermarking & Authentication

Pravin M. Pithiya[1], H.L.Desai[2]
[1]PG Student, Department of Electronics & Communication Engineering SPCE, Visnagar, Gujarat, India
[2]Assistant Prof. Department of Electronics & Communication Engineering SPCE, Visnagar, Gujarat, India

Abstract:- This paper introduces an algorithm of digital image watermarking based on Discrete Wavelet Transform (DWT). In this technique the embedding and extraction of the watermark is simple than other transform. In this algorithm watermarking, de watermarking of the image is done and it also checks the authentication of the watermarked image and de watermarked image. This paper also successfully explains digital image watermarking based on discrete Wavelet transform by analysing various performance parameters like PSNR,MSE,SNR and NC.

Keywords:- Authentication, Digital watermarking, De- watermarking, Discrete Wavelet Transform (DWT), Discrete Cosines Transform (DCT,) human visual system (HVS), MSE(Mean Squared Error), NC(Normalised co relation factor), PSNR(Peak Signal to Noise Ratio), SNR(Signal to Noise Ratio).

I. INTRODUCTION

The use of internet growing faster day to day and the need to display multimedia contents on the internet become necessary. Intellectual property right; documents are not fast information but property. YouTube, face book, Torrents, pirate bay such other video, audio, image, documents resource websites are now became water and food for youngsters across the globe so it is necessary to protect the rights of authors. so digital protection is necessary and in-evitable. There are many popular techniques for this such as Steganography, Digital signature, Fingerprinting, cryptography and Digital watermarking but Digital watermarking is proved best out of them. Digital watermarking is nothing but the technology in which there is embedding of various information in digital content which we have to protect from illegal copying. This embedded information to protect the data is embedded as watermark. Beyond the copyright protection, Digital watermarking is having some other applications as Broadcast monitoring, Indexing, fingerprinting, owner identification, etc. Digital watermarks are of different types as robust, fragile, semi fragile, visible and invisible. Application is depending upon these watermarks classifications. There are some requirements of digital watermarks as integrity, robustness and complexity.

In digital watermarking, a watermark is embedded into a cover image in such a way that the resulting watermarked signal is robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment. This project presents a digital image watermarking based on two dimensional discrete wavelet transform (DWT). Signal to noise ratio (SNR), MSE(Mean Squared Error), NC(Normalised co relation factor), PSNR(Peak Signal to Noise Ratio) and similarity ratio (SR) are computed to measure image quality for each transform..

According to Working Domain, the watermarking techniques can be divided into two types

a) Spatial Domain Watermarking Techniques

b) Frequency Domain Watermarking Techniques

In spatial domain techniques, the watermark embedding is done on image pixels while in frequency domain watermarking techniques the embedding is done after taking image transforms. Generally frequency domain methods are more robust than spatial domain techniques[1].

Spatial Domain Techniques

Spatial watermarking can also be applied using colour separation. In this way, the watermark appears in only one of the colour bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. However, the mark appears immediately when the colours are separated for printing. This renders the document useless for the printer; the watermark can be removed from the colour band. This approach is used commercially for journalists to inspect digital pictures from a photo-stock house before buying unmarked versions[1].

(a) Least Significant Bit(LSB)

The earliest work of digital image watermarking schemes embeds watermarks in the LSB of the pixels. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (i.e., least significant) bit, of selected pixels of the image. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. For instance, an attacker could simply randomize all LSBs, which effectively destroys the hidden information [1].

(b) SSM Modulation Based Technique

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. This is done for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, and to prevent detection. When applied to the context of image watermarking, SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark[1].

Frequency Domain Techniques

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. For example, the HVS is more sensitive to low-frequency coefficients, and less sensitive to high-frequency coefficients. In other words, low-frequency coefficients are perceptually significant, which means alterations to those components might cause distortion to the original image. On the other hand, high-frequency coefficients are considered insignificant; thus, processing techniques, such as compression, tend to remove high-frequency coefficients aggressively. To obtain a balance between imperceptibility and robustness, most algorithms embed watermarks in the midrange frequencies[1][2].

(a)Discrete Cosine Transformation (DCT)

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image[1][2][7].

(b)Discrete Wavelet Transformation (DWT)

The Discrete Wavelet Transform (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. Wavelets have their energy concentrated in time and 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. One of the main challenges of the watermarking problem is to achieve a better trade-off between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies[1][6] .

II. BASICS OF DWT

The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. A two-dimensional image after three-times DWT decomposed can be shown as Fig.1. Where, L represents low-pass filter, H represents high-pass filter. An original image can be decomposed of frequency districts of HL1, LH1, HH1. The low-frequency district 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.
The information of low frequency district is a image close to the original image. Most signal information of original image is in this frequency district. The frequency districts of LH, HL and HH respectively represents the level detail, the upright detail and the diagonal detail of the original image[11] [13][14] [17].

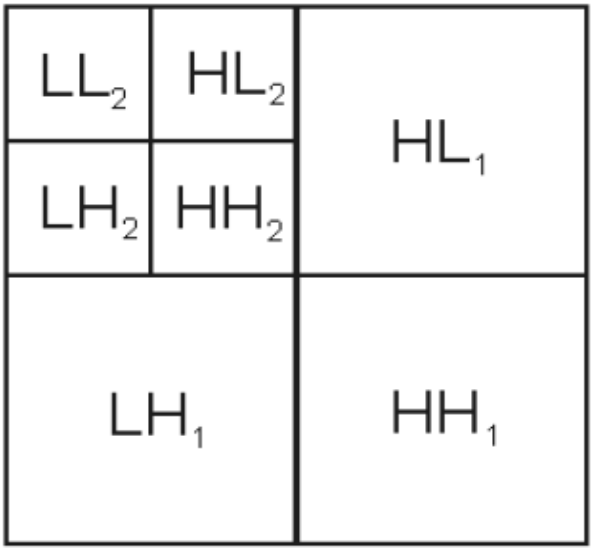

Figure 1.DWT Decomposed [11]
According to the character of HVS, human eyes is sensitive to the change of smooth district of image, but not sensitive to the tiny change of edge, profile and streak. Therefore, it's hard to conscious that putting the watermarking signal into the big amplitude coefficient of high-frequency band of the image DWT transformed. Then it can carry more watermarking signal and has good concealing effect[9].

III. PROPOSED METHOD OF WATERMARK EMBEDDING & EXTRACTION PROCESS:

3.1 Watermark Embedding using DWT:

The Procedure of watermark embedding is shown in fig.2.

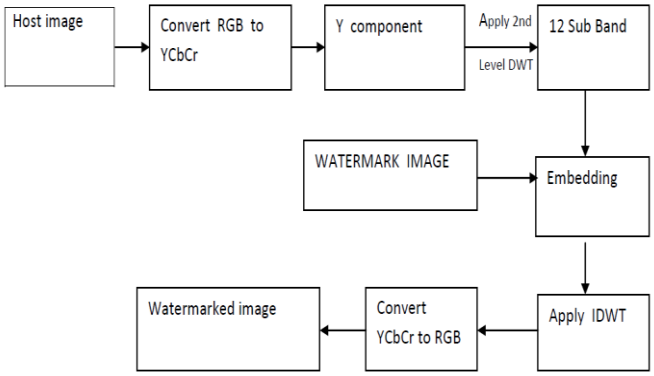

Figure 2: Flowchart of Watermark Embedding Process

Algorithm for watermark embedding :

The Watermark embedding steps using this technique are following:

1. Read colour host image.
2. Convert RGB to YC_bC_r components.
3. Apply 2^{nd} level DWT.
4. Embed the watermark components in to the frequency subcomponents .
5. Apply IDWT.
6. Convert YC_bC_r to RGB.
7. Get watermarked image

8. Check Authentication.

3.2 Watermark Extraction using DWT:

The Procedure of watermark extracting is shown in fig.3.

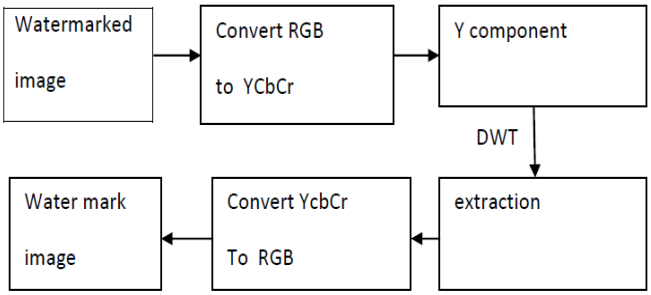

Figure 3: Flowchart of Watermark Extraction Process

Algorithm for watermark extraction :

The Watermark extraction steps using this technique are following:

1. Read Watermarked image.
2. Convert RGB to YC_bC_r components.
3. Apply DWT.
4. Extract the watermark components from frequency subcomponents .
5. Convert YC_bC_r to RGB.
6. Get watermark image
7. Check Authentication.
8. Calculate for MSE,PSNR,SNR&NC.

IV. PERFORMANCE EVALUATION

To evaluate the performance of the proposed method, we have to check the performance parameters. In this experiment the host image is LENA of size 512*512 and the watermark image is a symbol of size 256*256 which is shown in figure 4 respectively. In our proposed algorithm, we have set gain factor =0.5.This algorithm has been implemented using MATLAB 10a.

Imperceptibility: Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark. To measure the quality of a watermarked image , the peak signal to noise ratio (PSNR) is used. The Visual quality of a watermarked image is evaluated by the peak signal-to-noise ratio (PSNR).

It is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

Where, MSE=Mean Squared Error between Original and distorted image. which is defined

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j) - K(i,j)\right]^2$$

Robustness: Robustness is a measure of the immunity of the watermark against attempts to remove or degrade it, internationally or unintentionally, by different types of digital signal processing attacks. We measured the similarity between the original watermark and the watermark extracted from the attacked image using the Normalized correlation factor given below Eq.

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j) * W'(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} W^2(i,j)}$$

Where N*N is the size of watermark, W (i j) and W' (i j) are the watermark and recovered watermark images respectively[15].

V. SIMULATION RESULTS

This section described results of proposed method for watermarking, de watermarking and authentication.

Figure 4: Original Image

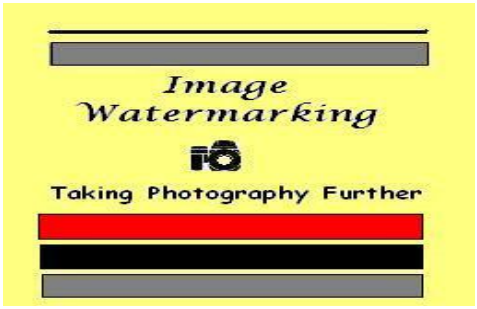

Figure 5: Watermark Image

Figure 6: Watermarked Image and Difference Image

Figure 7 De-watermarked Image and Difference Image

Table 1: Observation for authentication between Original Image and Watermarked Image

Parameter	value
Window size	5
Random point in image	[417 464]
Original Image intensity	207.6
Watermarked Image intensity	220.24

Result: Watermarked Image is authenticated.

Table 2: Observation for authentication between Original Image and De -watermarked Image

Parameter	value
Window size	5
Random point in image	[417 464]
Original Image intensity	207.6
De Watermarked Image intensity	206.04

Result: De Watermarked Image is authenticated.

Table 3: Observation of Performance Parameters for RGB of image

Parameters	Red	Green	Blue
MSE	24.2576	24.3029	24.3508
PSNR	45.1081	45.1	45.0915
SNR	86.0848	81.8587	81.7539
NC	0.99979	0.9994	0.99937

VI. CONCLUSION

There are many types of algorithms for digital image watermarking. Each type of algorithms has its own advantages and disadvantages. No method has perfect solution for digital watermarking. Each type has robustness to some type of attacks but is less efficient to some other types of attacks. each type of digital watermarking depends on the nature of application and requirements. In this paper we presented a new method of embedding watermark into colour image. The RGB image is converted to YCbCr and watermarked by using discrete wavelet transform (DWT). The luminance component Y of image is considered for embedding watermark. The performance of the proposed method can be evaluated by PSNR,SNR,MSE and NC for RED,BLUE and GREEN. Existing techniques have worked on the gray scale of image, we have taken results for RED,BLUE and GREEN separately. Proposed technique results have shown that technique presented in this paper is very effective for watermarking and de watermarking authentication and also support more security and exact correlation between original watermark and extracted watermark.

REFERENCES

[1]. Manpreet Kaur, Sonika Jindal & Sunny Behal " A Study of Digital Image Watermarking" Volume 2, Issue 2(ISSN: 2249-3905) ,February 2012.
[2]. Dr. Vipula Singh "Digital Watermarking: A Tutorial", (JSAT), January Edition, 2011
[3]. Darshana Mistry "Comparison of Digital Water Marking methods" (IJCSE)Vol. 02, No. 09, 2010.
[4]. Saraju P. Mohanty "Digital Watermarking : A Tutorial Review" ,1999
[5]. Prachi Khanzode, Siddharth Ladhake and Shreya Tank "Digital Watermarking for Protection of Intellectual Property" IJCEM, Vol. 12, April 2011.
[6]. Anuradha , Rudresh Pratap Singh "DWT Based Watermarking Algorithm using Haar Wavelet" ISSN 2277-1956/V1N1-01-06
[7]. Charles Way Hun Fung, Antonio Gortan & Walter Godoy Junior "A Review Study on Image Digital Watermarking" 2011.
[8]. Lin Liu "A Survey of Digital Watermarking Technologies", 2005
[9]. Mei Jiansheng1, Li Sukang and Tan Xiaomei "A Digital Watermarking Algorithm Based On DCT and DWT", Nanchang, P. R. China, 2009, pp. 104-107
[10]. Tribhuwan Kumar Tewari, Vikas Saxena "An Improved and Robust DCT based Digital Image Watermarking Scheme", International Journal of Computer Applications (0975 – 8887) Volume 3 – No.1, June 2010
[11]. Vivek Tomar "A Statical comparison of Digital Image Watermarking Techniques",[2012]
[12]. Akhil Pratap Singh "Wavelet Based Watermarking on Digital Image", [2010]
[13]. Shital Gupta, Dr Sanjeev Jain "A Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform", [2010]
[14]. Nikita Kashyap "Image Watermarking Using 3-Level Discrete Wavelet Transform",[2012]
[15]. Noel k.mamalet, "Fundamental concepts and overview of wavelet theory", second edition.
[16]. Rafael C.Gonzalez, Richard E.Woods "Digital Image Processing" second edition.
[17]. Sarvesh Kumar Yadav,Mrs.Shital Gupta,Prof.Vineet richariya "Digital Image Watermarking Using DWT and SLR Techniques against Geometric attacks"IJCTEE, Volume 2,issue1.