ROBUST IMPERCEPTIBLE DIGITAL IMAGE WATERMARKING BASED ON DISCRETE WAVELET&COSINE TRANSFORMS

Raj kumar Jaiswal , S. Ravi

***Abstract*- Digital watermarking is a technique by which we can get the more authentication and copyright protection.In the age of internet,a huge amount of multimedia data has been transferred in terms of audio, video and image.For transferring a data in high speed and secure manner,digital image watermarking is used. To provide an authentication and copyright protection in digital image watermarking, two methods,spatial domain method and frequency domain method are used, where the frequency domain method is too much imperceptibleas compared to spatial domain. The peak signal to noise ratio (PSNR) is used as a metric to evaluate the performances of the method taken for discussion as PSNR value presents the robustness of the watermark.PSNR value is a measure of the watermarked image quality and penalizes thevisibility of noise in an image. Thus, two images that areexactly the same will produce an infinite PSNR value.Thus we can get robust and imperceptible watermarking by using a DWT and DCT algorithm.**

***Index Terms*–Digital Watermarking Technology, Watermarking Technique, PSNR,DWT&DCT.**

I. INTRODUCTION

The words "Digital watermarking " came into existence in 1993 , when Tirkelpresented two watermarking techniques for hiding the watermark data in the images[1]. Watermarking is used for the following reasons:proof of ownership (copyrights and IP protection), copying prevention, authentication, data hiding. Watermarking process divided into two sections, namely, watermark embedding section and watermark detection and extraction section. Digital image watermarking technology has many applications in protection, certification, distribution, digital media and label of the user information.It has become a very important research area in information hiding. In the watermarking field,digital image watermarking is focused because it can provide robustness,imperceptibility, adjustability and security as compared to the other multimedia entities like audio and video.

Raj kumar Jaiswal, Department of Computer Science Pondicherry University, Puducherry-605014, INDIA
S. Ravi, Department of Computer Science Pondicherry University, Puducherry -605014, INDIA

There are three healthy reason for it .First, more number of test images can be obtained easily.Secondly, enough redundant information can be transferred to provide a chance to embeddedthewatermark easily.Third, any image watermarking algorithm can be upgraded for the audio and video watermarking also.The success of the high speed internet,cost-effective and popular digital recording and storage devices, the higher bandwidth and quality of service for both networks wired and wireless media have made it possible to generate,replicate,transmit, and distribute digital content in an effortless way. The protection of important entities ofdigital media has become an important issue which is solved by digital watermarking efficiently and effectively[2].The general watermarking diagram is shown below in figure 1, in which the circular shape rectangular parts are elective parts.

If the digital image watermarking is to be effective, it should have the following features[3]:

1. Adjustability. The algorithm should be tunable to various degrees of robustness, quality, or embedding capacities to be suitable for diverse applications.

2. Robustness. The embedded watermarks should not be removed or eliminated by unauthorized distributors using common processing methods, concerning with compression, filtering, cropping, quantization and others.

3. Security.The watermarking procedure should rely on secret keys to ensure security, so that pirates cannot detect or remove watermarks by statistical analysis from a set of images or multimedia files. An unauthorized user, who may even know the exact watermarking algorithm, cannot detect the presence of hidden data, unless he/she has access to the secret keys that control this data embedding procedure.

4.Imperceptibility. The watermark should be invisible in a watermarked image/video or inaudible in watermarked digital music. Embedding this extra data must not degrade human perception about the object. Evaluation of imperceptibility is usually based on an objective measure of quality, called peak signal-to-noise ratio (PSNR) or a subjective test with specified procedures. Watermarking deals with decomposing original image called cover image using some Wavelet transforms[4] and embedding watermark into one of the sub bands (LL,LH,HL,HH) the obtained image is called watermarked image (Stego Image), this image have

been transmitted through a channel,where various noisesaffect watermarked image [5],[6],[7]. The receivedside implanted watermark hasbeen extracted from watermarked image[5].For watermark implanting, Discrete Wavelet Transform(DWT) has been used, Domain Wavelet Transform usedDydic DWT[9] . It is used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system[10].

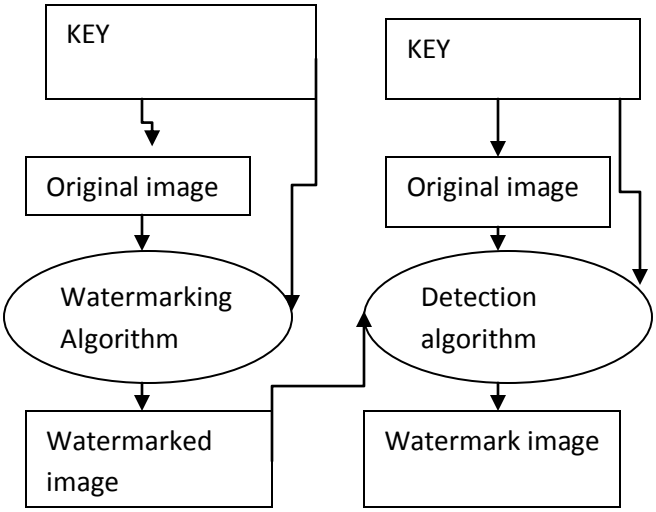

Fig.1.General flow chart of digita lwatermarking.

Further performance improvements in DWT based digital image watermarking algorithms could be obtained by combining DWT with DCT [11]. The idea of applying two transforms is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking. In this paper, we will describe a digital image watermarking algorithm based on comparing two methods; DWT &DCT**.** Watermarking is done in DWT by level1 decomposition and calculating the wavelets coefficients of carefully selected DWT lowest sub-bands, in case of DWT and DCT method level1 decomposition of cover image and calculating the wavelets coefficients of carefully selecting DWT lowest sub-bands followed by the application of the DCT transform of watermark on the selected LL sub-bands. Analysis of image is based on performance parameters like signal to noise ratio (SNR) of original and watermarked image [9] peak signal to noise ratio (PSNR) 2 and 3 wavelet has been used to analyze watermarking .

II.DIGITAL WATERMARKING TECHNOLOGY

As an emerging technology, digital watermarking involves the ideas and theories of different subject coverage, such as signal processing, cryptography, probability theory and stochastic theory,network t echnology, algorithm design and other techniques [12]. Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author‘s serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is should be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenario**.**The domains are different and have their own pros and cons and are used in different scenario**.**

A. Classification of Digital Watermarking[13].

In this section the digital watermarks, features, their techniques and application are classified and segmented into various categories**.**

1) According to characteristics/robustness

*A.Robust:*Robust watermarking is mainly used to specified copyright information of the digital works, the embedded watermark can be oppose the common edit processing, image processing and lossy compression and the watermark is not ruined after some attack and can still be detected to provide certification. It opposes various attacks, geometrical or non-geometrical without affecting embedded watermark**.**

*B.Semi fragile:*Semi fragile watermarking is capable of surviving some degree of the change to a watermarked image, like the addition of quantization noise from lossycompression**.**

2) According to attached media/host signal

*A.Image watermarking***:** This is used to conceal the special information into the image
and to later detect and extract that special information for the author‘s ownership**.**

*B.Video watermarking***:**This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method

has to require real time extraction and robustness for compression

*CAudio watermarking:*This application area of watermarking is one of the most popular and hot issue due to internet music, MP3**.**

D.Text watermarking: This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.

E.Graphic watermarking: It was embeded the watermark to 2D or 3D computer generated graphics to indicate the copyright.

3) According to perceptivity:

A.Visible watermark: The watermark that is visible in the digital data like stamping a watermark on paper, (ex.) television channels, like HBO, whose logo is visibly superimposed on the corner of the TV picture.

*B.Invisible watermarking:*This is a technology available which can embed information into an image which cannot be seen, but can be extract with the right software.It is not able to prevent the theft of our images this way, but We can prove that the image that was stolen was ours , which is almost as good.

4) According to its purpose:

*A.Copyright protection watermarking:*This means if the owner want others to see the mark of the image watermark, then the watermark can be seen after adding the watermark to the image, and the watermark still exists even if it is attacked.

B.Tampering tip watermarking: It protects the integrity of the image content, labels the modified content and resists the usuallossy compression formats.

C.Anti-counterfeiting watermarking: It is added to the building process of the paper notes and can be detected afterprinting, scanning, and other processes.

6) According to domain:

*A.Spatial domain:*This domain focuses on modifying the pixels of one or two randomly selected subsets of images. It directly loads the raw data into the image pixels. Some of its algorithms are Least significant bit,Synchronous state machine modulation based technique.

*B.Frequency domain:*This technique is also called transform domain. Values of certain frequencies are altered from their original. Thereare several commonly used transform domain methods, such as DCT, DWT, and DFT.

7) According to detection process:

A.*Visual watermarking***:**It needs the original data in thetesting course, it has stronger robustness, but its application is limited.

B. Semi blind watermarking: It does not require an original media for detection.

*C.Blind watermarking:*It does not need original data, which has wide application field, but requires a higher watermark technology.

Table I.*Comparision between Spatial domain and Frequency domain***[12][14]**

Feature	Spatial Domain	Frequency Domain
Computation Cost	Low	High
Robustness	Fragile	More robust
Perceptual Quality	High control	Low control
Computational Complexity	Low	High
Computational Time	Less	More
Capacity	High	More
Example of Application	Mainly Authentication	Copy right

IIIDIGITAL WATERMARKING TECHNIQUES

Images are represented andstored in spatial domain as well as in transform domain. The transform domain image which is called frequency domain image is proceed in terms of its frequencies; whereas, in spatial domain, it is proceed by pixels. In general terms, transform domain means the image is segmented into multiresoution frequency. To transfer an image to its frequency representation, we can use several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Each of these transforms has its own characteristics and represents the image in different ways. Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients. In case of spatial domain,which is called pixel domain simple watermarks could be embedded in the images by modifying the pixel values or Least Significant Bit (LSB) values. However, more robust watermarks could be embedded in the transform domain of images by modifying the transform domain coefficients. In 1997, Cox et al. presented a paper "Secure Spread Spectrum Watermarking for Multimedia" [15], one of the most cited paper (cited 2985 times till April' 2008 as per Google Scholar search), and after that most of the research work is based on this work. Even though spatial domain

based techniques cannot sustain most of the common attacks like compression, high pass or low pass filtering etc., researchers presented spatial domain based schemes. First, briefintroductions of some classical well-known spatial domain based schemes are beinggiven as follows [19]:

3.1SPATIAL DOMAIN BASED

3.1.1 LSB BASED SCHEMES

In a digital image, information can be inserted directly into every bit of image information or the more busyareas of an image can be calculated so as to hide such messages in less perceptible parts of an image.Tirkelet.A[17] is one of the first used techniques for image watermarking. Two techniques were offered tohide data in the spatial domain of images by them. These methods were based on the pixel values' Least Significant Bit (LSB) modifications. The algorithm proposed by Kurah and MHughes[16].to embed in the LSB and it was known as image downgrading . An example of the less predictable or less perceptible is Least Significant Bit insertion. This section explains how this works for an 8-bit grayscale image and the possible effects of altering such an image. The principle of embedding is fairly simple and effective. If we use a grayscale bitmap image, which is 8-bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel.

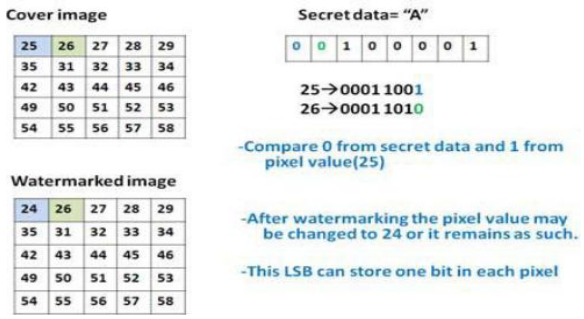

Fig.2 An example of 1 bit LSB [18]

In a gray scale image each pixel is represented by 1 byte consisting of 8 bits. It can be represented by 256 gray colors where 0 is black and 255 is represented as white. The standard of encoding uses the Least Significant Bit of each of these 8 bits , the bit on the right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component, it is mostly not going to be detectable; the human retina becomes the limiting factor in viewing pictures. For the sake of this example only the least significant bit of each pixel will be used for implanting information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example, we change the underline pixel [18]. Schyndel et al. [19] proposed a technique in which a watermark is generated using a m-sequence generator. The watermark was implanted to the least significant bit (LSBs) of the original image to produce host image to the watermarked image. The watermark was extracted from a watermarked image by taking the least significant bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark. They showed that the resultingimage contained an invisible watermark with simple extraction procedures. But the watermark, was not robust to additive noise. Hajjaji*et al.* [20] proposed a method for watermarking of medical image, in which a set of data is inserted in a medical image. The watermarking method is based on the least significant bits (LSBs) in order to check the integrity and confidentiality of, medical information and to maintain confidentiality for the patient and hospital data. For 10% compression rate, the watermark is successfully recovered. Disadvantage of this technique is that all the substituted values are extracted when a Gaussian noise is applied in the watermarked image. Puneet Kr Sharma and Rajni, [21]proposed aimage watermarking technique and different security issues. To hide logo (secretimage) into the cover image they used LSB algorithm. In LSB, each of the pixel of the cover image is replaced by the bits of the secret image. Then 2nd LSB of each pixel of the cover image is replaced by the bits of the secret image and so on. Then PSNR and Mean square error are calculated for different bit substitution from LSB to MSB in image. The PSNR and MSE found for 1st LSB bit substitution was 55.8784 respectively. Deepshikha Chopra et al[23] proposed a watermarking technique and a visible watermarking techniqueusing Least Significant Bit (LSB) algorithm.The least significant bits of pixels are selected to hide the information. They applied various attacks on the watermarkedimage and their impacton the quality of images are measured using MSE and PSNR. KoushikPal[22] presented a biomedical image watermarking technique by modifying bit replacement algorithm in spatial domain, which is much better than the conventional simple LSB technique. They embedded multiple copies of the same information in several bits of the cover image starting from the lower order to the higher orders. So even if some of the information is lost due to an attack,they still collect the remaining information and recover the watermark from the cover image using the bit majority algorithm. Some

of the work done by some authors are shown the table 2.

Table 2. SPATIAL DOMAIN TECHNIQUE

Author Name	FEATURES	RESULT
Hajjaji et al.[20]	Data insertion: i) SHA-1 (Secure Hash Algorithm) ii) Error Correcting Code (ECC): TurboCode Data detection: Harris Corner Detector	For 10% compression rate,the watermark is successfully recovered (for the IRM and Echographicmedi calimages).
Puneet Kr Sharma and Rajni[21]	i) Pseudo-random number generator ii) LSB embedding algorithm	LSB or 1st Bit Substitution PSNR = 55.8784 & MSE =0.1680 8th BitSubstitution PSNR = 14.3467 & MSE =2.3900e+003
Chopra et al[23]	Least Significant Bit (LSB) algorithm	LSB or 1st Bit Substitution PSNR = 54.87 &MSE = 0.21 MSB or 8th Bit Substitution PSNR = 14.3467&MSE=2.3900e+003
Sharma et al [24]	i)A pseudo random number generator ii)The information hiding and extraction system iii)VisualCryptography iv)Two different cover images areused for coveringthe secret share	Watermarked image forBaboons PSNR(with oneLSB) (db) =54.45 PSNR(with three LSB) (db)=44.15 Watermarked image for Leena PSNR(with one LSB) (db) =51.15PSNR(with threeLSB) (db)= 44.17

The features of LSB (Least-Significant-Bit) are:
a. It is simple to understand
b. Easy to implement
c. It results in stego-images that contain hidden data yet appear to be of high visual fidelity[25].

3.2FREQUENCY DOMAIN BASED

Digital Watermarking has emerged as a new area of research in an attempt to prevent illegal copying and duplication. In order to compare the imperceptibility and robustness of the both algorithms make use of simple attacks such as resizing, rotation and cropping.The frequency-domain techniques modify the values of some transformed coefficients. The frequencydomaintechnique first transforms an image into a set offrequency domain coefficients. The watermark is then embedded in the transformed coefficients of the image such that the watermark is invisible and more robust for some image processing operations. Finally, the coefficients are inverse transformed to obtain the watermarked image. Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are the three main methods of data transformation. This technique is complex and watermark cannot be easily recovered at the receiver end as compared to the spatial domain technique.Xiang-Gen Xia *et al*. [26] proposed a watermarkingtechnique based on the DiscreteWavelet Transform (DWT). They performed two–level decomposition using the Haar Wavelet filters. The watermark, modeled as Gaussian noise,was added to the middle and high frequency bands of the DWT transformed image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the end. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images. MahaSharkas*et al*. [27] proposed a dual digital image watermarking technique for improved protection and robustness. They applied frequency domain technique (DWT) into the primary watermark image and then embedded secondary watermark in the form of a PN sequence. The resulting image is embedded into the original image to get the watermarked image. They applied compression, low pass filtering, salt and pepper noise and luminance change attack into the watermarked image to increase the robustness of thetechnique. In all four attacks secondary watermark was detectable. , Chang Dong Yoo*et al*. [28] proposed an algorithm which was based on

embedding the watermark image in three times at three different frequency bands, namely, low, medium andhigh and the results proved that the watermark cannot betotally destroyed by either low pass, medium or high pass filter. P.Ramana Reddy *et al*. [29] proposed an algorithm that embeds and extracts the watermark in frequency domain and it is checked for salt and pepper and Gaussian noise attacks. They applied watermark in the DWT coefficients of the original image.

$$Iw(x,y) = I(x,y) + k.w(x,y) \quad (1)$$

whereIw(x,y) represents watermarked image, k denotes the gain factor. Robustness of the watermarked image increases with the increase in gain k but the quality of the final watermarked image is reduced. Preeti Gupta[30] proposed a cryptography-based blind image watermarking technique that embed more number of watermark bits in the gray scale cover image. They applied blind watermarkingtechnique that uses watermark nesting and encryption. An extra watermark is embedded into the main watermark then main watermark is embedded into the DWT domain of the cover image. This technique embeds more number of bits in the cover image. Mistry[31] proposed digital image watermarking and compared different digital watermarking methods. Image or video is embedded information data within an insensible form for human visual system but in a way that protects from attacks such as common image processing techniques. This paper introduced Spatial domain (like LSB) and transform domain (like DCT, DWT) methods. Authors found that DCT and DWT watermarking is comparativelymuch better but complex than the spatial domain encoding.

Some of the research work done by some of the researchers on frequency domain with their features and results are shown in Table 3. Transformed domain based watermarking schemes are more robust as compared to simple spatial domain watermarking schemes. 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. Either of Discrete Fourier Transform(DFT), Discrete Cosine Transform (DCT) orDiscrete Wavelet Transform (DWT) can be usedbut DCT is the most exploited one. A General transformed domain based scheme, as presented by Cox's[34].

Table3. FREQUENCY DOMAIN TECHNIQUE

Author Name	Features	Result
Harpuneet Kaur[33]	i) Watermark nesting (at level 2) Means embed one watermark in otherand encryption. ii) Used DWT based technique	PSNR of main watermark after embedding watermark1 in it =17.3239 dB PSNR of gray scale cover image after embedding watermarked watermark =37.1587dB
Xia-mu Niu*et al*. [32]	i)Gray level digital watermark ii) Stack filter's threshold decomposition technique iii) DCT	PSNR = 30.7dB Disadv-due to the multiplewaterm arks, the PSNR of the watermarked imageis not very high comparedwith traditionalmethod
Xiang-Gen Xia *et al.* [26]	i)Multiresolutio n watermarking method ii)DWT, iii)Pseudo-random codes, iv) Haar DWT	They test algorithm with common image distortions. Signature can be detected using DWT compared to DCT approach
Maha Sharkas*et al.* [27]	i)Dual watermarking technique ii)DWT domain	PSNR = 44.1065dB Disadv-Secondary watermark was still detectable when multi threshold DWT tech was applied on the watermarked image.

3.2.1DCT BASED WATERMARKING SCHEMES

The Discrete Cosine Transform (DCT) is the most popular, due to several reasons. One of the reason is that the most of the compression techniques are developed in the DCT domain (JPEG, MPEG, MPEG1, and MPEG2) and therefore image processing is more familiar with it. DCT is one of the most common linear transformationsin digital signal process technology. Two-dimensional discrete cosine transform (2D-DCT) is defined

$f(jk) =$
$a(j)a(k)\sum_{m=0}^{N-1} \quad \sum_{n=0}^{N-1} f(nm)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$[2
]

The corresponding inverse transformation (2DIDCT) is defined as

$f(mn)$
$$= \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} a(j) \;\; a(k)f(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad [3]$$

The 2D-DCT can not only concentrate on the main information of original image into the smallest low frequency coefficient, but also it can cause the image blocking effect being the smallest, which can realize the good compromise between the information centralizing and the computing complication [35]. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarkinginformation into the middle frequency bands of an image. In order to invisibly embed the watermark that can survive lossy data compressions, a reasonable tradeoff is to embed the watermark into the middlefrequency range of the image. The middle frequency bands are chosen such that they have minimized that they avoid the most visual important parts of the image (low frequency) without over-exposing themselves to removal through compression and noise attacks. DCT domain watermarking can survive against the attacks such as noising, compression, sharpening, and filtering[36].The popular block-based DCT transform segments image non-overlapping blocks and applies DCT to each block. These results in giving three frequency sub-bands: low frequency sub-band, mid-frequency sub-band and high frequency sub-band. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub band so that the visibility of the image will not be affected and the watermark will not be removed by compression.

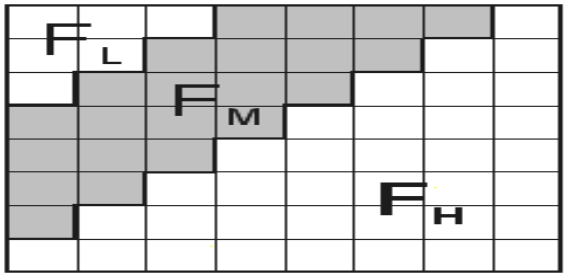

Fig.3 Middle Band Frequencies In 8x8 Dct Block

The DCT allows an image to be broken up into different frequency bands, low frequency band (FL), middle frequency band(FM), and high frequency band(FH). The most appropriate band for altering the watermark is the middle frequency band, because embedding in low frequency band will modify the most important parts of the image and that will degrade image quality and distort it on the other hand modifications in higher frequency is exposing the modified pixels to removal through compression and noise attacks. Middle frequency is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image [37].The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has special property that most of the visually significant information of the image is concentrated in just a few coefficients of the DCT [38]. As DCT is having good energy compaction property, many DCT based digital image watermarking algorithms are developed. It's referred as 'Energy compaction Property'. The DCT for image A with M x N size is given by:

$DCT_{pq} =$
$\alpha_p\alpha_q\sum_{m=0}^{M-1} \quad \sum_{n=0}^{N-1} A_{mn}\cos(\frac{\pi(2m+1)}{2M})\cos(\frac{\pi(2n+1)q}{2N})$(4)

where, 0≤p≤ $M-1$,and 0≤q≤N-1

$$\alpha_p = \begin{cases} {}^{1}/_{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases}$$

$$\alpha_q = \begin{cases} {}^{1}/_{\sqrt{N}}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

Cox et al. [39] proposed a secure spread spectrumwatermarking algorithm. This algorithm uses the Discrete Cosine Transformation in gray scale

image. Existing algorithm is embedded and detectedusing DCT and DWT according to [40]paper.

3.2.2DWT BASED WATERMARKING SCHEMES

Discrete wavelet transforms (DWT), which transforms a discrete time signal to a discrete wavelet representation. It converts an input series x0, x1,xm, into one high-pass wavelet coefficient series and one low-pass wavelet coefficient series (of length n/2 each) given by:

$$H_{i=}\sum_{m=0}^{k-1} x_{2i-m} \,.\, s_m(z) \quad (5)$$
$$L_{i=}\sum_{m=0}^{k-1} x_{2i-m} \,.\, t_m(z) \quad (6)$$

where s_m (Z), $.\, t_m$(Z): wavelet filters, K: the length of the filter, and I =0... [N/2]-1.

In practice, such transformation will be applied recursively on the low-pass series until the desired number of iterations is reached[41]. The basic idea in the DWT for a one dimensional signal is the following. A signal is split into two parts, usually high frequencies and low frequencies. The edge components of the signal are largely due to the high frequency part. The low frequency part is split again into two parts of high and low frequencies. This process is continued an arbitrary number of times, which is usually determined by the application at hand.

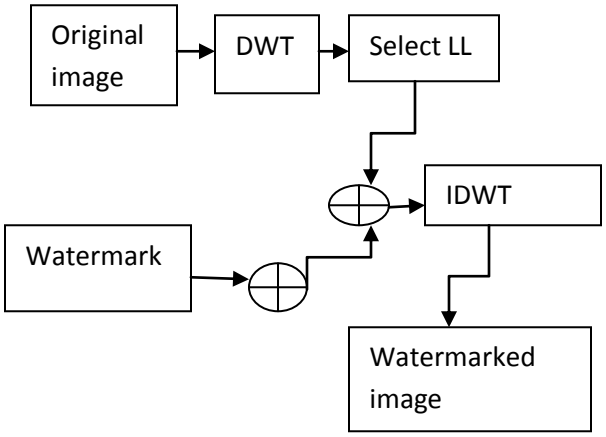

Fig.5. WatermarkEmbedding using DWT

A step of wavelet transform decomposes an image into four parts: HH, HL, LH and LL as shown in figure 5. LL is low frequency coefficient, LH is high frequency coefficient horizontally, HL is high frequency coefficient vertically, and HH is high frequency coefficient diagonally. Watermark should be embedded in low frequency coefficients[42].

IV. PERFORMANCE EVALUATION

4.1 Measuring Imperceptibility

Imperceptibility of an embedded watermark can be expressed either as fidelity or quality measure. Fidelity expresses as a measure of similarity between the original and watermarked cover.

The widely used peak signal-to-noise ratio (PSNR) measurement [47] which measures the maximum signal to noise ratio found on an image is used as an objective measure for the distortions introduced by the watermarking system. The PSNR is given by [47,48]:

$$PSNR\left(I_{ORG,}I_W\right) = \left(\frac{255^2}{MSE\,(I_{ORG\,},I_w)}\right) \quad (7)$$

where MSE is mean square error between the original image $I_{ORG,}$ and the watermarked one I_W. The MSE is defined as :

$$MSE\left(I_{org}\,,I_W\right) = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(I_{org}\,(i,j) - I_w(i,j))^2 \quad (8)$$

where, M and N are the image dimensions. When SNR approaches infinity, the original image and output image are totally the same. SNR provides only a rough approximation of the quality of the watermark as it does not take into account, the Human Visual System (HVS). The evaluation relies strictly on the observations under varied conditions.

4.2Measuring Robustness

Common signal processing attacks are applied to the watermarked images to measure and compare the robustness of the three techniques. The Bit-correct ratio (BCR) for the extracted logo after every attack is measured. The use of the bit-correct ratio (BCR) has become common recently, as it allows for a more detailed scale of values. The bit correct ratio (BCR) is defined as the ratio of correctly extracted bits to the total number of embedded bits and can be expressed using the formula.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 will report on robustness results which we obtained for three digital signal processing attacks such as resizing, cropping and rotation.

$$\text{BCR}=\frac{100}{l}\sum_{n=0}^{l-1} \quad \begin{cases} 1, \\ 0, \quad W'_n \neq W_n \end{cases} W'_n = \quad (9)$$

where, l is the watermark length, W_n corresponds to the nth bit of the embedded watermark and W'_n corresponds to the nth bit of the recovered watermark

In experiments [44,45], firstly 256×256 and 537×358 standard test images are used (cameraman.tif,

moon.tif).According to DCT technique, we can calculate PSNR MSE at different values of alpha.In Table IV,1) In Cameraman image(256×256),whenAlpha = 0.01, thenPSNR = 34.78, 2) In Moon image(537×358),whenAlpha = 0.01,thenPSNR = 40.54. Different values of alpha are taken, for examples, 0.01, 0.1, 0.2, 0.5, 1, and 2. So, it is found that when the size of image is increased at the same value of alpha, PSNR value of large image is better than smaller image. So, PSNR value is increased by means of image quality increase without decreasing alpha factor [46].

Table IV. Cameraman and Moon Image with different values of alpha and PSNR

CAMERAMAN IMAGE SIZE(256× 256)	**MOON IMAGE SIZE (537×358)**
1) $\alpha = 0.01, PSNR = 34.78$	1)$\alpha = 0.01, PSNR = 40.54$
2) $\alpha = 0.1, PSNR = 14.78$	2)$\alpha = 0.1, PSNR = 20.54$
3) $\alpha = 0.2, PSNR = 8.76$	3)$\alpha = 0.2, PSNR = 14.52$
4)$\alpha = 0.5\ , PSNR = .80$	4)$\alpha = 0.5, PSNR = 6.5$
5)$\alpha = 1, PSNR = -5.2$	5) $\alpha = 1, PSNR = 0.54$
6) $\alpha = 2, PSNR = -11.2$	6) $\alpha = 2, PSNR = -5.47$

V**.**Advantages of DWT over DCT

According to[24] and [25], there is the DWT advantage over DCT as:
1. It is not necessary to divide the input coding into non-overlapping 2-D blocks, it has higher compression ratios and eliminates the blocking artifacts.
2. It allows good localization both in time and spatial frequency domain.
3. The transformation of the whole image introduces inherent scaling
4. Better identification of which data is relevant to human perception higher compression ratio.

VI**.**Advantages of DCT over DWT

1. It always depends on the application , but in general, DCT provides a simple and efficient implementation with real components (instead of complex ones coming out from DFT).
2. Moreover, DCT concentrates on the energy in the lower coefficients.
3. DWT is more difficult to handle since the direct outcome is not just a set of coefficientsfor image compression as in JPEG 2000,
4. DWT provides a great quality and Multi resolution properties since it is not based on MacroBlocs.

VII.CONCLUSIONS

In this paper, we have presented various features for digital watermarking like overview, framework, techniques, applications, challenges and limitations. Besides, a brief and comparative analysis of DWT and DCT watermarking techniques is presented with their advantages and disadvantages which can help the new and budding researchers in related areas. We also tried to classify the digital watermarking in all the known features like robustness, host signal, perceptivity, purpose, watermark type, domain, detection process and use of keys.From all the results derived,it can be concluded that proposed methodologies are much efficient in terms of PSNR value. When DCT and DWT methods are used separately, they have some advantages and disadvantages.

REFERENCES

[1]R.G. Schyndel, A. Tirkel, and C.F Osborne, ―A Digital Watermark‖, Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.
[2]Christine I. Podilchuk, Edward J. Delp, ―Digital watermarking: Algorithms and applications‖, IEEE Signal processing Magazine, July 2001.
[3].Lie W-N, Chang L-C (2006) Robust and high quality time-domain audio watermarking based on lowfrequencyamplitude modification. IEEE Trans Multimedia 8(1):46–59
[4]NagarajV.Dharwadkar& B. B. Amberker International Journal of Image Processing Volume (4): Issue (2) 89 Determining the Efficient Subband Coefficients of Biorthogonal Wavelet for Gray level Image WatermarkingInternational Journal of Image Processing Volume (4): Issue (2)
[5]Chu, W, 2003. "DCT-Based Image Watermarking Using Subsampling," IEEE Trans. Multimedia, 5(1):34-38.Lin, S. and C. Chin, 2000. "A Robust DCT-based Watermarking for Copyright Protection," IEEE Trans. Consumer Electronics, 46(3): 415-421.
[6]Deng, F. and B. Wang, 2003. "A novel technique for robust image watermarking in the DCT domain," in Proc. of the IEEE 2003 Int. Conf. on Neural Networks and Signal Processing, vol. 2, pp: 1525-1528.
[7]Wu, C. and W. Hsieh, 2000. "Digital watermarking using zero tree of DCT," IEEE Trans. Consumer Electronics , vol. 46, no.1, pp: 87-94.
[8]Digital Image Steganography:Survey and Analysis of Current Methods Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc
[9]Kevitt Zhang Guangnan, Wang Shushun. A Blind Watermarking Algorithm Based on DWT for Color Image.
[10]Kim, Y., Kwon, O., Park, R.: Wavelet Based Watermarking Method for Digital Images Using the Human Visual System. In: IEEE International Symposium on Circuits and Systems, vol. 4, pp. 80–83 (July 1999)
[11]Nikolaidis, A., Pitas, I.: Asymptotically Optimal Detection for Additive Watermarking in the DCT and DWT Domains. IEEE Transactions on Image Processing 2(10), 563–571 (2003).[12]Jiang Xuehua, ―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on IntelligentComputation Technology and Automation.

[13]ChiragSharma,DeepakPrashar,“ T based robust technique of watermarkingappliedondigital Images”, International Journal ofSoft Computing and Engineering (IJSCE),Volume-2,Issue-2,May 2012
[14]Mahmoud El-Gayyari, ―Watermarking Techniques Spatial Domain Digital Rights Seminar ©I, Media Informatics University of Bonn Germany.
[15] Cox, Ingemar J., et al. "Secure spread spectrum watermarking for multimedia." *Image Processing, IEEE Transactions on* 6.12 (1997): 1673-1687.
[16]Kurah, C. AND Mchughes, J. 1992.A cautionary note on image downgrading.In Proceedings of the IEEE Computer Security Applications Conference.Vol. 2. IEEE Computer Society Press,Los Alamitos, CA,153–159..
[17]R. Schyndel, A. Tirkel, and C. Osborne, “A Digital Watermark,” Proc. IEEE Int.Conf. on Image Processing, Nov. 1994, vol. II, pp. 86-90.
[18]R.AARTHI, 2V.JAGANYA, &3 S.POONKUNTRAN “Modified LsbWatermarkingFor Image Authentication” International Journal of Computer &Communication Technology (IJCCT) ISSN (ONLINE): 2231 -0371 ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012.
[19]R. Schyndel, A. Tirkel, and C. Osborne, “A Digital Watermark,” Proc. IEEE Int.Conf. on Image Processing, Nov.
1994, vol. II, pp. 86-90.
[20]Hajjaji, Mohamed Ali, AbdellatifMtibaa, and El-BeyBourennane."A Watermarking of Medical Image: Method Based'LSB'."*International Journal of Computer Science Issues* (2011).
[21Puneet Kr Sharma and Rajni, “Analysis of Image Watermarking using Least Significant Bit Algorithm” International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012, pp. 95-101..
[22]Pal, Koushik, G. Ghosh, and M. Bhattacharya."A Novel Digital Image Watermarking Scheme for Data Security Using Bit Replacement and Majority Algorithm Technique."*InTech, Watermarking* 1 (2012).
[23]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) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), pp.36-41
[24]Mr. Abhay Sharma, Mrs. RekhaChaturvedi, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, *“ New Improved and Robust Watermarking Technique based on 3rdLSB substitution method*” International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 ISSN 2250-3153, pp. 1-4.
[25]Brigitte Jellinek, “Invisible Watermarking of Digital Images for Copyright Protection” University Salzburg, pp. 9 –17, Jan 2000.
[26] Xia,Xiang Gen ,Charles,GBoncelet,Gonazzalo R arce,A multi resolution watermark for Digital images IN proc.IEEE 1997 pp 548-551.
[27]MahaSharkas, Dahlia ElShafie, and NadderHamdy, Senior Member IEEE, “A Dual Digital-Image Watermarking Technique” World Academy of Science, Engineering and Technology 5 2005, pp. 136-139.
[28] Lee, Sunil, Chang Dong Yoo, and Ton Kalker. "Reversible image watermarking based on integer-to-integer wavelet transform." *Information Forensics and Security, IEEE Transactions on* 2.3 (2007): 321-330.
[29]P. Ramana Reddy, Munaga.V.N.K.Prasad, D. SreenivasaRao, “Robust Digital Watermarking of Color Images under Noise attacks”, International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009, pp.334-338.
[30] Preeti Gupta, “Cryptography based digital image watermarking algorithm to increasesecurity of watermark data”, International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518.
[31]DarshanaMistry, “Comparison of Digital Water Marking methods,” 21st Computer Science Seminar SA1-T1-7. IJCSE, Vol. 02, No. 09, ISSN : 0975-3397 , 2010, pp. 2905-2909
[32] Zhang, Yong, Bian Yang, and Xia-Mu Niu. "Reversible watermarking for relational database authentication."*Journal of Computers* 17.2 (2006): 59-66.
[33] HarpuneetKaur, “Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data” Computer Science & Engineering Department, Thapar Institute of Engineering & Technology. May 2006, pp. 1-69.
[34]Cox, Ingemar J., et al. "Secure spread spectrum watermarking for multimedia."*Image Processing, IEEE Transactions on* 6.12 (1997): 1673-1687.
[35] Mei Jiansheng1, Li Sukang1 and Tan Xiaomei” A Digital Watermarking Algorithm Based On DCT and DWT”,104-107, International Symposium on Web Information Systems and Applications (WISA’09) 2009.
[36] AlBaloshi,M.;Al-Mualla,M.E.; Etisalat Univ. Coll., Sharjah” A DCT-Based Watermarking Technique for Image Authentication” 754 – 760, International Journal 2007.
[37] Lin lue” A Survey of Digital Watermarking Technologies”, 1-12, WISA 2009.

[38] Mei Jiansheng1, Li Sukang1 and Tan Xiaomei” A Digital Watermarking Algorithm Based On DCT and DWT”,104-107, International Symposium on Web Information Systems and Applications (WISA’09) 2009 .
[39] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Transactions on Image Processing, 6(12), December 1997,pp.1673-1687.

[40] A. Piva, M. Barni, F. Bartolini, V. Cappellini, “DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image,” Proceedings of International Conference on Image Processing, Washington, DC, October 26 - 29, 1997, pp. 26-29.
[41]Ben Wang1, Jinkou Ding2, Qiaoyan Wen1, Xin Liao1, Cuixiang Liu,” An image watermarking algorithm based on DWT DCT AND SVD” 1034-1038,IEEE 2009.
[42] Munesh Chandra, ShikhaPandey” A DWT Domain Visible Watermarking Techniques for Digital Images”421-427,IEEE 2010.
[43] Kamran Hameed, AdeelMumtaz, and S.A.M. Gilani” Digital Image Watermarking in the Wavelet Transform Domain”83-86, World Academy of Science, Engineering and Technology 13 2006.
[44] www.advancecoursecode.com
[45]Www.codeforge.com/libs/highlight/stles/sunburst.css
[46] RIDZOŇ, R.; LEVICKÝ, D.: Usage of different color models in robust digital watermarking, 978-1-4244-3538-8/09/$25.00 ©2009 IEEE.
[47]Taha El Areef, Hamdy S. Heniedy, S .Elmougy, and Osama M. Ouda, “Performance Evaluation of Image Watermarking Techniques”, Third International Conference on Intelligent Computing and Information Systems, Faculty of Computer & Information Sciences, ICICIS 7002 ,March 15-18, 2007, Cairo.
[48] S. Voloshynovskiy, S. Pereira, T. Pun, University of GenevaJ.J. Eggers and J.K. Su, University of Erlangen-Nuremberg," Attacks on Digital Watermarks: Classification, E(1)stimation-based Attacks and Benchmarks ", 2001.

Raj Kumar Jaiswal B.Tech.,M.Tech.(Pondicherry university) Assistant Professor in ECE department from NRI IT Vijaywada A.P ,India. Research areas are Image processing ,Wireless Sensor Network, mobile ad hoc network & its enhancement.

S.Ravi, Asst. Professor, Dept. of Computer Science & Engineering at Pondicherry Central University Puducherry ,India . Having wide experience in the field of teaching. Research areas are Image Processing, its Enhancements, and His research work has been published in many national and international journals.