DIGITAL WATERMARKING: A SURVEY

SAMAPTIKA PANDA[1]
P.G. Dept. Of Computer Science and Application
Jyoti Vihar, Sambalpur University, Burla, Sambalpur,Odisha,India
[1]pandasama.panda@gmail.com

Y.KARALI[2]
P.G. Dept. Of Computer Science and Application
Jyoti Vihar, Sambalpur University, Burla, Sambalpur,Odisha,India
[2]yasobanta0706karali@gmail.com

Dr. C.S.PANDA[3]
P.G. Dept. Of Computer Science and Application
Jyoti Vihar, Sambalpur University, Burla, Sambalpur,Odisha,India
[3]dr.chandrasekharpanda@gmail.com

Abstract

This is the era of digital information as digital image plays a vital role in every field of human lives. A digital image is both informative and flexible since it is easy to edit and redistribute. The vulnerability of digital image increases along with its use. So the security and confidentiality need to be maintained. Digital watermarking is the technique that provides security to the digital image where a low energy signal (watermark) is embedded in the original signal (host) to make the host imperceptible. The host signal may be any form of digital multimedia data like image, audio or video. When the watermarking technique is performed on the host signal, it becomes free from unauthorised access and can only be detected or extracted as required by the authorised receiver.

Key word- Watermarking, DCT, DWT, Spread spectrum, LSB, Predictive, Patchwork, DFT, Robustness, Fidelity, Imperceptibility

1. INTRODUCTION

Digital data is a combination of different type of data like audio, video, image, text, graphics etc. Combination of all these data is known as multimedia data. To secure the multimedia data watermarking is used. Watermarking is the process of embedding an image with another image. When the process is carried out in digital image it is known as digital watermarking. A cover is created over the original image to secure the data. Cover image is also known as the host image that is embedded with a low frequency signal to produce the watermarked image. The watermarked data must be transmitted to the receiver in a secure channel to avoid the chances of attack. At the result it produces a digital image that is watermarked by a secure image. It is generally used for copyright protection, intellectual property right, broadcast monitoring, finger printing etc. A layman cannot distinguish between original image and the watermarked image if watermarking is done in invisible mode but if the watermarking is done in visible mode then any one can mark the change. So visible watermarking is less secured then the invisible watermarking. The embedded image may be binary or gray scale image, spread spectrum sequence, pseudo random binary sequence etc [1]

(a) Original image

(b) watermark image.

(c)Watermarked image

2. APPLICATIONS OF WATERMARKING

Recently multimedia data are in great use and distribution as it secure and flexible to distribute multimedia data. Digital multimedia data has more flexibility so there is more chance of unrestricted duplication and copyright material. To protect the data from unauthorised access several method are introduced as encryption, watermarking and digital signature etc. Encryption is the process of converting data to another form so that it prevents the unauthorised access of data in the transmission medium. (2) Decrypted data is same as original file as header that can be detected and deleted easily by recording files or changed by format conversion. The process of encryption and decryption is known as cryptography. Digital signature is a measure to authenticate an electronic document. On the other side watermark embedded a secret signal called watermark directly in to the original signal in such a way that both the signal are concatenated with each other always.

Digital watermarking has numerous application areas like copyright protection, broadcast monitoring fingerprinting, authentication and covet communication.[3]

All the application of watermarking is categorised in to 2 types depending on the security of the data

2.1 Secure applications

2.2 Non secure applications

2.1. Secure applications

Digital watermarking is also used for secure application that is the application dealing with the copy or copyright protection.

2.1.1 Copyright protection

Watermarking is used to protect the intellectual property right. Data owner can embedded via watermark represent copyright information in his data watermark prevent the unauthorised copy and distribution of content watermark is used to proved ownership of product in court.[4]

2.1.2. Information hiding.

Watermarking is also used to secure the information within the image. It is another important application of watermarking.

2.1.3. Fingerprinting

Finger printing is used to authenticate a user. It has a great use in the field of securing intellectual property right of owner helps to find out the unauthorised person who has broken their license agreement by supplying data to third party.

2.1.4 Broadcasting monitoring

To protect the broadcasting message in the network watermark is also used to protect the commercial product along with TV product, video, sound.

2.1.5. Covert communication.

Secret message can be embedded imperceptibly to the digital image or video to communicate information from sender to the intended receiver while maintaining low probability of intercept by other intended receiver.

2.1.5 Tamper detection/Authentication

If image is tamper than the authenticity is hampered that application is mostly used in photo forensic photo journalism where the integrity of data is to be maintained a watermark is used to describe work. Description of files must be unique and hard to obtain by attacker fragile watermark. Embedded to digital content indicate weather data is altered change in original image change the watermark signal.

2.2. Non secure application

Digital watermarking is also used for non secure application that is the application not dealing with the copy or copyright protection.

2.2.1. indexing

To secure indexing of video mail, news item, movies used by search engine watermark is used.

2.2.2 Medical application

Embedding data patent into detail images watermark is used. Insertion of name in the x-ray is a use of watermarking. Other application areas are data embedding, error detection, tamper proofing, and compression

3. PRACTICAL CHALLENGES OF WATERMARK

Watermark alone is not sufficient to secure the data along with the watermark technology. A secure protection protocol must be applied. A secure protection protocol is chosen for specific recruitment of data hiding algorithm .A good watermark protect the data is not destroyed or weakened by both malicious and non maliciously again it must authenticate the owner unambiguously. This property can be classified as fundamental and alternative. Fundamental recruitment include capacity, fidelity, imperceptibility and robustness, all the 3

component are interdependent increase in imperceptibility of the image causes lower the strength of watermark image embedding large amount of information reduce the imperceptivity of the image alternative requirement include performance that is the speed of embedding and detection of digital image.

4. WATERMARK ATTACK

4.1 INTRODUCTION TO WATERMARKING ATTACK

Attack is a destructive approach, in digital watermarking attack is done to hamper the original message or to the communication channel. To avoid attack on watermarked image algorithm are must be written in such a way that it is difficult to break the algorithm without proper key. Watermark algorithms are written to securely transmit the watermarked data over the communication medium from sender to the receiver. Watermark algorithm work in 3 steps

- Find out the weakness of previous watermarking algorithm
- Suggest for the improvement of algorithm
- Check the effects of applying new watermarking algorithm

4.2 TYPES OF ATTACK:

A simple attack destroys the original data through the process of compression. When noise is added or signal processing like sampling, quantization, decoding, encoding, compression decompression are the way to hamper the data.

4.2.1. Depending on intention of attacker attacks are of 2 types

a. Intentional—

Attacker is supposing to attack. Here the attacker is well known about the effect of attack. Attacker may attack to the watermarked image or to the channel through which watermarked data is supposed to be travelling.

b. Unintentional attack:--

Attacker is not suppose to attack ,when signal is under processing several steps are carried out like coding decoding, compression, decompression , cropping, geometric transform , noise, filtering, printing, scanning where the data is need to be compressed. Data is compressed means the important parts are kept secured and unimportant parts are discarded. Compression is done to keep the data in minimum memory space but during compression watermarked data may be treated as unimportant and discarded.

4.2.2 Depending on the watermarked image at the output end attack is categorised in to two types

a. Robustness attack

Robust watermarking should survive some common changes occur during image processing or other operation .After the modification the original image is not same as the extracted image and called as “attack” .It is not the targeted attack. When an image is attacked it remove some important data of the original image decreasing the visual quality of the image, after the attack it is difficult to detect the watermarked image.[5]

Some of the robustness attacks are

- Image degradation
  It is the process of removal of data from the image. Degradation or removal of data causes watermark to be undetectable. When the image is cropped or noise like Gaussian is inserted then part of the image is removed or if the row and column removal operation is done then partially image is removed along with the watermarked image so it is difficult to detect the watermarked image after it is cropped.
- Image enhancement-
  When an image is enhanced it is better than the original image for a particular application. It involves operation like convolution that desynchronizes the original image. It include operation like histogram equalization, histogram matching, contrast stretching, smoothing, median filtering, Gaussian filtering etc
- Image compression
  Compression is done to reduce memory space to store image. Compression is always associated with the method of decompression. Compression reduces the storage cost of an image. Compression may be lossy or lossless, if lossless compression method is used then watermark can be recovered by the decompression process as it is less destructive then the lossy mode. But if lossy compression is done then it is difficult to find the watermarked data as the data is already destructed.JPEG compression is one of the most common compression attacks in digital image.
- Image transformation
  It is more useful in the restoration of image .but it creates a great threat to the robustness of the image due to the resynchronization effect. Different types of transformation are applied to the digital image commonly used transformation is Rotation, Scaling and Translation commonly known as RST

transformation. It is included in the geometric transformation. Other transformations are aspect ratio change, shearing, reflection, projection etc.

b. Presentation attack-

The attacker main aim is to destroy the visual quality of image. For a digital image visual effect is a great factor introduction of any noise like salt and pepper or impulse can easily destroy the image quality. If a data is not represented properly then it becomes valueless.

4.2.3Depending on the basis of intent again attacks are of different type

a. Malicious-

Malicious attack is unrecoverable attack. The watermarked image is not recoverable after the attack. Common malicious attacks are printing, scanning, collusion, forgery, re watermarking etc. [6] It is again divided into two categories

- Blind attack-in blind attack the watermark is make undetectable without knowing about the watermarked algorithm
- Informed attack- it is opposite of blind attack, the watermark is made undetectable by using the specific algorithm that was used for watermarking the image

B .Non malicious –

If attack is the result of a normal operation then it is known as malicious attack. It is recoverable attack. Lossy compression is a type of non malicious attack where the compression of different type of data like audio, video, image is done to reduce the storage space and storage cost but it remove the important part of original data partially. Different types of non malicious attack are

- Geometric attack-
  Geometric attack involves basic geometric transformation in an image. It includes geometric changes like rotation, scaling, translation, cropping, row column blanking, warping etc. It is very much dangerous as it may cause the detection of watermark image become difficult or impossible.
- Signal processing—
  It is also called non geometric attack. Common signal processing attacks include sampling, quantisation, compression of image, addition of noise like (salt and pepper, impulse, periodic, Gaussian, gamma, exponential etc), filtering, brightness, sharpening, histogram etc.
- Protocol attack-
  It is a type of invertible attack [7] where the watermark is invertible means attacker subtracts his own watermark from watermarked data and claim as the owner of the watermarked data. This concept creates conflict on ownership of the watermarked image. To avoid such situation make the watermarked image veritable means it should not be possible to extract a watermark from non watermarked data.

4.2.4. Depending on the target attacks are

a. On the data-
   Here data is hampered. Attacker destroys the data of the watermarked image. In digital watermarking two images are embedded either original data or watermarked data. (8)If any one of the two data is hampered then the watermarked image is tempered.
b. On the system-
   If attacker attacks the system in which watermarking process is carried out then the watermarked data can easily attack. Attacker may also change the path in which watermark data is travelling so it is not reached at the proper receiver end.

Watermark attack

Depending on	Types of attack
Intention	Intentional, unintentional
Image quality at output	Robust, presentation
Intent	Malicious, non malicious
Target	Attack On data, attack on system

5. Removal of attack

To reduce the chances of attack on the digital image, it is necessary to remove the effect of noise in the image. The process of digital watermarking can be described as the original image known as the host image when passes through a low signal image it is known as the watermarked image then the embedded image is transfer through the communication channel and the receiver end the watermarked image is extracted to find the original image. Noise may disrupt the message in the communication channel so different counterfeit should be prepared to avoid the noise or attack in the process of digital watermarking.

To reduce the attacks on watermarked image some steps should be taken [9]

- Do not watermark the image again and again.
- Use watermark that is non invertible (code must be attach to host data).
- Watermarking should be done on the high frequency component of an image.
- The watermarking information should be overloaded on maximum number of pixel.
- The different types of attack should be forecasted so user will be aware of the attack.
- Only authenticated data should be watermarked.
- The key used for the process for encryption and decryption must be secure.
- Data should be properly checked before sending through the channel.
- Different types of filter must be used to find and remove the noise component in a digital image.

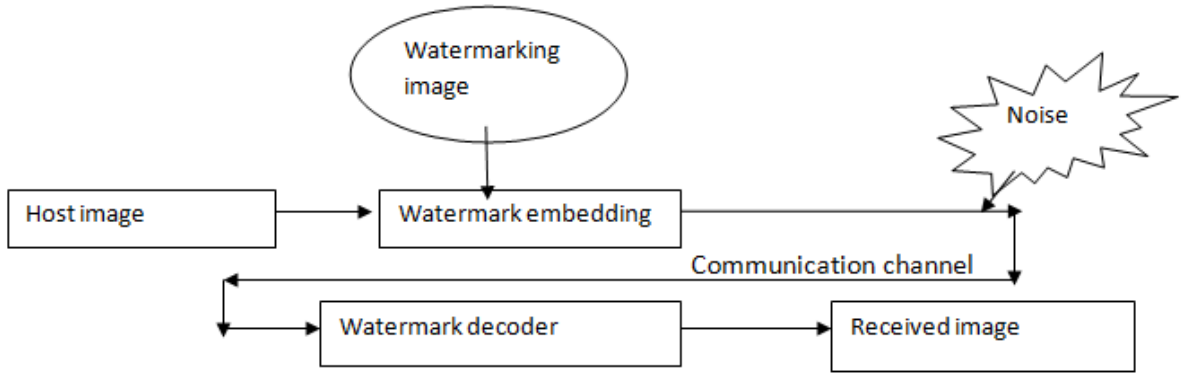

Fig: watermarking process with noise attack

The significance of a watermarking property in any particular application depends upon the requirement in particular application.[10]

A watermark image produces good quality result if their measure 3 qualities are satisfied the qualities are robustness, imperceptibility and fidelity. All the three qualities are dependable on one another.

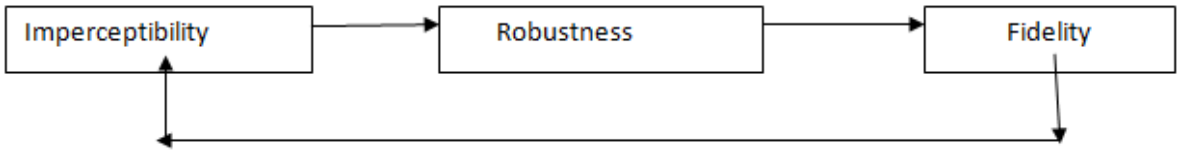

Fig: dependency between robustness, imperceptibility and fidelity

The 3 qualities are defined as

- Imperceptibility: process of hiding a watermark so that visual quality does not hamper. Imperceptibility can be archived if human cannot distinguish between watermark image and host image.(11)
- Robustness: a watermark is said to be robust if it survive after the signal processing operation.(12)
- Fidelity: Fidelity is the visual similarity between original image and watermarked image

6. Performance analysis

Performance of a watermark algorithm can be measured by checking the resistance to any type of attack. There is no metrics available to accurately measure the strength of a watermark algorithm. To check the performances check the imperceptibility, fidelity, robustness of the algorithm.

6.1Method to check imperceptibility

Imperceptibility means the superficial quality of the original image should not be distorted by the presence of watermark image. To check imperceptibility choose any one method

if f(x,y)-is original image

f’(x,y)-watermarked image

- **MSE**(mean square error)-
  It helps to find average of square of error. Square root of MSE is having common use as it makes an error metrics for numerical prediction. Larger the MSE value less similar watermark with original image.
  MSE is calculated as

$$MSE = 1/XY \sum_{i=0}^{x} \sum_{j=0}^{y} (f(x,y) - f'(x,y))^2$$

- **PSNR**(peak signal to noise ratio)-
  PSNR is calculated between original and watermarked image .larger PSNR more similar watermark with original image. PSNR is measured in DB.
  $PSNR_{db}=10/\log_{10}(max^2/MSE)$

6.2 **Method to check image fidelity**-

Fidelity is the visual similarity between original image and watermarked image. High fidelity is good for image watermarking.

6.3 **Method to check Robustness** --

Robustness analysis is quality measure for watermarked image; it is used to check reliability and readability of extracted watermarked image

- CRC(correlation coefficient)
  This metric is used to measure the compatibility between watermark and original image.

  Crc=

$$\sum_{i=0}^{n} \sum_{i=0}^{n} w(m,n)w'(m,n) / \sqrt{\sum_{i=0}^{n} \sum_{i=0}^{n} w(m,n)} \sqrt{\sum_{i=0}^{n} \sum_{i=0}^{n} w'(m,n)}$$

  Where w and w' are embedded and extracted watermark respectively.
- Bit rate error(BER)
  Used for binary sequence watermarked BER is defined as ratio between number of incorrectly decoded bit and length of binary sequence. For embedded and extracted watermark sequence of length B bits, the bit rate error become's

BER = Number of error bit / Total no of bit sent

Where w and w' are embedded and extracted watermark respectively.

- Accuracy ratio-(AR)

AR is calculated as similarity between original watermark and extracted watermark .AR is the ratio of no of correct bit between original watermark and extracted watermark. If AR=1 then original image is equal to the extracted image.

7. Study of different existing techniques of watermarking

Digital watermarking is developed at a high rate since mid 90's.In the early stage embedded message is treated as a noise in the communication process. At that time host data and embedded data are independent of each other hence known as blind watermarking later on the concept of fidelity and robustness introduced in digital watermarking where the host data is dependent on the embedded data and known as informed embedding. To improve the concept of fidelity and robustness spread spectrum is introduced.

Various watermarking system are categorised into to two types [13]

- Spatial domain
- Frequency domain

Watermarking in Spatial domain is done by just changing some of the bits of data in the image it does not change the data majorly here a subset of pixel is chosen and the watermarking is done where as in the frequency domain takes the advantage of human visual system. In the frequency domain firstly image is to be transferred in to the frequency domain either by DWT or DCT then only the watermarked image is embedded with it .by applying the watermarking in different domain and using different technology authors had found different result.

Technique used in watermarking

Watermarking domain	Technique used in watermarking
Spatial domain	LSB, patchwork technique, predictive coding
Frequency domain	DCT, spread spectrum , dwt, combination of DCT and DWT

7.1 LSB(Least Significant Bit)-

It is the earliest method of data hiding. It is very simple to carry out but the problem is that it cannot satisfy the basic of robustness. R.Van schyndal et al (1994) describe two techniques on LSB in the first method they replace the LSB with pseudo noise and in the second method they added the LSB with the pseudo noise. They generate a watermark using an m sequence generator the watermark was embedded to LSB of original image. Here cross correlation based detection was proposed however this was not robust to additive noise.[14] To repair image Kue.ming et al(2012)work on the watermarking based on image in painting Using image half toning technique.LSB is used to extract halftone information and reference image is achieved from inverse halftone. He implied it as a lossless technique and found excellent result. [15]

7.2 PATCH WORK

Blender statistical et al (1996) described the patchwork algorithm. Here n pair of random image pairs are chosen (a,b) and increase a by one to become more brighter and decrease b by one so it become more darker. Watermark is detected by comparing the sum of difference of a and b of n pair of point .it is simple and easy to implement this method is highly resistant to non geometric attack. But the major problem is Low bit embedding difficult to decode image.[16]

7.3PREDICTIVE

Based on the correlation between adjacent pixel matsui and tanaka[1999]proposed a predictive coding scheme here a set of pixel is chosen that is to be watermarked and alternate pixel are replaced by difference between adjacent pixel. This method can be improved by key adding a constant to all differences. Cipher key is used at the receiver end to retrieve the embedded watermark this is more robust to LSB.[17]

7.4 DCT (Discrete Cosine Transform)

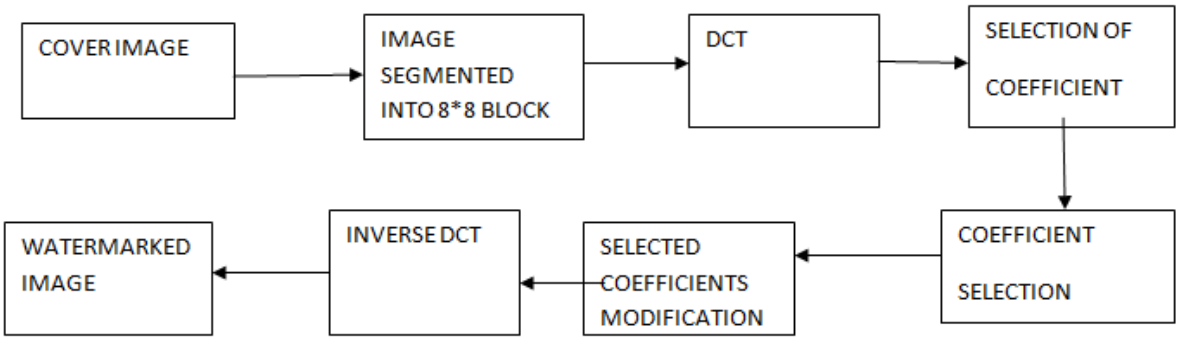

Fig: an example of DCT based watermarking

Heather wood et al takes an invisible digital watermark in spatial and DCT domain for colour image .They carry out operation in two step in first step embedded watermark directly into spatial domain while in second step convert it into DCT domain as they uses DCT domain original image is used for extraction process. Here result image is same as original that means a lossless technique. [18]

A watermarking scheme based on integer DCT for medical image is developed by Lin gao et al [2012]in integer DCT and difference expansion method. Image is firstly divided into some non overlapping expansion block after which the different expansion embedding and extracting algorithm used on the blocks whose energy is below threshold. And he found that DCT avoid distortion of truncation error lead to faster processing. Integer DCT can be easily implemented on hardware device.[19]

B kaur a kaur[2011]developed DCT based image hiding system in which image is segmented into 8*8 than each segment is again divided into8*8 and forwarded DCT is applied to each block. Concentrate on low frequency Energy compaction that is the major advantage of this method where image is divided into frequency band low and high, easy embedding of image high resistance to JPEG compression and noise. As compaction is done in block it suffered from visual artefact.[20]

7.5. DWT (Discrete Wavelet Transform)

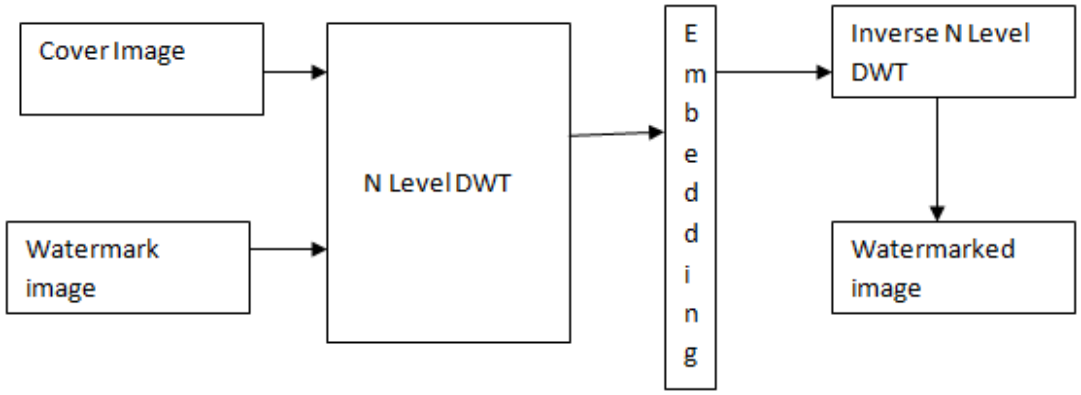

Fig: DWT based watermarking technique

Chirag shrarma et al [2012] works on the DWT based robust technique of watermarking applied on digital image and he found that it is useful for watermark extraction then LSB with more robustness. This method overcomes additive noise, filtering intensity adjustment, histogram equalization, JPEG compression, scaling and rotation.[21]

Xiao zou et al[2012]works on the geometric attack on the digital image watermarking on the wavelet domain. Here watermarking is done after decomposing the whole image into 3 level of DWT. watermark the image and then carry out other operation and he found that this method is robust against geometric attack.[22]

N.kaewkamnerd and k.r.RAo [2000] developed a wavelet transform based image adaptive watermarking scheme. Here although embedding is done in the higher level sub band but fidelity is hampered. To avoid perceptual degradation of image watermarking is done carefully.[23]

M.berni et al [2001] developed an improved wavelet Based watermarking through pixel wise masking. They carry out operation on HVS. Watermarking is added to largest detail band. The watermark weighing function is calculated as a simple product of data extracted from HVS. Watermark is detected by correlation between the pixels.[24]

Victor et al [2004] developed an algorithm based on adaptive image watermarking in high resolution sub band of DWT weighting function is the product expression of data extracted from HVS system.[25]

Bou chen and Hang shen [2009] developed a new robust fragile double image watermarking algorithm using improved pixel wise masking model and a new bit substitution based on pseudorandom sequence. This method embeds robust and fragile watermark into sensitive part and insensitive part of wavelet coefficient making 2 watermark non interfering.[26]

Peng liu and zhizhong ding[2009] proposed a blind image watermarking scheme based on wavelet tree quantisation. The largest two coefficients are selected as significant coefficient and difference between them is taken as significant difference. A watermark bit is embedded by comparing significant difference with average and maximum quantised value.[27]

By working on the DWT domain and adding Gaussian noise to the watermarking process then extracting the watermarked image with correlating with section of original image X.Xia et al[1997]found that this method is Robust to additive noise, resolution reduction, compression. But it is not robust for low frequency; it works only on middle and high frequency band.[28]

7.6 SPREAD SPECTRUM

I cox et al[1997] developed a spread spectrum based watermarking for multimedia and they found that non blind DCT spectrum Remove visual distortion, producing good result for robustness and fidelity of a image.[29]

7.7 DFT (Discrete Fourier Transform)

Fm Borland et al [2012] work on the DFT domain and embedded the watermark in phase information in DFT domain since the phase distortion is more sensitive to HVS so it is more robust to tempering than any other method. [30]

7.8 COMBINATION OF DCT AND DWT-

On working on the blind watermarking algorithm for copy right protection L feng Lzheng et al [2010] found that this is more robust and imperceptible as visual artefact due to DCT is reduced with high PSNR value. They embedded a binary image with a set of 3 level DWT transformed of a host image then DCT of each selected DWT sub band is computed and pseudo noise sequence of watermark bit are embedded with middle frequency coefficient of corresponding DCT block. Extraction procedure is same as embedding process used to extract

DCT middle band frequency of each sub band. Finally correlation between mid band coefficient and pseudo noise sequence is calculated to determine the watermark bit[31]. A comparative study on DWT and DCT done by Radhika V total and K.S.Bapat [2013] in the year 2013 found that DWT has significant advantages over DCT because of structural attack. DWT has significant advantages over geometric attack such as scaling, rotation, cropping etc. DWT is found as more robust to the attack then DCT with high imperceptibility.[32]

8. COMPARATIVE STUDY OF DIFFERENT EXISTING WATERMARKING TECHNIQUE

Method	Author	Title	Techniques	Conclusion	Year
Lsb	R.ven Schyndel, Tirkel, Osborne [23]	A digital watermark	Watermark using an m sequence generator the watermark is embedded to LSB of original image cross correlation based detection was proposed	Simple method, Not robust, not for complex image Not robust to additive noise.	1994
	Kue.ming[15]	watermarking based on image in painting Using image half toning technique	LSB is used to extract halftone information and reference image is achieved from inverse halftone..	He implied it as a lossless technique and found excellent result	2012
Patchwork	W. Bender[16]	Technique for data hiding	N pair of (a,b) chosen a-lighten b-darkens	Simple and easy high resistance to non geometric attack Low bit embedding Difficult to decode image	1996
Predictive	Matsui ,Tanaka [17]	Multimedia watermarking technique	Correlation between pixel was exploited and a set of watermarked pixel is chosen and alternate pixel are replaced with the differentiate between pixel	Robust technology Require a cipher text	1999
DCT	B kaur ,A kaur[20]	Steganographic approach for hiding image in DCT	Image is segmented into 8*8 than each segment is again divided into8*8 Concentrate on low frequency Energy compaction	Easy embedding of image high resistance to JPEG compression and noise Suffered from visual artefact	2011
	Heather wood [18]	invisible digital watermark in spatial and DCT domain for colour image	Carry out operation in two step in first step embedded watermark directly into spatial domain while in second step convert it into DCT domain as he uses DCT domain original image is used for extraction process..	Here result image is same as original that means a lossless technique	2011
	Lin gao[19]	A watermarking scheme based on integer DCT for medical image	Image is firstly divided into some non overlapping expansion block after which the different expansion embedding and extracting algorithm used on the blocks whose energy is below threshold.	He found that DCT avoid distortion of truncation error lead to faster processing. Integer DCT can be easily implemented on hardware device.	2012
DWT	X xia[28]	Multiresolution watermark for digital image	Watermark was inserted into middle and high frequency of the original image.	Robust to additive noise, resolution reduction, compression. Not robust for low frequency	1997
	Chirag Shrarma [21]	DWT based robust technique of watermarking applied on digital images	Multimedia image is divided into low and high order bit again low order bit are divided into two part and high order bit are divided in to two part.	Useful then LSB It has robust technology than any other DWT method.	2012

	N.kaewkamnerd K.r.Rao [23]	wavelet transform based image adaptive watermarking scheme	Watermark is embedded in higher level sub band	Avoid perceptual degradation Fidelity of image is hampered	2000
	M.Barni ,Bartolini f,P.Iva [24]	An improved wavelet Based watermarking through pixel wise masking	Operation is carried out on HVS. Watermarking is added to largest detail band. The watermark weighing function is calculated as a simple product of data extracted from HVS. Watermark is detected by correlation	Less robust to blurring Watermark is embedded on high frequency band so it is more robust.	2001
	Vitor.v, Guznan, Meana [25]	Analysis of a wavelet based watermarking algorithm	An algorithm based on adaptive image watermarking in high resolution sub band of dwt weighting function is the product expression of data extracted from HVS system.	Image fidelity is not secured. It is helpful for securing imperceptibility of image.	2004
	Xiao zou [22]	Geometric attack on the digital image watermarking on the wavelet domain	Here watermarking is done after decomposing the whole image into 3 level of DWT. watermark the image and then carry out other operation.	He found that this method is robust against geometric attack.	2012
	Peng liu Zhizhong Ding [26]	A blind image watermarking scheme based on wavelet tree quantisation	The largest two coefficients are selected as significant coefficient and difference between them is taken as significant difference.	A watermark bit is embedded by comparing significant difference with average and maximum quantised value	2009
	Bou chen ,Hang shen[27]	A new robust fragile double image watermarking algorithm	Algorithm using improved pixel wise masking model and a new bit substitution based on pseudorandom sequence.	This method embeds robust and fragile watermark into sensitive part and insensitive part of wavelet coefficient making 2 watermark non interfering	2009
Spread spectrum	I.Cox [29]	Secure spread spectrum watermarking for multimedia	Non blind DCT spectrum Remove visual distortion	good for robustness and fidelity of a image.	1997
DFT	Fm Borland[30]	Survey of watermarking algorithms for medical images	Embedded the watermark in phase information in DFT domain since the phase distortion is more sensitive to HVS	it is more robust to tempering then magnitude distortion More robust	2012
Combination of DCT and DWT	L feng , Lzheng[31]	A DWT and DCT based blind watermarking algorithm for copy right protection	a binary image embedded with a set of 3 level DWT transformed of a host image then DCT of each selected DWT sub band is computed and pseudo noise sequence of watermark bit are embedded with middle frequency coefficient of corresponding DCT block	more robust and imperceptible as visual artefact due to DCT is reduced with high PSNR value	2010
	Radhika V total K.S.Bapat[32]	A comparative analysis of watermarking in digital image using DWT and DCT	DWT has significant advantages over DCT because of structural attack. DWT has significant advantages over geometric attack such as scaling, rotation, cropping etc	DWT is found as more robust to the attack then DCT with high imperceptibility	2013

A review on the result obtain from the analysis—

Techniques	Attack	Robustness
LSB	Blurring	Low
	Scaling to half size	Low
	Resize of scaled image	Low
	Cropping	Low
DCT	Blurring	Medium
	Scaling to half size	Medium
	Resize of scaled image	High
	Cropping	Low
DWT	Blurring	Medium
	Scaling to half size	Medium
	Resize of scaled image	Medium
	Cropping	Low
Combination of DCT and DWT	Blurring	High
	Scaling to half size	High
	Resize of scaled image	Medium
	Cropping	Medium

9. CONCLUSION

Now a day's watermarking is a rapidly growing area it focus on the image fidelity, robustness and imperceptibility of image .There are several technique are developed to watermark an image. Each technique has its own advantages and disadvantages. Here I have studied several techniques to watermark an image, from the above study DWT is found as a good method for watermarking. Spatial method is fast and require low resource, high performance over scaling and additive noise spatial method include technique like LSB, Patch work , Predictive where LSB is more workable. Frequency domain is more complex then spatial domain but heaving more no of advantages. DCT is one of the frequency domain technique which is highly resistant to JPEG compression but create some visual artefact, while DWT is more preferred DWT is more robust against intentional or unintentional removal again watermark image require good fidelity DWT gives a good platform for watermarking as it restore image fidelity, imperceptibility and robustness of image.

10. REFERENCE

[1] Vaishali Jabade etel" literature review on wavelet based digital image watermarking" ijca(0975 – 8887) vol -31 no-1 2011
[2] G.J.Simmons, "The History of Subliminal Channels", IEEE Jou. On selected areas in Communications, Vol.16, No.4, pp.452-462 , May1998.
[3] Hitesh Agrawal "improved digital watermarking scheme using DCT and neural technology" BTech, NIT Rourkela 2007
[4] Vidyasagar et al "a survey of digital image watermarking techniques" 3rd IEEE International conference on industrial informatics,2005,pp 709-713
[5] Chaw seng woo et el"Digital Image watermarking for copyright protection and authentication " phd paper , Queensland University of Technology 2007
[6] T.Mita Kumari"image adaptive watermarking using wavelet transform",Mtech,NIT,Rourkela 2007
[7] Craver, S., Memon, N., Yeo, B.-L., and Yeung, M.M., "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications." IEEEJournal On Selected Areas in Communications. Vol. 16, No. 4, (May 1998): pp. 573-586.
[8] Alekha mohanty"study and implementation of watermarking algorithms", Mtech,NIT,Rourkela 2006
[9] Martin Dietze" second generation image watermarking in the wavelet domain"Ph.d,School of Sciences in the University of Buckingham,29 March 2005
[10] Barun pandhwal,D.S.Choudhari"an overview of digital watermarking techniques"IJSCE, vol-3, issue-1, mar 2013 pp-416-420
[11] Mitchell D.Swanson et all, "Multimedia data embedding and Watermarking technologies " Proceedings of the IEEE, Vol 86(6) pp. 1064-1087, June 1998
[12] Mitra Abbasfard" Digital Image Watermarking Robustness: A Comparative Study"2009 Computer Engineering,http://ce.et.tudelft.nl/,2009
[13] C.linand ,Y.ching "A robust image hiding method using wavelet technique" journal of information science and engineering vol 22 2006 pp 163-174
[14] R.van schyndel,A.tirkel and C.osborne "A digital watermark "proc ieee international conformance image processing vol 2 1994 pp 86-90
[15] Kue.ming etel " Watermarking based on image in painting Using image half toning technique" IJASC VOL15,NO1,PP 79-88 2012
[16] W Bender D.Gruhel, N. Morimoto,A.lu "Techniques for data hiding " Ibm system journal vol 35 nos 3,4,1996 pp313-336
[17] Matsui et al " Multimedia watermarking technique"proc IEEE vol 87 1999 pp-1079-1107
[18] Heather wood "Invisible digital watermark in spatial and DCT domain for colour image" Adam state college, Alamosa, Colorado.

[19] Lin gao et al" A watermarking scheme based on integer DCT for medical image is developed by" wavelet analysis and pattern reorganisation Icwapr2012 international conference2012 pp 33-37
[20] B.kaur et al "Steganographic approach for hiding image in dct domain "international journal of advances in engineering and technology,vol 1issue 3 2011 pp72-78
[21] Chirag shrarma et al "DWT based robust technique of watermarking" ijsce vol-2 issue-2 2012 issn-2231-2301
[22] Xiao zou et al " Digital image watermarking algorithm resistant to geometric watermarking attack on the wavelet domain" JICS 2012 issn-3391-3399
[23] N.kaewkamnerd and k.r.RAo" wavelet based image adaptive watermarking scheme" IEEE Electronic letters vol 36 feb 2000 pp-312-313
[24] M.barni et al" An improved wavelet Based watermarking through pixel wise masking"IEEE transctionson image processing volume 10,2001,pp 783-791
[25] Vitor V, Guznan, Meana "Analysis of a wavelet based watermarking algorithm"IEEE preceding of the internationalconference on electronics,communication and computer vol 36,2004 pp 283-287
[26] Bou chen and Hang shen " A new roubust fragile double image watermarking algorithem"IEEE international conference on multimedia and ubiquitous engineering,2009 pp 153-157
[27] Peng liu and zhizhong ding"A blind image watermarking scheme based on wavelet tree quantisation"second IEEE international symposium on electronic commerce and security 2009 pp218-222
[28] X xia et al " Multiresolution watermark for digital image" IEEE proceeding international conference image processing vol.1 1997 pp 548-551
[29] I cox et al "Secure spread spectrum watermarking for multimedia" IEEE trans image processing vol 6 1997 pp1673-1687
[30] F.M. Borland "Survey of watermarking algorithms for medical images"ijett vol-3 issue3 2012
[31] L Feng L.Zheng et al" A DWT and DCT based blind watermarking algorithm for copy right protection" proceding of IEEE international conference computer science and information tech vol 7,2010 pp 455-458
[32] Radhika V total and K.S.Bapat" A comparative analysis of watermarking in digital image using DWT and DCT" ijsrp ,vol 3,issue2 ,2013 issn 2250-3153
[33] Meenu singh et al"Digital Image Watermarking Techniques: A Servey"IJCST vol-4,issue-6,june 2013,pp51-55
[34] Farhad Saeed" a blind watermarking algorithm based On dct-dwt and arnold transform" ijsce, ISSN : 2319-7323 Vol. 2 No.06 Nov 2013
[35] D.G. Rindhe" A Review Of Digital Watermarking" IJAIEM,vol-2,issue 5,may 2013