Digital Watermarking Applications, Parameter Measures and Techniques

Namita Tiwari[1†] and Sharmila[2††],
Maulana Azad National institute of Technology (MANIT)
Bhopal, India

Summary
Nowadays Digital watermarking is important for the protection against illegal redistribution of digital data as of high popularity and accessibility over the internet. Digital watermarking is used to protect digital data in the form of images, audio, and video. Digital image watermarking is the technique in which watermark is inserted in the form of images that contains some hidden information and then it detects and extracts that hidden information. Some important requirements for the watermarking scheme are robustness, copyright protection, fidelity and many more so that they can handle several types of image processing attacks. This paper includes classification of digital watermarking techniques, application, parameter measures and attacks on digital watermarking. It also includes performance evaluation of techniques on the bases of performance parameters like PSNR values and MSE values.

Key words:
Digital Watermarking, Spatial Domain, Frequency domain, LSB, DCT, DWT, DFT, DHT.

1. Introduction to Digital Watermarking

The fast development of the web within the past few years has rapidly increased the supply of digital knowledge like audio, images, text and videos to the public. Thus, the problem of protective transmission of data becomes necessary. So, the solution of this downside is Digital Watermarking, which is the most typical and presumably the strongest technique for shielding digital knowledge. The word 'digital watermarking' was first given by 'Tirkel' in 1993, who gives two watermarking techniques to hide the watermark data in the images [1]. Digital watermarking is the technique in which data is hidden or embedded into the digital signal and this embedded information can be image, audio, video or text. The embedded information is called as watermark and the watermark can be extracted as well as detected. A watermark can be a pattern or a digital signal which is embedded into a cover object. Normally the data hidden can be copyrights, ownership, trademarks, logos, and the legitimate receiver [2,3].

Digital watermarking is necessary because of the following issues:

- Prove authenticity of an image
- Copyright notices
- To avoid forgery
- Security purpose
- Protect form illegal redistribution of digital media

This paper includes some digital image watermarking techniques in the spatial domain and in the frequency domain with their comparison, advantages and disadvantages.
This review paper organized in following sections:
Section 2: Working principle of watermarking
Section 3: Characteristic of digital watermarking
Section 4: Application of digital watermarking
Section 5: Parameter used in image watermarking
Section 6: Classification of digital watermarking technique
Section 7: Attacks on digital watermarking
Section 8: Comparison between Spatial domain and Transform domain and result analysis of different techniques
Section 9: Conclusion

2. Working Principal of Digital Watermarking

Watermarking system mainly consist of two modules;

- Watermark embedding
- Watermark extraction

Watermark embedding and extraction process has a cryptographic key which could be either a public key or a secret key. The key is used for security reasons, which prevent it from unauthorized parties [4]. Cover object is the original image to be watermarked. Watermark is another image use for watermarking on the cover image. Watermarked data is an output data which is obtain by superimposing of original image and watermark image.
Embedding process of watermark image is shown in fig. 1.

Manuscript received March 5, 2017
Manuscript revised March 20, 2017

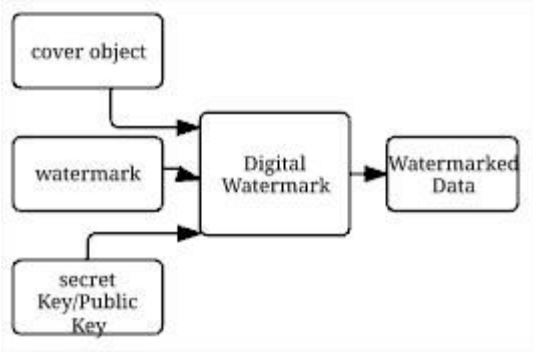


Fig. 1 Digital watermarking: Embedding process

Watermark, cover object and secret key or public key are given as the input to watermark embedding process. Either a text or an image can be used as a watermark object. The output data received is the extracted watermark data.
Extraction process of digital image watermarking is shown in Fig. 2.

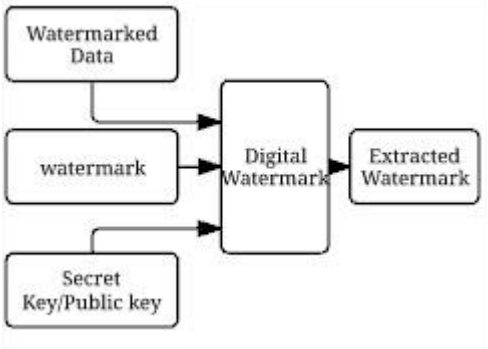


Fig. 2 Digital Watermarking: Extraction process

For extraction process Watermark or the original data, the Watermarked data and the secret key or the pubic key are the input data. The output is recovered watermark.

3. Characteristics of Digital Watermarking

Digital watermarking system has following properties.

3.1 Robustness: Robustness means the watermark embedded in a data can survive under various attacks and processing operations like rotation, scaling, compression etc. It should be robust against different geometrical and non-geometrical attacks.

3.2 Non-perceptibility: Watermark object can neither be seen by a human eye nor be caught by a human ear, it can only be find out through special processing or dedicated circuits. The watermark should be processed in such a way that it does not affect the quality of embedded data.

3.3 Security: Only the authorized users can detect, extract and modify the watermark and thus an owner can achieve the purpose of copyright protection.

3.4 Payload capacity: The payload capacity of watermark describes maximum amount of data that can be embedded as a watermark into a digital media. The size of the embedded information is often important as many systems require a big payload to be embedded. As a big payload also provide a security to a digital media.

3.5 Verifiability: The watermark should be embedded in such a way that it able to give the full and reliable proof of the ownership of copyright protected information products. It can be used for protecting data from illegal distribution as the data is being protected by the watermark. It is also used for identifying the authenticity.

3.6 Fidelity: When we add a watermark into an image there is a large possibility that it will affect the quality of original image. We must keep this property of the image's quality to a minimum, so that the fidelity of an image should be maintained.

4. Applications of Digital Watermarking

Watermarking system can be used in different areas and some of the application of digital watermarking are:

4.1 Broadcast Monitoring: The Broadcast monitoring system can protect commercial advertisements and valuable TV products. This application of digital watermark identifies that when and where works are broadcasted by identifying watermark embedded in these works. There are different technologies which can monitor playback of sound recorded during transmission. The digital watermarking is an alternative to these technologies due to its reliable automation detection.

4.2 Data Hiding: In digital watermarking data hiding is one of the most common application. Data hiding is the method in which data is sent secretly in such a way that no unauthorized person can detect it.

4.3 Proof of Ownership: To prevent the unauthorized modification of data, the authorized person identification is watermarked into the original data.

4.4 Data Authentication: The image can be easily meddled without even being detected. The Watermark like text, signature, and set of words can be embedded into the image to avoid this temper and to maintain the originality. Meddling of image can easily be identified now, as the pixel value of the embedded data would change and does not match with the original pixel values. And if the image

is being copied then it will lose its authenticity as the embedded data would not be copied along with that copied image. One of the solution of content authentication is digital signature technology [5].

4.5 Medical Application: Using the technique of visible digital watermarking name and details of the patients can be printed on the X-ray and Magnetic Resonance and imaging (MRI) scans reports [6]. The medical reports play a vital role in the treatment of the patient. If the reports of different patients are mixed, then the wrong diagnosis of a disease for a patient based on unidentified report may lead to an inimical treatment. Therefore, embedding of date and patient name in a medical report could decrease the possibility of maltreatment and increases the patient confidentiality and security.

4.6 Fingerprinting: A fingerprinting technique is used to identify the origin of illegal copy. In this every copy is watermarked with a unique serial numbers or unique sequence of bits.

4.7 Copy and Playback Control: Watermarks for monitoring, identification and proof of ownership do not fend illegal copying. But sometimes it serves as a powerful investigation tool. Despite, it is possible for playback devices to react to embedded signals. So, if the owner wants to develop such a system in which the duplication recording is prohibited then manufactured recorder must include watermark detection circuitry. Such systems are being currently developed for DVD video.

4.8 Owner Identification: The owner identification of an item is somewhere written on the cover of an object. For example, identification mark of the paper manufacturer on the top corner of the paper. These types of the watermark can be easily removed from the paper by cropping the image or by tearing the paper. So, to overcome from this problem digital watermarking is used. It embeds the watermark in the form of bits and forming an integral part of the content.

4.9 Locating Content Online: Nowadays contents are uploaded in a large volume on the internet for information sharing, research and communication purpose. It also has become a largest platform for sales. Also, the identification of the owner becomes very important and that will be possible with the help of watermarking.

4.10 Media Forensics: Forensic watermark is the technique which enhance the ability of owner to detect and respond to misuse of its assets. Media Forensic watermark is used not only to collect the evidence for criminal, but also to enforce the contractual usage agreement between the owner and the people with which it shares its content.

4.11 Copyright Protection: For the protection of prominent data, the data owner can embed the watermark in the data. There has always been a problem in providing the identity of the owner of an object. And if there's a dispute regarding the ownership of data then the identity of the owner can be easily extracted from the watermark.

4.12 Digital Rights Management (DRM): Digital Rights Management is a technique which is defined as the description, identification, trading, protection, monitoring and tracking of all forms of usages over tangible and intangible assets.

5. Parameters Used in Image Watermarking

To calculate the quality performance of watermarked image, some of the parameters used in image watermarking are:

5.1 Peak Signal to Noise Ratio (PSNR): PSNR is used to find out the degradation in the hidden image with respect to the original image. It is calculated in eq. (1)

$$PSNR = 10\, log_{10}[P^2 / MSE] \quad (1)$$

Where P is the peak signal value. P is equal to 255 for images having channel depth of 8-bit.

5.2 Signal to Noise Ratio (SNR): It measures the signal strength with respect to the background noise. Eq. (2) shows the SNR value calculation.

$$SNR = 10\, log_{10}(S / N) \quad (2)$$

Where

$S = signal\ strength\ and$

$N = background\ noise$

5.3 Mean Square Error (MSE): Mean Square error between original image and distorted image is calculated as eq. (3).

$$MSE = \frac{1}{ab}\sum_{x=1}^{a}\sum_{y=1}^{b}[c(x,y) - e(x,y)]^2 \quad (3)$$

Where, a and b are height of the original image and distorted image, respectively. $c(x,y)$ is the pixel value of cover image and $e(x,y)$ is the pixel value of embedded image.

5.4 Bit Error Ratio (BER): Bit Error ratio is the ratio of the number of bits modified or changed (C) after applying watermarking to the total number of original bits in the image $(H * w)$. Hence, it is calculated as eq. (4):

$$BER = \frac{C}{H*w} \quad (4)$$

Where C is the number of error bits.

H is height of watermarked image and w is the width of watermarked image.

5.5 Normalized Correlation (NC): Normalized correlation measures the similarity between the original watermark image and the watermark extracted from the attacked image. Where $w(x,y)$ is the pixel value of cover image and $w'(x,y)$ is the pixel value of embedded image. NC value is calculated as eq. (5).

$$NC = \frac{\sum_{x=1}^{N}\sum_{y=1}^{M} w(x,y)*w'(x,y)}{\sum_{x=1}^{N}\sum_{y=1}^{M} w^2(x,y)} \quad (5)$$

6. Classification of Digital Watermarking Technique

There are several criteria based on which Watermarking techniques are classified.

Fig. 3. Shows the classification of watermarking technique.

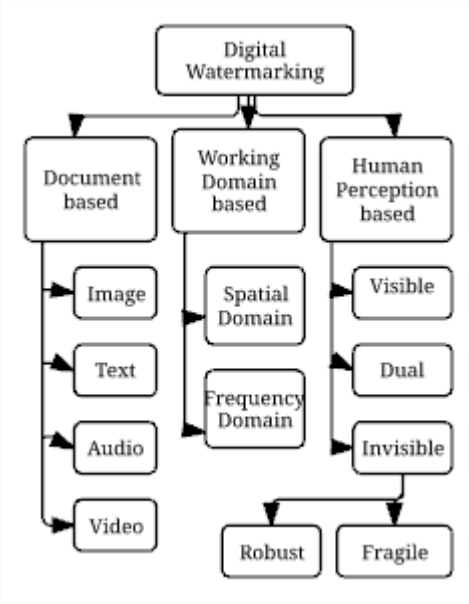


Fig. 3 Classification of Digital watermarking techniques

6.1 According to document:

6.1.1 Image Watermarking: Image watermarking technique is used to hide the data in an image and to detect and extract the data for the author's ownership.

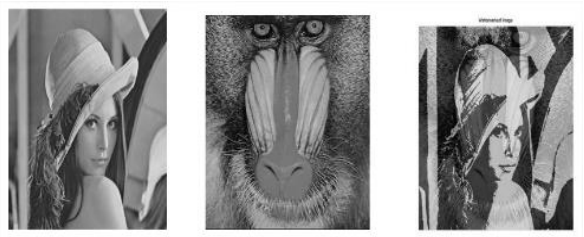
6.1.2 Text Watermarking: Text watermarking technique adds the watermark in text files like pdf and doc to prevent the changes made in text. The watermark is embedded in font shape.

6.1.3 Audio Watermarking: These techniques add watermark in audio stream to control audio applications. Nowadays, copyright issues are very common for audio data. So, to prevent the ownership of audio data watermarking is necessary.

6.1.4 Video Watermarking: Video watermarking technique add watermark in video stream to control the video application. This is the extension of image watermarking.

6.2 According to human perception:

6.2.1 Visible Watermarking: Visible Watermarking is the most primitive way of watermarking. Visible watermark is the technique in which watermark is embedded in a visual content in such a way that they are visible when the content is viewed. Visible image watermarking of Lena image is shown in fig. 4.



Original image | Watermark image | Watermarked Image

Fig. 4 Visible Watermarking

6.2.2 Invisible Watermarking: Visible watermarking is the technique in which, secret information is hidden into an audio files, video files and in images but it cannot be observed. The watermark cannot be seen but it can be detected algorithmically. As the watermark, cannot be seen by human eye it can be used for the proof of ownership in the case of fraud. This watermark is used as a backup for the Visible Watermark [7].

a) Fragile Watermarking: Fragile watermark is the technique in which watermark gets altered when the watermark content is modified. Temper-proofing is one of the applications of fragile watermarking. The method is useful in situations where it is mandatory to prove that the file is not tampered, such as using a file as evidence in a court, but this method is unsuitable for recording the credentials of copyright holder of the file since it can be easily removed. If any change is made to the signal the

extraction algorithm will fail. This watermarking technique is easier to implement as compared to robust watermarking techniques [8] explained in the next sub-section.

b) Robust Watermarking: In this technique, changes to the watermarked content will not affect the watermark. In this, the watermark can be detected after significant levels of tampering of all kind. The uncovering or detecting process of the watermark can only give the probability of availability of the watermark. If the watermark is robust, then during the extraction process watermark should be correctly recovered even if the modification is strong.

6.2.3 Dual Watermarking: Dual Watermarking technique is done by the combination of both visible watermarking and invisible watermarking. It contains both the watermarks inside the cover image.

6.3 According to working domain:

On the bases of working domain Digital Watermarking is classified into two parts, first one is the Spatial domain and second one is the Transform domain. Classification according to working domain is shown in fig. 5. And they are further classified as follows.

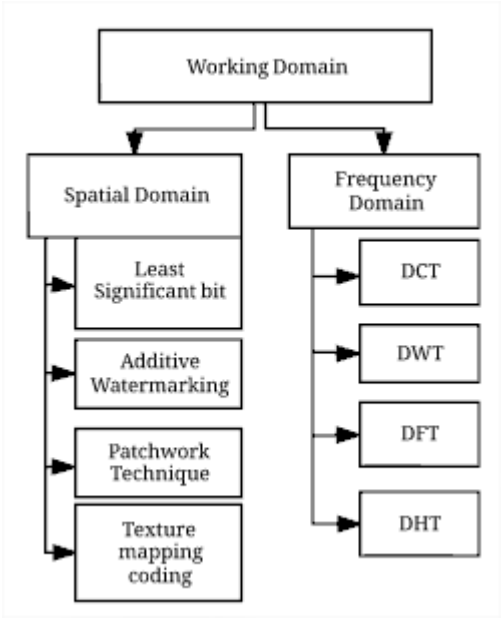


Fig. 5 Classification according to working domain

6.3.1 Spatial Domain: Spatial domain mainly focused on modifying pixel values of one or two randomly selected subsets of images. This algorithm directly loads or embed the raw data into image pixels. Some of the algorithm of spatial domain technique are LSB, Patchwork, text mapping coding, Additive watermarking etc.

*a) Least significant bit Technique (LSB)**:*** LSB technique is one of the simplest Technique to implement. During this process watermark bit is added to the least significant bit of each pixel. Only the last bit of each pixel is read to disclose the watermark data during extraction or detection method. In this method, even if the watermarked image is cropped the receiver can still get the required data, as the data is embedded number of times. This technique is very sensitive to noise and cannot be used for practical purposes. Also, it is not very robust [9].

Advantage of LSB Technique: -
1. Simplest method to implement.
2. Computational complexity of LSB is very less for both embedding and extraction of watermark.
3. Degradation of image quality is less.
Disadvantage of LSB Technique: -
1.This method is not very robust to various attack.
2.Attacks like cropping, shuffling, and scaling destroy the embedded watermark.
3. It is very sensitive to noise.

b) Patchwork Technique: Patchwork is the statistical technique which is developed by Bender et al. In this technique watermark patches are inserted based on a statistic found using a Gaussian distribution. The technique works as follows. Two patches are randomly selected say patch A and patch B. Patch A image data is brightened and Patch B image data is darkened [10]. This technique uses redundant pattern encoding to embed data within an image.

Advantage of Patchwork Technique: -
1.In this Technique robustness is very high against various attacks.
Disadvantage of Patchwork Technique: -
1.Very small amount of information can hide.

c) Additive Watermarking: Spatial domain technique is one of the simplest and most straightforward technique for embedding the watermark. In this, pseudo random noise pattern is added to the intensity of image pixel. The noise signal is usually a floating-point number or an integer like -1, 0, 1. In this noise is generated by a key which ensure that watermark can be detected [11].

d) Texture mapping coding: Texture mapping coding is the technique in which watermark is hidden in the texture part of the image. This method is useful for only those images which have some text part. The Data is hide within the continuous random texture pattern of an image. Thus, the method is suitable for only those images having variable texture [12].

Advantage of Texture Mapping Coding Technique: -
1. The information is embedded in the continuous random texture pattern of an image.
Disadvantage of Texture Mapping Coding Technique: -
1.This method is only suitable for those areas which have large number of texture images. The method requires the human intervention.
Table 1 shows the characteristics and drawback of spatial domain technique [10] [9] [16] [15]. Spatial domain technique is easy to implement and understand. But from security point of view it is not secure.

Table 1: Characteristics and drawback of spatial domain technique

Characteristics	***Drawbacks***
1. All these methods are robust against some common operations like media filter, rotation etc. 2. In this the Watermark is embedded in pixel domain. 3. During watermark embedding, no transform is applied to host signal. 4. The watermark data can be detected or extracted by correlating the expected pattern with the received signal. 5.This technique is very simple to implement and understand. 6.Computational complexity is very less.	1.Almost in all spatial domain technique the original image is altered during the embedding phase. 2. Image processing operation like lossy image compression can destroy the watermark. 3. Intermediate party can easily alter the watermark. 4. Less embedding capacity of watermark is one of the main drawbacks of spatial domain technique.

6.3.2 Transform Domain: This technique is also known as frequency domain. Values of some frequencies are changed from their original one. There are some common used frequency domains methods, such as DCT, DFT, DWT, and DHT.

a) Discrete Cosine Transform (DCT): In digital watermarking DCT technique is one of the most widely used technique. Robustness is more in this technique as compare to the spatial domain. Transform domain algorithms are robust against simple image processing operation like blurring, low pass filtering etc. But they are not so strong against some geometric attacks like rotation, scaling etc. Transform domain techniques are difficult to implement as its computational complexity is very high. DCT have excellent energy compaction property [13]. DCT of 2-D image is defined as $C = \{g(i,j),\ i,j = 0,1,\dots,M-1\}$. In eq.6 the input image g, and the DCT coefficients for the output image G are computed. In the equation g is the input image having $M \times M$ pixel, $g(i,j)$ is the intensity of the pixel of the image and $G(a,b)$ is the DCT coefficient of the DCT matrix. Formula for DCT transform is defined as:

Forward DCT transform in shown in eq. (6).

$$G(a,b) = \sigma(a)\sigma(b)\sum_{i=0}^{M-1}\sum_{j=0}^{M-1} g(i,j)\cos\left[\frac{(2i+1)a\pi}{2M}\right]\cos\left[\frac{(2j+1)b\pi}{2M}\right] \quad (6)$$

Eq. 7 shows the inverse of DCT transform.
Inverse DCT transform:

$$g(i,j) = \sigma(a)\sigma(b)\sum_{a=0}^{M-1}\sum_{b=0}^{M-1} G(a,b)\cos\left[\frac{(2i+1)a\pi}{2M}\right]\cos\left[\frac{(2j+1)b\pi}{2M}\right] \quad (7)$$

Where

$$\sigma(a) = \begin{cases} 1/\sqrt{2}, & for\ a = 0 \\ 1, & for\ a = 1,2,3,\dots M-1 \end{cases}$$

$$\sigma(b) = \begin{cases} 1/\sqrt{2}, & for\ b = 0 \\ 1, & for\ b = 1,2,3,\dots M-1 \end{cases}$$

DCT have Alternate current (AC) Coefficient and Direct current (DC) coefficient. Generally, middle frequency and higher frequency coefficients are chosen for embedding of watermark bit [14]. Fig. 6 shows the frequency bands of DCT coefficient.

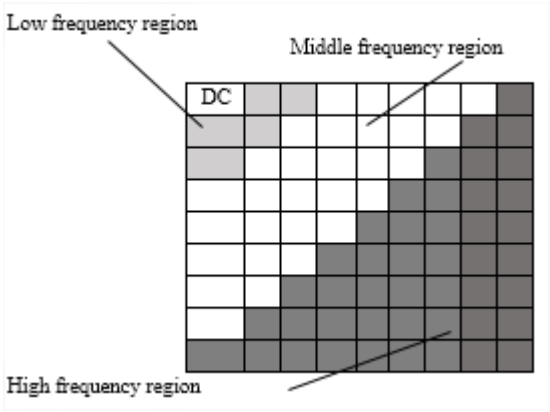


Fig. 6 Frequency bands of DCT coefficient

Advantage of DCT Transform: -
1.In this watermark is hidden into the coefficient of middle and high frequency, so the image visibility will not get affected and the watermark cannot be hacked or removed by anyone.
Disadvantage of DCT Transform: -
1.Some higher frequency component are suppressed during the quantization.
2. Under scaling attack this technique doesn't work.

b) Discrete Wavelet Transform (DWT): Discrete Wavelet T3ransform is a technique which is used in many different areas like digital image processing, image

compression, digital watermarking etc. DWT technique is based on small waves called as wavelet of variable frequency and limited duration. Decomposition of the image is take place into three different direction i.e. horizontal, vertical and diagonal. The process of decomposition is as follow: firstly, it divides the image into four wavelets (LL, LH, HL, HH), where H denotes the high pass filter and L denotes the low pass filter. The first letter (H or L) shows the filter in horizontal direction whereas second letter (H or L) shows the filter in vertical direction. For example, LL wavelet is obtained by applying low pass filter in horizontal direction and low pass filter in vertical direction [16] [17]. Three level of decomposition [18] is shown in fig.7.

This method helps in effective compression of the image and in hiding of data in the image.

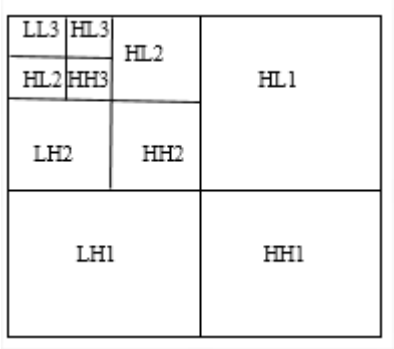


Fig. 7 Decomposition of DWT

Characteristics of DWT Watermarking

1. As it is decomposed into three different direction i.e. horizontal, vertical and diagonal, it reflects the anisotropic properties of Human Visible System (HVS).
2. It is computationally efficient.
3. The magnitude of DWT coefficient is larger in the lowest band (LL) where as it is smaller for other bands (HH, LH, HL) at each level of decomposition.
4. Texture pattern and edges of an image are easily located by high resolution sub bands.

Advantages of DWT Technique: -

1.It is more robust to cropping.
2. It is effective in structural attacks.
3. Compression ratio is very high which is relevant to human perception.
4. DWT has multi resolution feature.

Disadvantages of DWT Technique: -

1.Computing cost is high.
2.It takes longer Compression Time.
3.Noise is present near edges of images.

c) Discrete Fourier Transform (DFT): Discrete Fourier transform is the transformation technique which transform the continuous function into its frequency components. Generally, the Fourier Transform of an image have complex values which leads to a magnitude and phase representation of the image. The 2-D DFT of an image $f(u,v)$ of size $M \times N$ is given as [19]:

$$F(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} f(u,v).e^{\frac{-j2\pi ux}{M}}.e^{\frac{-j2\pi vy}{N}} \quad (8)$$

Where

$u = 0, 1, 2, \ldots . M-1$ and

$v = 0, 1, 2, \ldots . N-1$

$f(u,v)$ is the value of the image at point (u,v) and $F(x,y)$ correspond to the DFT coefficient at point (x,y) in frequency domain. It is robust against some geometric attacks like rotation, scaling, cropping etc.

Characteristics of DFT watermarking

1.It is invariant to Rotation, Scaling and Translation (RST). And hence it is used to recover the data from geometric distortions.
2. Generally real image DFT values are complex.
3. Its strongest components are the central components which contains the low frequencies.

Advantages of DFT Technique: -

1. Invariant to Rotation, scaling and translation (RST) and can be used to recover from geometric distortion.

Disadvantages of DFT Technique: -

1. Its implementation is very complex.
2. Computing cost is also high.

d) Discrete Hadamard Transform (DHT): Discrete Hadamard transform is mainly used in image processing and image compression. It is a non-sinusoidal transform and it is based on Hadamard matrix [20]. It is an orthogonal square matrix of order n whose values are (± 1) and uses less number of coefficients compared to other techniques. It satisfies the following relation:

$$HH^T = I$$

Where,

$H = N \times N$ Hadamard Matrix

$I =$ Identity matrix

The Normalized Hadamard Matrix is defined as [21] eq. (9):

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix} \quad (9)$$

In Hadamard Matrix value of $H_1 = 1$. The Hadamard Matrix is generated using Kronecker product $\otimes$ of

matrices. Eq. 10 shows the Kronecker product of the matrices.

$$H_n = H_{n-1} \otimes H_2 \quad (10)$$

For the value $n = 2$ and $n = 3$ the Hadamard matrix is define as:

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

The complexity of this transformation technique is very less as this Technique needs only simple addition and subtraction operation. For hiding or embedding the watermark, Hadamard Transform has more useful middle and high frequency band as compare to the other high gain transformation technique like DCT and DWT at high noise level. DCT and DWT techniques are suitable only when the channel noise is less [21]. During compression, watermark added using DCT and DWT may get lost but it doesn't happen in Hadamard transform.

Characteristic of Hadamard Transform

1.It uses only simple addition and subtraction operation. No multiplication and division operation is applied.
2. Real values are used in a matrix not complex value which makes this transformation technique easier.
3.This technique survive under the image compression attack.
4. Computational complexity is less as compared to other transformation technique.
5. Middle and high frequency bands are used for watermarking.
6.Hadamard matrix should satisfy the orthogonality.

Advantage of DHT Technique: -

1. Computational cost is less.
2. It is less complex as only addition and subtraction is used.
3. Real values used are +1 and -1.
4. It is more efficient.
5. survive under lossy image compression attack.
6. It is a fast transformation technique.

Disadvantage of DHT Technique: -

1. It is less complex as compare to other transform technique but more complex than spatial domain technique.

7. Attacks on Digital Watermarking

There are different intentional or unintentional attacks that can be performed on watermarked data. The accessibility of image processing software's in wide range, made it possible to perform attacks on watermarking system. The purpose of these attacks is to foil the watermark Various type of watermarking attacks are as follows:

7.1 Removal attack: This type of attack is very dangerous as these attacks intends to remove the watermark data from the watermarked object.

7.2 Interference attack: Interference attacks are those types of attack in which noise is added to the watermarked object. Examples of Interference attack are lossy compression, quantization, averaging, remodulation and denoising etc.

7.3 Geometric attack: Rotation, cropping, flipping can be performed on an image as these types of manipulations affects its geometry. Cropping of image from the right-hand side and from bottom is an example of geometric attack.

7.4 Security Attack: In this case, we talk about an attack on security. An attacker try to change or modify the watermark is the watermark algorithm is known to him. A watermarking algorithm is secured if the embedded or hidden information cannot be destroyed, detected or forged.

7.5 Cryptographic attacks: These types of attack deals with the security of the watermarking technique. One of the examples of these type of attack is the oracle attack [22]. In this attack, a non-watermarked object is developed when a public watermark detector device is available.

7.6 Active attacks: In this type of attacks, an attempt is made to remove the watermark or simply make the watermark undetectable.

7.7 Passive attack: In this, attacker do not remove the watermark instead just tries to find out whether the watermark is present in an image or not.

7.8 Image compression: Image compression is used for reducing the storage capacity and for decreasing the cost of bandwidth required for the transmission of data [23]. Generally, lossy compression methods are more harmful than the lossless compression method. Lossless compression method can recover the watermark image but the probability of recovery in lossy compression is very less.

8. Comparison and Result Analysis

Following table 2 shows the comparison between spatial domain and transform domain Digital Watermarking [23] [12]. Different parameters are used to compare the Spatial domain and Frequency domain like Computation cost,

Computation complexity, Robustness, Capacity, Computational cost and Effectiveness.

Table2. shows that the computational complexity of spatial domain is low while for the transform domain it is high.

Table2: Comparison Between Spatial Domain and Transform Domain

Factors	***Spatial domain***	***Transform domain***
Computation cost and computational complexity	Less	High
Robustness	Less Robust	More Robust
Capacity and Computational cost	High	Low
Effectiveness	Less	More

8.1 Result Analysis based on PSNR and MSE values

Mohanty et al. [24] presents a robust watermarking scheme. In this, subimage is used for the watermarking process which eliminates the chance of removal of watermark. An approach is given by Mohanty et al. for creation of synthetic compound watermark. Grey scale image or color image can be used as a watermark. Mohanty's algorithm for Additive watermarking technique gives the PSNR value of 35.17 dB and MSE value of 19.76 dB on Lena image of size 512×512 shown in fig. 8.

(a) Original image (b) Image with invisible Watermark

Fig. 8 Invisible watermarking

Amit Kumar et al. [25] presents the watermarking scheme using LSB technique. In this technique, the watermark is embedded in least significant bit of the cover object. So, the PSNR value is calculated for every bit. In table 3, the PSNR value calculated for LSB technique is 51.14 dB which is only for the first bit.

Jagdish C Patra et al. [26] presents the novel DCT domain watermarking scheme for image authentication based on Chinese Remainder Theorem (CRT). With the use of CRT, the security is improved and low computational complexity is achieved. One of the disadvantage of this scheme is that it is not robust against several noise attacks.

Robust digital image watermarking scheme in DFT domain is presented by M. Cedillo-Hernandez et al. [27]. The author calculated the speeded up robust feature (SURF) point during the embedding process and stored it in advance for the detection process. The method is robust to affine distortion and it allows the simple RST attacks. The PSNR value and MSE value for the given algorithm is 45 dB and 2.05 dB

More the PSNR value of image shows the less distortion of image and more the MSE value of an image shows the more distortion in an image. As the PSNR value and MSE values are inversely proportional to each other.

Baisa L. Gunjal et al. [28] presents the robust non-blind digital watermarking scheme. In his research paper a comparative study is performed in DWT and DWT-FWHT-SVD domains. For DWT decomposition, orthogonal 'Haar' wavelet is used. PSNR value for DWT is 42.79 dB which is more than DCT.

Even though DWT gives better PSNR value compared to DCT, the researchers uses DCT based watermarking technique for hardware implementation. Because DCT is easy to implement as compare to DWT.

The image watermarking using block coefficient in DHT is presented by Elham Moeinaddini et al [29]. For embedding the watermark two adjacent block of DHT coefficient are modify. DHT scheme is easy to implement as compare to other transformation techniques. This algorithm gives the better robustness under JPEG image compression.

Table 3 shows the comparison of different watermarking techniques on Lena image of size 512×512.

Table 3: Comparison of different watermarking methods on Lena image

Sno	***Techniques***	***Authors***	***PSNR(dB)***	***MSE***
1.	Additive watermarking technique	Mohanty et al. [24]	35.17	19.76
2.	LSB	Amit Kumar Singh et al. [25]	51.14	0.50
3.	DCT	Jagdish C. Patra et al. [26]	41.42	4.68

4.	DFT	M. Cedillo-Hernandez et al. [27]	45	2.05
5.	DWT	Baisa L. Gunjal et al. [28]	42.79	3.41
6.	DHT	Elham Moeinaddini et al. [29]	45.09	2.01

Table 3 shows that DHT technique has higher PSNR value as compare to other transformation techniques.

Fig. 9 shows the PSNR values on 3 different types of attacks i.e. JPG compression, Media filter and Gaussian attack. Graph represents the comparison of Mohanty et al. [24], Mohammad et al. [30] and Moeinaddinietal et al. [29] algorithms on different types of attacks.

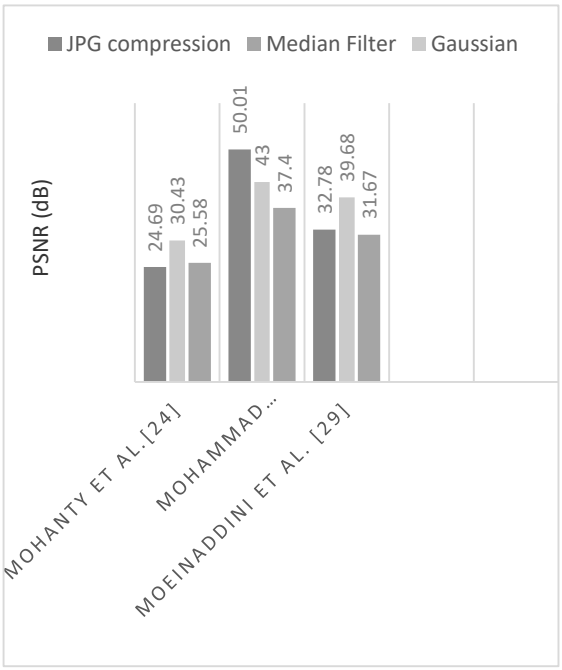


Fig. 9 PSNR values on different types of attacks

9. Conclusion

In this paper, we focused on digital watermarking techniques, applications, characteristics of digital watermarking and attacks, also discussed the advantages and disadvantages of different techniques and comparison between spatial domain and transform domain. This paper shows that for security purpose transformation techniques are more suitable. Spatial domain techniques are easy to implement, however, there is scope of enhancing the security. Hadamard transform is the fastest technique in transformation domain as it uses only simple addition and subtraction operation. It is less complex.

Based on the PSNR values and MSE values results of different authors have been compared.

In this paper, we have tried to give the complete knowledge of digital watermarking which will help the new researchers to get the maximum knowledge about this domain.

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] Su, J.K., F. Hartung, and B. Girod, "Digital Watermarking of Text, Image, and Video Documents", University of Erlangen- Nuremberg: Erlangen,1999.
[3] Bami, M., et al., Watermark embedding: hiding a signal within a cover image. Communications Magazine, IEEE, 2001. 39(8): p. 102-108.
[4] Navneet Kumar Mandhani, "Watermarking Using Digital Sequences", MS thesis, Andhra University, August 2004.
[5] Edin Muharemagic and Borko Furht, "A Survey of watermarking techniques and applications", 2001.
[6] G. Coatrieux, L. Lecornu, Members, "A Review of digital image watermarking in health care", Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE.
[7] B. Surekha, Dr. G. N. Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January,2011.
[8] Kaur Gurpreet and Kaur Kamaljeet, "Image Watermarking Using LSB (least significant bit)," International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), ISSN: 2277 128X, Vol. 3, ISSUE. 4, April 2013.
[9] K.P. Soman, K.I. Ramachandran- "Insight into Wavelets from, Theory to Practice".
[10] CHAPTER 2: LITERATURE REVIEW, Source: Internet.
[11] Jiang Xuehua, "Digital Watermarking and Its Application in Image Copyright Protection", International Conference on Intelligent Computation Technology and Automation, 2010.
[12] Tamirat Tagesse Takore, Dr. P. Rajesh Kumar and Dr. P. Rajesh Kumar, "A Modified Blind Image Watermarking Scheme Based on DWT, DCT and SVD domain Using GA to Optimize Robustness", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016.
[13] Satyanarayana Murty, M. Uday Bhaskar and P. Rajesh Kumar, "A semi-blind refrence watermarking scheme using DWT-DCT-SVD for copyright protection", International journal of computer science and information technology, pp. 69-82, vol. 4, No. 2, 2012.
[14] Chunlin Sone, Sud Sudirman, Madjid Merabti, "Recent Advances and Classification of Watermarking Techniques

in Digital Images", School of Computing and Mathematical Science, Liverpool John Moores University, UK.
[15] Darshana Mistry, "Comparison of Digital watermarking methods", (IJCSE) International journal on Computer Science and Engineering Vol. 02, No. 09, 2010.
[16] Advith J, Varun K R and Manikantan K, "Novel Digital Image Watermarking Using DWT-DFT-SVD in YCbCr Color Space", (ICETETS) International conference on emerging trends in Engineering, technology and science, 2016.
[17] Anuradha, Rudresh Pratap Singh, "DWT Based Watermarking Algorithm using Haar Wavelet," International Journal of Electronics and Computer Science Engineering, Vol. 1, No. 1, 2012.
[18] Jingbing Li, Wencai Du, Yaoli Liu and Yen-wei Chen, "The medical image watermarking algorithm based on DFT and logistic map", (ICCCT) International Conference on Computing and Convergence Technology, 2012.
[19] Prat, W. K., "Digital Image processing", John Wiley Editions, 1991.
[20] A. N. Akansu and R. A. Haddad, "Multiresolution Signal Decomposition: Transforms, Subbands and Wavelets", Academic Press Inc., 1992.
[21] A.T. S Ho, Shen Jun, A. K. K. Chow, and J. Woon, "Robust digital image-in-image watermarking algorithm using the fast Hadamard transform," in Proc.IEEE ISCAS'03, vol. 3, May 2003, pp. 826-829.
[22] Dr. Vipula Singh, "Digital Watermarking: A Tutorial", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), January Edition, 2011.
[23] Prabhishek Singh, R S Chandha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March 2013.
[24] Saraju P. Mohanty, Bharat K. Bhargava "Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks", ACM Transactions on Multimedia Computing, Communications and Applications, Vol. 5, No. 2, Article 12, November 2008.
[25] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, "A Novel Technique for Digital Image Watermarking in Spatial Domain", IEEE International Conference on Parallel, Distributed and Grid Computing, 2012.
[26] Jagdish C. Patra, Jiliang E. Phua, Cedric Bornand, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression", Digital Signal Processing 20, 1597–1611,2010.
[27] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, and H. Perez-Meana, "Robust Digital Image Watermarking Using Interest Points and DFT Domain", IEEE International Conference on Telecommunications and Signal Processing (TSP), 2012.
[28] Baisa L. Gunjal, Suresh N.Mali, "Comparative Performance Analysis of Digital Image Watermarking Scheme in DWT and DWT-FWHTSVD Domains", Annual IEEE India Conference (INDICON), 2014.
[29] Elham Moeinaddini, Roya Ghasemkhani, "A novel image watermarking scheme using blocks coefficient in DHT domain", The International Symposium on Artificial Intelligence and Signal Processing (AISP), 2015.
[30] Mohammad Amrollahzadeh, Siamak Talebi, "A blind JPEG image watermarking in the DCT domain", IEEE Iranian Conference on Electrical Engineering, 2010.