IMAGE DIGITAL WATERMARKING: A SURVEY

*V. Ashok kumar[1], Ch. Srinivasa Rao[2], C. Dharmaraj[3]

[1]Department of E.C.E, AITAM, Tekkali, A.P, INDIA
[2] Department of E.C.E, JNTUCE, Vizianagaram, JNTUK,A.P, INDIA
[3] Department of E.C.E, GITAM, A.P, INDIA
[1]venkuash123@rediffmail.com, [2]ch_rao@rediffmail.com, [3]dharmaraj.cheruku@gitam.edu

Abstract

Nowadays digital watermarking is important for the protection against illegal redistribution of digital data as of high popularity and accessibility over the internet.Digital image watermarking techniques havebeen developed widely in recent years to maintain thebroadcasting media and content authentication, broadcastmonitoring, copy control, and many other applications.Therefore, many studies have used digital image watermarkingto solve these problems. This present paper starts with a basic model of digital imagewatermarking, discusses the characteristics and its applications, presents the various categories of DWM and reviews some of the techniques andalgorithms used in image watermarking. It also includes performance evaluation of techniques on the basis of performance parameters like PSNR values and NCC values.

Keywords: **Digital Watermarking, Watermarking System, Watermarking applications, PSNR, NCC.**

1. INTRODUCTION

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.The term "Digital Watermark" was coined by Andrew Tirkel and Charles Osborne in December 1992. The first successful embedding and extraction of a steganography spread spectrum watermark was demonstrated in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin[1].

The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They were used as a means to identify the papermaker or the trade guild that manufactured the paper. The marks often were created by a wire sewn onto the paper mold. Watermarks continue to be used today as manufacturer's marks and to prevent forgery and fraud.

A general scheme for digital watermarking is given in figure 1. The inputs to the embedding process are watermark, cover object and a secret key. The key is used to enforce security and to protect the watermark. Only owner of the data knows the key and it is not possible to remove the watermark from the cover image without the knowledge of the key. Then, the watermarked image passes through the transmission channel. The transmission channel may include the possible attacks, such as lossy compression, geometric distortions, any signal processing operation and conversion of digital to analog and analog to digital,

etc. The channel for the watermarked data could be a lossy, noisy, unreliable channel. Thus the received data may be different from the original watermarked data. The inputs for extraction are the received watermarked data and the key corresponding to the embedding key. The output of the watermarking scheme is the watermarked data.

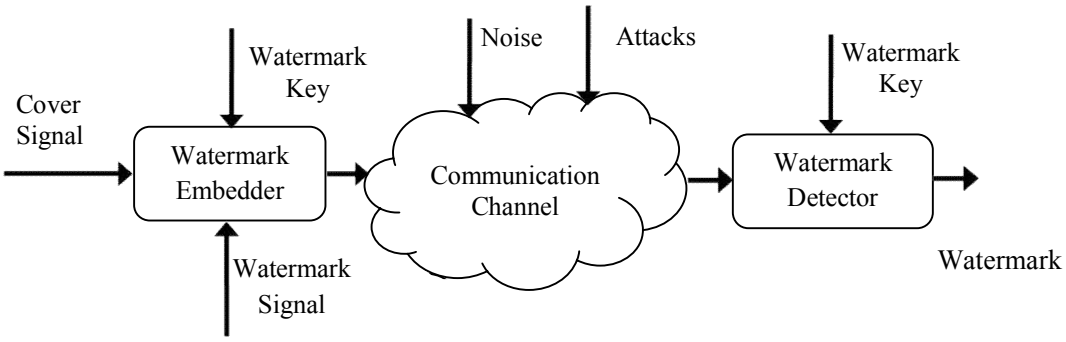

Figure 1: General Process of digital watermarking

2. Characteristics of Digital Watermarking

A digital watermarking is a kind of technique that secretly embedded a noise-tolerant digital data such as an audio, video or image data. It is used to identify ownership of the copyright of digital data.There are a number of authors that have discussed the characteristics of watermarks [2, 3, 4, 5]. Digital watermarking concerns to solve some issues properly, thus, the present paper highlight the main characteristics of watermarked image. Some of the characteristics are robustness, tamper resistance, Non-perceptibility, fidelity, Pay-load capacity computational cost, Security, Verifiability and false positive rate.

a) Robustness: Robustness means the watermark embedded in a data can persist under various attacks and geometric operations like rotation, scaling, compression etc. It should be robust against different geometrical and non-geometrical attacks. The watermark embedded in a data also survives common signal processing operations such as digital-to-analog-to-digital conversions and lossy compression. In addition, not all watermarking algorithms have the same level ofrobustness, Some techniques are robust against somemanipulation operations, however, they fail against otherstronger attacks [6]. Moreover, it's not always desirablefor watermark to be robust, in some cases; it's desired forthe watermark to be fragile [7]. Therefore, the robustnesscan be classified as following:

i. **Robust:** The watermark is designed to be able to persist against incidental and intentional attacks [8]. This kind of watermarking can be used in broadcast monitoring, copyright protection, fingerprinting, and copy control [9].

ii. **Fragile:** The watermark in this type is designed tobe destroyed at any kind of modification, to detectany illegal manipulation, even slight changes,involving incidental and intentional attacks. The Fragile watermarks are mainly used in contentauthentication and integrity

verification. They useblind detection type [9], as it will be discussed indetection Types. In addition, the implementationof fragile techniques is easier than theimplementation of robust ones [10].

iii. **Semi-fragile:** The watermark in this type is robustagainst incidental modifications, but fragileagainst malicious attacks [11]. And it is used forimage authentication [12].

b) Imperceptibility: Imperceptibility (also known as Invisibility and Fidelity) is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image [13]. In other words, the watermarked image should look similar to the original image, and the watermark must be invisible in spite of occurrence of small degradation in image contrast or brightness. However, the challenge is that imperceptibility could be achieved, but the robustness and the capacity will be reduced, and vice versa, imperceptibility may be sacrificed by increasing the robustness and the capacity [14]. Moreover, the watermark not always desired to be invisible, sometimes, it is preferred to have visible watermark into the image [15].

c) Capacity: Capacity (also known as Payload) refers to the number of bits embedded into the image. The capacity of an image could be different according to the application that watermark is designed for [13]. Moreover, studying the capacity of the image can show us the limit of watermark information that would be embedded and at the same time satisfying the imperceptibility and robustness [4].

d) Security: Security is the ability to resist against intentional attacks. These attacks intended to change the purpose of embedding the watermark. Attacks types can be divided into three main categories: unauthorized removal, unauthorized embedding, and unauthorized detection [13]. According to the specific usage of watermarking, the specific feature should be available in the watermark to resist the attacks. Therefore, for unauthorized removal, the watermark should be robust and not to be removed, and for unauthorized embedding (also known as forgery), the watermark should be fragile or semi fragile to detect any modification. Lastly, for unauthorized detection, it should be imperceptible watermark [16].

e) Low Complexity: The cost is the reason behind studying the complexity, so it should be at a reasonable cost [17]. It describes the economics of using watermark embedders and detectors, because it can be very complicated and depends on business model that is used. The main two issues of complexity are the speed of embedding and detection, and the number of embedders and detectors [13].

3. Applications of Digital watermarking

Watermarking techniques may be relevant in the following application areas [26] which includes copyright protection, copy protection, tamper detection, broadcast monitoring, finger printing and other areas [18].

3.1 Copyright Protection

The primary use of watermarking is where an organization wishes to assert its ownership of copyright for digital objects. This application is of great interest to 'big media' organizations and of some interest to other vendors of digital information such as news and photo agencies. These applications require a minimal amount of information to be embedded, coupled with a high degree of resistance to signal modification (since they maybe subjected to deliberate attack). For example, now a days, a news channel "AAJ-TAK" is showing the animal's clips (which are already shown on "Discovery" Channel) by hiding the discovery channel's logo on the video clips. As per the law, The AAJ-TAK should show the curtsey-sign and should pay the copyright fee to the Discovery channel. In such cases, there is a strong need of watermarking as once the digital data is broadcasted, anybody else can start selling it without paying the IPR value to its owner.

3.2 Copy Protection

Watermarking can be used as a strong tool to prevent illegal copying. For example, if an audio CD has a watermark embedded into it, then any of the system (Hardware like DVD, or software) cannot make a copy of it, and even if it copies, the watermark data will not get copied to new duplicate audio CD. Now the duplicate CD can be easily found because it does not have watermark data. Some schemes have attempted to satisfy more complex copy protection requirements. An early example is the Serial Copy Management System (SCMS), introduced in the 1980s, which enabled a user to make a single digital audio tape of a recording they had purchased but prevented the recording of further copies (i.e. second generation) from that first copy. The scheme failed ultimately because not all manufacturers of consumer equipment were prepared to implement the scheme in their products.

3.3 Tamper Detection

In this application area, it is necessary to assure that the origin of a data object is demonstrated and its integrity is proved. One example of tamper detection is photographic forensic information which may be presented as evidence in the court. Given the ease with which digital images can be manipulated, there is a need to provide proof that an image has not been altered. Such a mechanism could be built into a digital camera [19]. For example, if a cop's camera catches an over speeding vehicle then when proving the driver guilty in front of the judge, the accused may claim that the video presented in the court is tampered and the car shown in the video does not belong to him. A watermarking system which is embedded in digital cameras may help to resolve the issue. If somebody tries to tamper the data, the watermark will get destroyed indicating that the data is tampered. In our country, a well-known example is the "Tahalka-Scam".

3.4 Broadcast Monitoring

There are several types of organizations and individuals interested in monitoring the broadcast of their interest. For example, advertisers want to ensure that they receive the exact airtime that they have purchased from broadcasting firms. Musicians and actors want

to ensure that they receive accurate royalty payments for broadcasts of their performances and copyright owners want to ensure that their property is not illegally rebroadcast by pirate stations. In 1997, a scandal broke out in Japan regarding television advertising. At least two stations had been routinely overbooking air time. Advertisers were paying for thousands of commercials that were never aired [16]. The practice had remained largely undetected for over twenty years because there were no systems in place to monitor the actual broadcast of advertisements. This broadcast monitoring can be implemented by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring stations can then receive broadcasts and look for these watermarks identifying when and where each clip appears.

3.5 Fingerprinting

If monitoring and owner identification applications place the same watermark in all copies of the same content, it may create a problem. If out of n number of legal buyers of content, one starts selling the contents illegally, it may be very difficult to catch who is redistributing the contents without permission. Allowing each copy distributed to be customized for each legal recipient can solve this problem. This capability allows a unique watermark to be embedded in each individual copy. Now, if the owner finds an illegal copy, he can find outwho is selling his contents by finding the watermark which belongs to only singly legal buyer. This particular application area is known as fingerprinting. This is potentially valuable both as a deterrent to illegal use and as a technological aid to investigation.

3.6 Annotation Applications

In this applications area, watermarks convey object-specific information (“feature tags” or “captions”) to users of the object. For example, patient identification data can be embedded into medical images. These applications require relatively large quantities of embedded data, while there is no need to protect against deliberate tampering. Normal use of the data object may involve such transformations as image cropping or scaling and will require the use of a technique that is resistant to those types of modification.

4. Watermarking techniques

There are several criteria based on which Watermarking techniques are classified. The DWM techniques classified into three categories based on the usage i.e. Document based, Working domain based and Human perception based. Based on the documentation, again classified into image, text, audio and video watermarking. Based on the Human perception, techniques are classified as Visible, Dual and Invisible techniques. Invisible technique is further classified as Robust and Fragile techniques. Based on working domain, the DWM techniques classified into Spatial, Frequency and Hybrid Techniques.The figure 2shows the classification chart of watermarking techniques.

4.1 Based on Document:

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

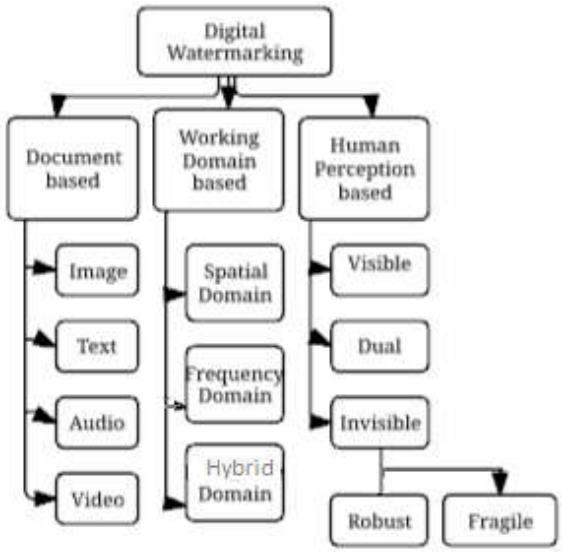

Figure 2: Water marking techniques

4.2 Based on Human Perception

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 figure 3.

Figure 3: (a) Original image (b) Water Mark (c) Water marked image

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.

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 [20].

a) Fragile Watermarking: Fragile watermark is the technique in which watermark gets altered when the watermark content is modified. Tamper-proofing is one of the applications of fragile watermarking. The method is useful in situations such as using a file as evidence in a court where it is mandatory to prove that the file is not tampered. 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 theextraction algorithm will fail. This watermarking technique is easier to implement as compared to robust watermarking techniques [21] explained in the next subsection.

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.

Based on Working Domain: On the basis of working domain Digital Watermarking is classified into two parts,first one is the Spatial domainsecond one is the Transform domain and third one is Hybrid domain. Classification chart of the WM techniques based on working domain is shown in figure 4.

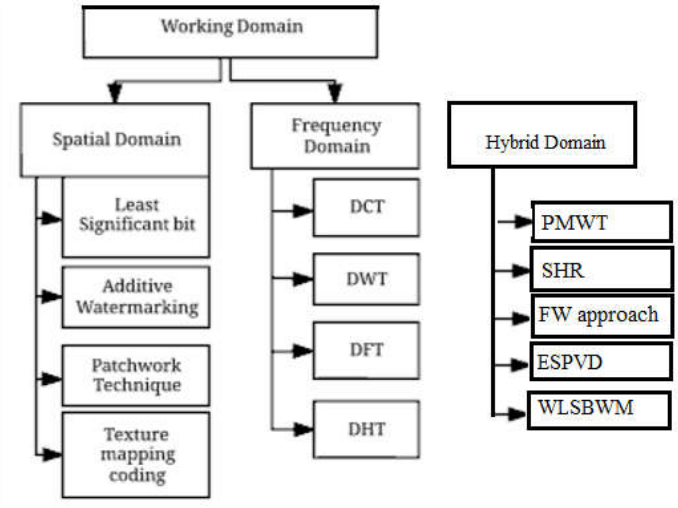

Figure 4: Classification chart of the WM techniques based on working domain.

- **Spatial Domain**: Spatial domain mainly focused on modifying pixel values of one or two randomly selected subsets of images. These algorithms directly load or embed the raw data into image pixels. Some of the algorithms 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 Techniques 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 [22].

*Advantages of LSB Technique***:**(1)This is the 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.
Disadvantages of LSB Technique: (1) This method is not very robust to various attacks. (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 An image data is brightened and Patch B image data is darkened. This technique uses redundant pattern encoding to embed data within an image.
*Advantage of Patchwork Technique***: -** In this Technique robustness is very high against various attacks.
Disadvantage of Patchwork Technique: Very small amount of information can hide.

c) Additive Watermarking: Spatial domain technique is one of the simplest and most straightforward techniques 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 [23].

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 [24].
*Advantage of Texture Mapping Coding Technique***:** The information is embedded in the continuous random texture pattern of an image.
Disadvantage of Texture Mapping Coding Technique: This method is only suitable for those areas which have large number of texture images. The method requires the human intervention [22] [25] [26]. Spatial domain technique is easy to implement and understand. But from security point of view it is not secure.

- **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 [27]. DCT transform is defined as:
Forward DCT transform in shown in eq. (1). and IDCT is shown in equation 2.

$$F(u,v) = c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\Pi(2x+1)u}{2M}\right]\cos\left[\frac{\Pi(2y+1)v}{2N}\right] \quad (1)$$

$$f(x,y) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} c(u)c(v)F(u,v)\cos\left[\frac{\Pi(2x+1)u}{2M}\right]\cos\left[\frac{\Pi(2y+1)v}{2N}\right] \quad (2)$$

Where $u = 0 \ldots M-1, v = 0 \ldots N-1$ *and*

$$c(u) = \begin{cases} \sqrt{\frac{1}{M}}, u = 0 \\ \sqrt{\frac{2}{M}}, u = 1 \ldots M-1 \end{cases} \qquad c(v) = \begin{cases} \sqrt{\frac{1}{N}}, v = 0 \\ \sqrt{\frac{2}{N}}, v = 1 \ldots N-1 \end{cases}$$

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 [28]. Fig. 5 shows the frequency bands of DCT coefficient.

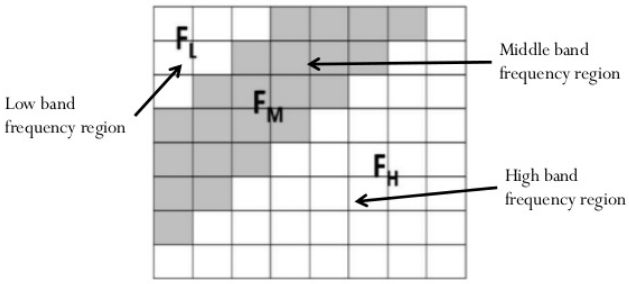

Figure 5: Frequency bands of DCT.

Advantage of DCT Transform: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.
Disadvantages 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): A wavelet is a kind of mathematical function used to divide a given function or continuous time signal to components of different frequency and to study each component with a resolution that matches its scale. A wavelet transform is the representation of a function by wavelets. The wavelets are scaled and translated copies (known as "daughter wavelets") of a finite length or fast decaying oscillating waveforms (known as the "mother wavelet"). The word wavelet is due to Morlet and Grossmann in the early 1980s. They used the French word "ondelette", means "small wave". Soon it was transferred to English by translating "onde" into "wave", giving "wavelet".Today wavelets play a significant role in astronomy, acoustics, nuclear engineering, sub-band coding, signal and image processing, digital watermarking, stenography, neurophysiology, music, magnetic resonance imaging, speech discrimination, optics, turbulence, earthquake prediction, radar, computer and human vision, data mining and pure mathematics applications such as solving partial differential equations etc.

In the wavelet transform an image signal can be analyzed by passing it through an analysis filter bank followed by a decimation operation. This analysis filter bank consists of a low pass and a high pass filter at each decomposition stage. When the signal passes through these filters it splits into two bands. The low pass filter, which corresponds to an averaging operation, extracts the coarse information of a signal. The high pass filter, which corresponds to a differencing operation, extracts the detail information of the signal. The output of the filtering operations is then decimated by two.The figures 6, 7 and 8 describes wavelet concept. Figure 9 describes the resultant images when wavelet operator is applied.

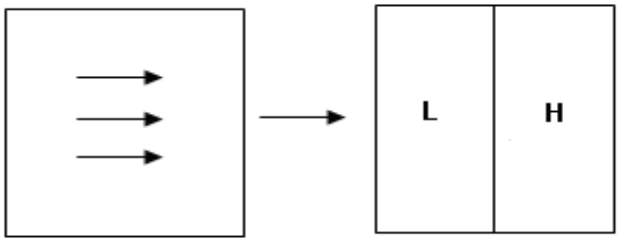

Figure 6: Horizontal wavelet transforms

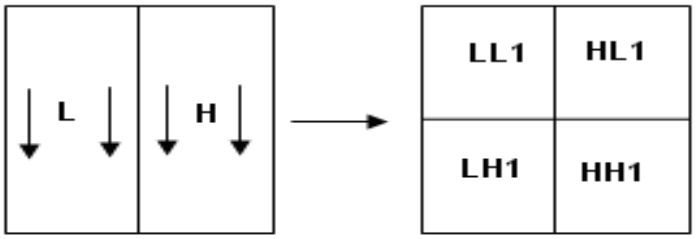

Figure 7: Vertical wavelet transforms for Figure 6

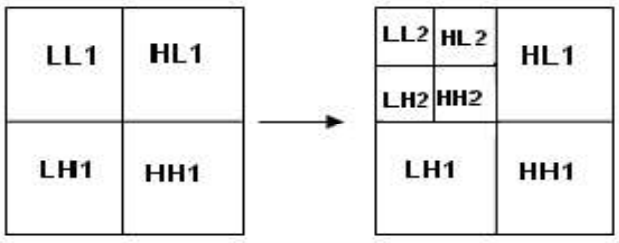

Figure 8:Second level wavelet transforms

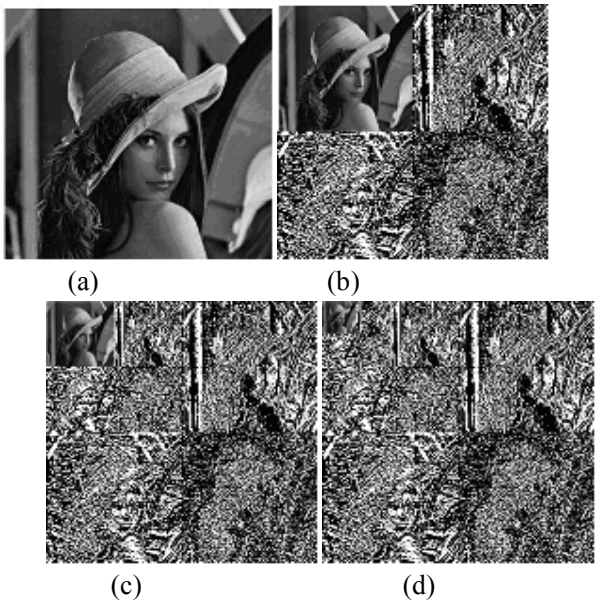

Figure 9: (a) Original Lena image (b) Level-1 wavelet transformed Lena image (c) Level-2 wavelet transformed Lena image (d) Level-3 wavelet transformed Lena image

*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.
*Advantage 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.
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. During compression, watermark added using DCT and DWT may get lost but it doesn't happen in Hadamard transform.

*Advantages 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***:**
It is less complex as compare to other transform technique but more complex than spatial domain technique

Based on Hybrid Technique:
In order to increase the robustness and imperceptibility, Hybrid techniques are used for embedding and extraction of watermark.These techniques uses the combination of both spatial and frequency domain methods. When there is a requirement of highly robust and imperceptible image then the hybrid techniques are preferred rather than the conventional watermarking techniques.

Edgebased sorted pixel value difference(ESPVD) to protect copyrights. This approachmainly consists of two phases: Watermark embedding phase and watermark detection and extraction phase. In the embedding phase, first of all motif patternapproach is used to generate the mixed Image and then, identify the edge pixel locations using morphological edge(ME) operator to embed the watermark. Now, sorted pixel value difference method is used to embed the watermark. The watermark extraction phase also uses the same procedure which is stated earlier to extract the watermark image.

Wavelet based Least Significant Bit Watermarking (WLSBWM) for high authentication, security and copyright protection. The approach utilizes Alphabet Pattern (AP) approach to generate shuffled image in the first stage and Pell's Cat Map (PCM) is used for providing more security and strong protection from attacks. PCM applies on each 5×5 sub images. A

wavelet concept is used to reduce the dimensionality of the image until it equals to the size of the watermark image. Apply the Discrete Cosine Transform in the first stage later applies N levels Discrete Wavelet Transform (DWT) for reducing up to the size of the watermark image. Insert the water mark image in LH_n Sub band of the wavelet image using LSB concept.

5. Attacks on Digital watermarking

Watermark attacks are classified into four main groups: Simple attacks theoretically are simple that effort to injure the embedded watermark by modifying the entire image without any attempt to recognize and separate the watermark. Examples include frequency based compression, addition of noise, cropping and correction. Detection-disabling attacks smash the relationship and make discovery of the watermark impracticable. Typically, they make some geometric distortion like zooming, shift in spatial, rotation, cropping or pixel incarnation, removal or insertion. The watermark in fact remains in the original information and can be recovered with increased intelligence of the watermark detector. Ambiguity attacks attempt to confuse the detector by producing fake watermarked data to discredit the authority of the watermark by embedding several additional watermarks so that it is not obvious which the first, authoritative watermark is. Removal attacks attempt to analyze or estimate (from more differently watermarked copies) the watermark, separate it out and discard only the watermark. Examples are collusion attack, de-noising or exploiting conceptual cryptographic weakness of the watermark scheme (e.g. knowledge of positions of single watermark elements). It should be noted that some attacks do not clearly belong to one group.

To find the effectiveness, the proposed approaches are usually tested against various robustness criteria. The proposed watermarking techniques are tested by using the different geometric attacks and transformations attacks such as salt and pepper noise attack, rotation attack, median filter attack, cropping attack, Gaussian noise attack, compression attack, Grey level blurring attack, Motion blurring attack and Sharpening attack.

Various type of watermarking attacks are as follows:

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

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, re-modulation and de-noising etc.

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

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.

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.

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

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.

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.

6. Performance parameters of Digital watermarking

The present paper discuss the various parameters used to evaluate the DWM i.e. Normalized Correlation Coefficient (NCC), Signal to Noise ratio (SNR), Peak Signal Noise Ratio (PSNR), Mean square error (MSE).

The quality of the watermark or the frangibility of the algorithm is assessed by the similarity measurement NCC between the referenced watermark W and the extracted watermark W* as given in Equation 3.

$$\rho = \frac{\sum_{i=0}^{N-1} w(i) \times w^{*}(i)}{\sum_{i=0}^{N-1} \left(w(i)\right)^{2}} \qquad (3)$$

Where, w(i) and w*(i) are the original watermark and the extracted watermark. In the above equation $\rho = 1$ indicates perfect correlation, while an extremely low value reveals that the watermarks are dissimilar. If NCC value ranges from 0.65 to 1.0 then one can say that the image preserves high quality after inserting the watermark [29].Perceptual quality is a measure of imperceptibility, obtained by determining both the amounts of distortion introduced to a host signal by a watermarking algorithm, and how detectable the distortion is. This can be achieved by PSNR. It is commonly used as a performance metric for digital image and video compression algorithms [30]. Perceptual quality is dependent upon the intended application of a watermarking system. In some cases, detectable amount of distortion may be acceptable if it ensures a higher bit rate or more reliable encoding. In other cases, it may be required that watermark data be completely imperceptible to a user.

The difference between the original image and the watermarked image is computed by Peak Signal Noise Ratio (PSNR). The bigger the PSNR is, the smaller is the difference, and PSNR is defined through given Equation 4.

$$\text{PSNR} = 10\log\left(255^2 / \text{MSE}\right) \quad (4)$$

$$\text{where MSE} = \sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - X'_{ij})^2 / MN$$

where M and N are respectively the length and the width of the host image; Xij denotes the gray level of the original image pixel; X'ij denotes the gray level of the watermarked image pixel.

7. Conclusion

Efficient Digital Image Watermarking Techniques requires exploration of features like robustness, Security, Imperceptibility and complexity against common Image processing operations. Different digital Image Watermarking approaches available in the current literature are mainly categorized into spatial domain and frequency domain methods. But the quality of the watermarked image highly depends upon the watermarking technique used. The present paper revealed the fact that the spatial domain techniques are easy to implement but not robust and imperceptible, where as the frequency domain methods overcomes the weak robustness problem of the spatial domain method and these techniques are used for high quality watermarked image. A comprehensive survey on various important aspects such as characteristics, applications, different types of attacks and performance parameters of digital watermarking methods are presented and discussed in this paper. The researchers are still finding reasons in their own way pertaining to improved robustness and imperceptibility as there is a growing a need for authentication of digital content.

References:

[1] A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. "Electronic Water Mark".DICTA 93, Macquarie University.p.666-673.

[2] I. Cox and M. L. Miller. A review of watermarking and the importance of perceptual modeling. In Proceedings of SPIE, Human Vision & Electronic Imaging II, volume 3016, pages 92–99, 1997.

[3] F. Hartung and M. Kutter. Multimedia watermarking techniques. Proceedings of the IEEE, 87(7):1079–1107, 1999.

[4]F. A. P. Petitcolas, R. Anderson, and M. G. Kuhn. Information hiding - a survey. Proceedings of the IEEE, 87(7):1062– 1077, 1999.

[5]R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp. Perceptual watermarks for digital images and video. Proc. of the IEEE, 87(7):1108–1126, 1999

[6]R. F. Olanrewaju, "Development of Intelligent Digital Watermarking via Safe Region," PHD, Electrical and Computer Engineering, International Islamic University Malaysia, Kulliyyah of Engineering, 2011.

[7]M. L. M. Ingemar J. Cox, Jeffrey A. Bloom, Jessica Fridrich, and Ton alker, Digital Watermarking and Steganography: Morgan Kaufmann ublishers, 2008

[8]J.-S. Pan, H.-C. Huang, and l. C. Jain, Eds., Intelligent Watermarking Techniques (Series on Innovative Intelligence. World Scientific, 2004,

[9]L. Jian and H. Xiangjian, "A Review Study on Digital Watermarking," in Information and Communication Technologies, 2005. ICICT 2005. First International Conference on, 2005, pp. 337-341.

[10]N. Cvejic, "Algorithms for Audio Watermarking and Steganography," Department of Electrical and Information Engineering, University of Oulu, 2004.

[11]A. G. Charles Fung, Walter Godoy Junior, "A Review Study on Image Digital Watermarking," presented at the The Tenth International Conference on Networks, St. Maarten, The Netherlands Antilles, 2011

[12]S. Jun and M. S. Alam, "Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/Semifragile Digital Image Watermarking," Instrumentation and Measurement, IEEE Transactions on, vol. 57, pp. 595-606, 2008

[13] M. L. M. Ingemar J. Cox, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, Digital Watermarking and Steganography: Morgan Kaufmann Publishers, 2008

[14] R. F. C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," Proceedings of the IEEE, vol. 90, pp. 64-77, 2002

[15] L. Jian and H. Xiangjian, "A Review Study on Digital Watermarking," in Information and Communication Technologies, 2005. ICICT 2005. First International Conference on, 2005, pp. 337-341.

[16] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," Proceedings of the IEEE, vol. 90, pp. 64-77, 2002

[17] J.-S. Pan, H.-C. Huang, and l. C. Jain, Eds., Intelligent Watermarking Techniques (Series on Innovative Intelligence. World Scientific, 2004

[18]Y. Yusof and O. O. Khalifa, "Digital watermarking for digital images using wavelet transform," in Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference on, 2007, pp. 665-669

[19]C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," Proceedings of the IEEE, vol. 90, pp. 64-77, 2002.

[20] 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.

[21] 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

[22] K.P. Soman, K.I. Ramachandran- “Insight into Wavelets from, Theory to Practice”.

[23] JiangXuehua, “Digital Watermarking and Its Application in Image Copyright Protection”, International Conference on Intelligent Computation Technology and Automation, 2010.

[24] TamiratTagesseTakore, 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

[25] Darshana Mistry, "Comparison of Digital watermarking methods", (IJCSE) International journal on Computer Science and Engineering Vol. 02, No. 09, 2010.

[26] 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.

[27] 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

[28] Chunlin Sone, Sud Sudirman, MadjidMerabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images", School of Computing and Mathematical Science, Liverpool John Moores University, UK

[29] Santi P. Maitya,Malay K. Kundub (2008), "DHT domain digital watermarking with low loss in image informations," International journal of electronics and communications

[30] Martin Kutter and Fabien Petitcolas (1999), "Fair Benchmark for Image Watermarking Systems", In Proceedings of SPIE Security and Watermarking of Multimedia Contents, volume 3657, pages 226, 239