www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11237-11245

A Review on Digital Watermarking Techniques, Applications and Attacks

Ms. Komal M.Shukla[1], Mr. Ashish K.Mehta[2]

1M.E. Student, B.H.Gardi College of Engineering & Technology,
Rajkot, Gujarat, India
komalmshukla@gmail.com

2Asst, Professor, B.H.Gardi College of Engineering & Technology,
Rajkot, Gujarat, India
akmehta@gardividyapith.ac.in

Abstract: In today's digital world, in every field there is massive use of digital contents. Digital documents can be copied and scattered easily to large numbers of people without any cost. People can download audio, image and video files, and they can share them with friends and they can influence or change their original contents. Due to this, there is more probability of copying of such digital information. So, there is an urgent need of prohibiting such illegitimate copyright of digital media. Digital watermarking (DWM) is the dominant solution to this problem. This paper aims to provide an exhaustive survey of digital watermarking techniques especially focuses on image watermarking types and its applications in today's world.

Keywords: Watermarking, Techniques, Applications, Attacks.

1. Introduction

The immeasurable attractiveness of the World Wide Web in the early 1990s established the commercial potential of offering multimedia resources through the digital networks. Since copying a digital data is very simple and swift too so, issues like, shelter of rights of the content and proving ownership, arises. Digital watermarking has been anticipated as one approach to carry out this. Digital watermarking came as a technique and a device to conquer shortcomings of existing copyright laws for digital data. Digital watermarking is a process in which owner identification (watermark) is embedded into the digital media at the sender end and later at the receiver end the embedded information is extracted to recognize the real owner/identity of the digital content.

The remaining parts of the paper are as follows:

- Section-2 describes the background of digital watermarking, and then we discuss the concept, classification of digital watermarking. It also describes the properties and architecture of watermarking
- Section-3 describes the various watermarking techniques
- Section-4 describes the watermarking applications.
- Section-5 describes the various possible attacks on the watermarks.

Some general terms and definitions are used in the area of watermarking presented below [2].

- Section-6 describes disadvantages of digital watermarking.
- Section 7 describes the various metrics used to evaluate the performance of the watermarked image

2. OVERVIEW OF DIGITAL WATERMARKING

Watermarking is defined as the procedure of embedding a message, text, logo or signature into a digital signal. Digital signal may be image, audio file, video or any other work of media. The field of digital watermarking is gaining popularity as a research topic in the letter half of the 1990s. When and how watermarking is used first is the topic of discussion but it can used at Bologna, Italy in 1282 .at first it is used in paper mills as paper mark of company. After that watermark is also used in currency notes of any country [1].Fig 1 shows an example of watermark on Indian currency

Fig. 1. Example of watermark on Indian currency[1]

Watermark (noun): The data that are provided to be hidden. The word watermark (verb) also refers to the process of embedding information, often similar to an actual watermark on paper.

Cover Media: The media that carries or hosts the watermark. Sometimes the expression original or host media is used.

Watermarked Data: The media which contains the watermark.

Embedding: The process of inserting the watermark into the original media.

Extraction: The process of extracting the embedded watermark from the watermarked data.

Detection: The procedure used for detecting whether the given media contains the watermark or not.

Watermarking: is the whole scheme of embedding and extraction.

Noise: This is defined as any unwanted component in the signal, introduced for example during transmission or through thermal processes.

Attack: The artificial process used, intentionally or non-intentionally, which modifies the watermarked data and destroys or alters the watermark in the data.

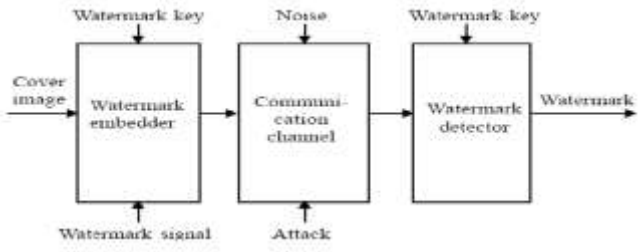

Fig. 2. Digital Watermarking System[10]

2.1 Classification of Digital Watermarking

There are different classifications of digital watermark algorithms.

2.1.1According to characteristics/robustness

a) Robust: Robustness watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, and the watermark is not destroyed after some attack and can still be detected to provide certification. It resists various attacks, geometrical or non-geometrical without affecting embedded watermark [3].

b) Fragile: Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking [3].

c) Semi fragile: Semi fragile watermarking is capable of tolerating some degree of the change to watermarked image, such as the addition of quantization noise from lossy compression[3].

2.1.2According to attached media/host signal

a) Image watermarking: This is used to hide the special information into the image and to later detect and extract that special information for the author‘s ownership. Maintaining the Integrity of the Specifications [3].

b) Video watermarking: This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method requires real time extraction and robustness for compression [3].

c) Audio watermarking: This application area is one of the most popular and hot issue due to internet music, MP3 [3].

d) Text watermarking: This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces[3].

e) Graphic watermarking: It embeds the watermark to 2D or 3D computer generated graphics to indicate the copyright [3].

2.1.3According to attached media/host signal

a) Visible watermark: The watermark that is visible in the digital data like stamping a watermark on paper, (ex.) television channels, like HBO, whose logo is visibly superimposed on the corner of the TV picture[3].

b) Invisible watermarking: There is technology available which can insert information into an image which cannot be seen, but can be interrogated with the right software. You can‘t prevent the theft of your images this way, but you can prove that the image that was stolen was yours, which is almost as good[3].

2.1.4According to its purpose:

There are classified into four categories [3]

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

b) Tampering tip watermarking: It protects the integrity of the image content, labels the modified content and resists the usual lossy compression formats.

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

d) Anonymous mark watermarking: It can hide important annotation of confidential data and restrict the illegal users to get confidential data.

2.1.5According to watermark type:

There are classified into two categories [3].

a) Noise type: Noise type has pseudo noise, Gaussian random and chaotic sequences.

b) Image type: There are binary image, stamp, logo and

label.

2.1.6 According to domain:

a) Spatial domain: This domain focuses on modifying the pixels of one or two randomly selected subsets of images. It directly loads the raw data into the image pixels. Some of its algorithms are LSB; SSM Modulation based technique [3].

b) Frequency domain: This technique is also called transform domain. Values of certain frequencies are altered from their original. There are several common used transform domain methods, such as DCT, DWT, and DFT [3].

Table I. Comparison between spatial domain & frequency domain [3 4 5]

Factors	Spatial Domain	Frequency Domain
Computational Cost	Low	High
Robustness	Fragile	More Robust
Perceptual quality	High control	Low control
Computational complexity	Low	High
Computational Time	Less	More
Capacity	High	Low
Example of Application	Mainly Authenticati on	Copy rights

2.1.7 According to detection process:

a) Visual watermarking: It needs the original data in the testing course, it has stronger robustness, but its application is limited [3].

b) Semi blind watermarking: It does not require an original media for detection [3].

c) Blind watermarking: It does not need original data, which Has wide application field, but requires a higher watermark technology [3].

2.1.8 According to use of keys:

a) Asymmetric watermarking: This is technique where different keys are used for embedding and detecting the watermark[3].

b) Symmetric watermarking: Here same keys are used for embedding and detecting the watermark [3].

2.2 Watermarking Properties

Watermarking need some desirable properties based on the application of the watermarking system [3].
Some of the properties are presented here:

a) Effectiveness: This is the most important property of watermark that the watermark should be effective means it should surely be detective. If this will not happened the goal of the watermarking is not fulfilled[1].

b) Host Signal Quality: This is also important property of watermarking. Everybody knows that in watermarking, watermark is embedded in host signal (image, video, audio etc.). This may put an effect on the host signal. So the watermarking system should be like as, it will minimum changes the host signal and it should be unnoticeable when watermark is Invisible[1].

c) Watermark Size: Watermark is often use to owner identification or security confirmation of host signal and it always use when data is transmitted. So it is important that the size of watermark should be minimum because it will increases the size of data to be transmitted[1].

d) Robustness: Robustness is crucial property for all Watermarking systems. There are so many causes by which watermark is degraded, altered during transmission, attacked by hackers in paid media applications. So watermark should robust, So that it withstand against all the attacks and threats [1].

3. WATERMARKING TECHNIQUES

Digital image watermarking techniques can be broadly classified into two major categories:
a) Spatial Domain Watermarking
b) Frequency Domain Watermarking

3.1 Spatial Domain:

Spatial domain digital watermarking algorithms directly load the raw data into the original image [4].Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Spatial domain is manipulating or changing an image representing an object in space to enhance the image for a given application. Techniques are based on direct manipulation of pixels in an image [6]. Some of its main algorithms are as discussed below [3]:

3.1.1 Least Significant Bit:

The earliest work of digital image watermarking schemes embeds watermarks in the LSB of the pi pixels. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (i.e., least significant) bit, of selected pixels of the image. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. For instance, an attacker could simply randomize all LSBs, which effectively destroys the hidden information. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications [7].

3.1.2 SSM Modulation Based Technique:

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

pseudo noise signal that is modulated by the embedded watermark [7].

3.1.3Texture Mapping Coding Technique:

This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage) [4], and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture [3].

3.1.4Patchwork Algorithm:

Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems Journal, 1996[8]. It is based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch an image data is brightened where as that of patch B is darkened (for purposes of this illustration this is magnified). The following are the steps involved in the Patchwork algorithm [3]:

- Generate a pseudo-random bit stream to select pairs of pixels from the cover data.
- For each pair, let d be the difference between the two pixels.
- Encode a bit of information into the pair. Let d < 0 represent 0 and d > 0represent Given that the pixels are not ordered correctly, swap them.
- In the event that d is greater than a predefined threshold or if is equal to 0, ignore the pair and proceed to the next pair. Patchwork being statistical methods uses redundant pattern encoding to insert message within an image.
- Correlation-Based Technique: In this technique, a pseudorandom noise (PN) pattern says W(x, y) is added to cover image I(x,y).

  $$IW(x, y) = I(x, y) + k*W(x, y) \quad (1)$$

  Where K represent the gain factor, IW represent watermarked image ant position x, y and I represent cover image. Here, if we increase the gain factor then although it increases the robustness of watermark but the quality of the watermarked image will decrease[3].

3.2 Frequency Domain

Frequency Domain methods are broadly applied than to Spatial Domain methods. The aim of this technique is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients[7]. Frequency domain watermarking provides more information hiding capacity and high robustness against various geometrical attacks. Frequency domain watermarking is more robust than spatial domain watermarking due to the embedding of watermark into the altered frequency coefficients of the transformed image [10 12]. Some of its well-known algorithms are discussed below [4]:

3.2.1Discrete Fourier Transform (DFT):

Transforms a continuous function into its frequency components [10]. It provides robustness against geometric attacks like scaling, cropping, rotation, translation etc. DFT of an original image is generally complex valued, which results in the magnitude and phase representation of an image. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform. DFT is resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, these are normalized coordinates, there is no synchronization are needed [33].

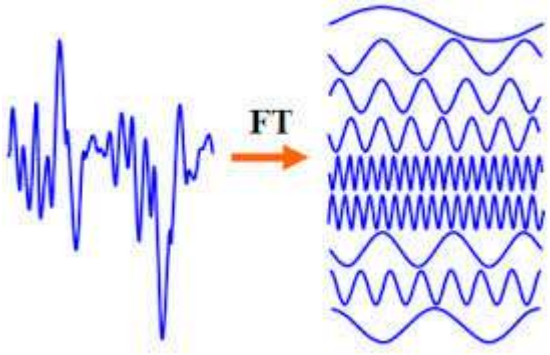

Fig. 3. The action of the Fourier Transform

3.2.2 Discrete Cosine Transform(DCT):

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image[3].

The first efficient watermarking scheme was introduced by Koch et al. In their method, the image is first divided into square blocks of size 8x8 for DCT computation [13] as shown in the Fig. 4[10].

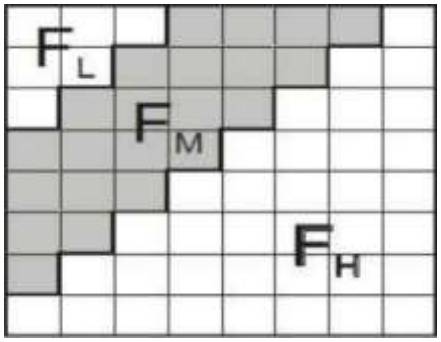

Fig. 4. DCT Coefficients[10]

In general, the DCT coefficients are divided into three bands (sets), namely low frequencies, middle frequencies and high frequencies. Fig. 4visualizes these bands. Low frequencies (FL) are correlated with the illumination conditions and high frequencies (FH) represent noise and small variations (details). Middle frequencies (FM) coefficients contain useful information and construct the basic structure of the image. Middle frequencies FM is chosen to embed the watermark as the embedding of watermark in a middle frequency band does not scatter the watermark information to most visual important parts of the image i.e. the low frequencies. It does not overexpose them to removal through compression and noise attacks where high frequency components are targeted [10 14 15].

Steps in DCT Block Based Watermarking Algorithm [16]

1) Segment the image into non-overlapping blocks of 8x8

2) Apply forward DCT to each of these blocks

3) Apply some block selection criteria (e.g. HVS)

4) Apply coefficient selection criteria (e.g. highest)

5) Embed watermark by modifying the selected coefficients.

6) Apply inverse DCT transform on each block

3.2.3 Discrete Wavelet Transform (DWT):

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called Wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL)[3]. DWT is the multi resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution [17]. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges [18].In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub- bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands – LL3, LH3, HL3, HH3.This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band. The three-level DWT decomposition is shown in Fig.5 [10]

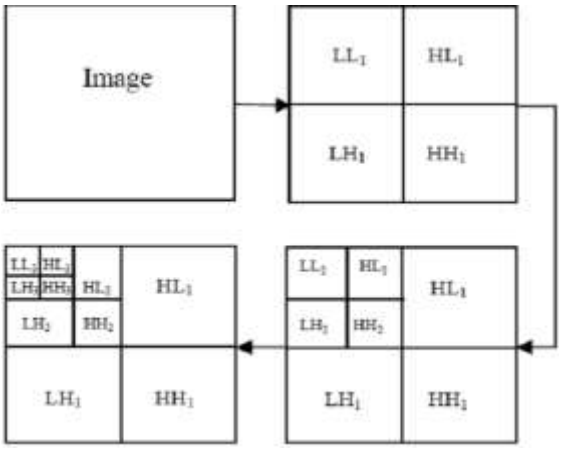

Fig. 5. 3-level discrete wavelet decomposition[10]

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well [10 19]. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well [19]. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image [20]. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies [21].

Table II. Comparisons of different watermarking techniques [3 4 6 22]

Algorithm	Advantages	Disadvantages
LSB	1.Easy to implement and understand 2.Low degradation of image quality 3. High perceptual transparency.	1. It lacks basic robustness 2.Vulnerable to noise 3.Vulnerable to cropping, scaling
Correlation	1. Gain factor can be increased resulting in increased robustness	1. Image quality gets decreased due to very high increase in gain factor.
Patchwork	1. High level of Robustness against most type of attacks	1. It can hide only a very small amount of information.
Texture mapping coding	1. This method hides data within the continuous random texture patterns of a picture.	1. This algorithm is only suitable for those areas with large number of arbitrary texture images
DCT	1. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	1. Block wise DCT destroys the invariance properties of the system. 2. Certain higher frequency components tend to be suppressed during the quantization step.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception.	1. Cost of computing may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames.
DFT	1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions	1.Complex implementation 2. Cost of computing may be higher.

4. Digital watermarking applications

Watermarking technologies is applied in every digital media whereas security and owner identification is needed [2 23]. A few most common applications are listed hereby.

4.1 Owner Identification:

The application of watermarking to which he developed is to identify the owner of any media. Some paper watermark is easily removed by some small exercise of attackers. So the digital watermark was introduced. In that the watermark is the internal part of digital media so that it cannot be easily detected and remove [2].

4.2 Copy Protection:

Illegal copying is also prevent by watermarking with copy protect bit. This protection requires copying devices to be integrated with the watermark detecting circuitry [2].

4.3 Broadcast Monitoring:

Broadcasting of TV channels and radio news is also monitoring by watermarking. It is generally done with the Paid media like sports broadcast or news broadcast [2].

4.4 Medical Applications:

Medical media and documents also digitally verified, having the information of patient and the visiting doctors. These watermarks can be both visible and invisible. This watermarking helps doctors and medical applications to verify that the reports are not edited by illegal means [2].

4.5 Fingerprinting:

A fingerprinting is a technique by which a work can be assigned a unique identification by storing some digital information in it in the form of watermark. Detecting the watermark from any illegal copy can lead to the identification of the person who has leaked the original content. In cinema halls the movies are played digitally through satellite which has the watermark having theater identification so if theater identification detected from a pirated copy then action against a theater can be taken[2].

4.6 Tamper proofing:

Digital watermarks which are fragile in nature can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content [2].

4.7 Image and content authentication:

In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. One example of digital signature technology being used for image authentication is the trustworthy digital camera [2 24].

4.8 Media Forensics

Forensic watermark applications enhance a content owner's ability to detect and respond to misuse of its assets. Forensic watermarking is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner and the people or companies with which it shares its content [2].

4.9 Locating Content Online

The volume of content being uploaded to the web continues to grow as we rely more and more on the Internet for information sharing, customer engagement, research and communication. It has also become a primary sales tool and selling environment, providing an opportunity to showcase our products or services and attract buyers from around the world [2].

4.10 Audience measurement

In this new media world of insatiable content consumption, audience measurement is becoming more and more critical. Beyond the hard numbers of how many people are accessing a program, understanding who is watching, how they engage with the content, when, where and through which media is essential for content providers, advertisers and broadcasters to better tailor their offerings and maximize impact[2].

5. Attacks on watermarking system

There are two main categories of Watermark Attacks [25]: Non-Intentional Attacks and Intentional Attacks.

5.1 Non-Intentional Attacks

Non-Intentional Attacks refer to those attacks, which are not imposed by an attacker. This class of attack is introduced mainly during the transmission of the media. For example, the embedded watermark will be lost if the image is compressed with JPEG codec, printed to paper (D/A conversion); the audio is recorded to a analog tape; noise addition when using wireless transmission, etc. Any watermarking techniques must be robust to this class of attack, since the media must be distributed from the content owner to the end user with some means of transmission [25].

5.1.1 Attacks induced by transmission

Noise is always introduced to the media when transmit through an analogue channel. Examples are analogue transmission of TV/Radio signal, printing a watermarked image on paper, etc. However, noise is not a serious attack to most of the digital watermarking techniques, unless the noise is large compared to the host signal. Assume M'=M+W+n, where n is the noise. M'• W = M • W+W• W+n• W. Since W • W is much larger than M • Wand n • W, the detection of the watermark is still success. Geometric transformation is another common attack induced during transmission. Transformation like shift, rotation, scaling, shearing, etc., would lead to the desynchronization of the detector with the embedded watermark. This is true for both cases of which the watermark is inserted to spatial domain or the frequency domain. This kind of attack is also used commonly by attacker intentionally, since one or two degrees of rotation is not detectable for human eye. However, this little rotation could make the watermark detection fail [25].

5.1.2 Digital Compression

Media files are always transmitted from distributors to end-users in a compressed format, since this kind of files are usually very large in size (especially video and audio files). However, most of these compressions are lossy compression. In such a situation, the embedded watermark will be removed or partly removed; especially those are inserted to the high frequency portion of the signal, since common lossy compression removes the high frequency part of the original signal. Cox [26] proposed to embed the watermark to the perceptual significant part of the media, in order to make the watermark to be robust to compression and other filtering attacks (since removing such a watermark will also degrade the host media). On the other hand, this introduced another challenge for the watermarking design, which is how to maintain the invisibility or inaudibility of the watermark [25].

5.2 Intentional Attacks

Intentional Attacks can be further sub-categorized to [27]: Detection Disabling Attacks, Removal Attacks and Ambiguity Attacks

5.2.1 Detection Disabling

Detection Disabling Attack aims at making the correlation detector, which is a common detector, fail to detect or extract the watermarked info. This class of attacks also knows as Geometric Attack, because many attacks in this class are achieved with geometric distortion like zooming, shifting in spatial or temporal domain, rotation, shearing, cropping, sub-sampling, removal or insertion of pixels, or any other kinds of geometric transformations. Since this class of attack does not remove the watermark info from the media, by using more sophisticate watermarking techniques may be able to recover the watermark from the attacked media, like *[25 28 29]*.

5.2.2 Removal Attacks

Removal Attack aims at destroying or removing the watermark or part of the watermark from the watermarked signal, such that the correlation detector cannot extract the watermark or the resultant score of the detection is lower than the threshold. For invertible watermarking techniques, attacker can look into the watermark insertion or extraction algorithm in the present of the inserter or the detector. Once the attacker figures out how the watermarking process is, a simple inversing processing can completely remove the watermark from the watermarked signal. Attacks like denoising, certain non-linear filtering operations, compression/decompression, statistical averaging, bit-by-bit removal, etc., can also diminishing the watermark, such that the output score of the detector is lower than the threshold [25].

5.2.3 Ambiguity Attacks

Ambiguity Attack refers to those attacks to the watermarking scheme or system, instead of the watermarking algorithm/techniques. Most of these attack origin from the question "What is a watermark?" One can watermark a

watermarked signal again with the same or different watermarking technique, such that it is unclear which the first and authoritative watermark of the owner is. Some techniques proposed to make a fake original from the watermarked signal, with the presence of the detector. Attackers can also easily to false the watermark detector in some access control system, which use watermark to store the access control information [30]. Sometimes we refer these kinds of attack to "deadlock problem", "IBM attacks" [31] and "confusion attacks". In the case of proving the ownership of the media, an even more simple attack which can apply is to pick some bits randomly from the watermarked or non-watermarked signal, apply an arbitrary function to it and claim that it is the watermark of the attacker. This problem exists because there is no answer to the question, "What is a digital watermark? [25].

6. Disadvantages of digital watermarking

Watermarks keep people from stealing photographs or illustrations from websites; online auctions and image hosts. They add copyright protection and can encourage interested parties to purchase the image instead of using it with an assumption that your labour is free. Increase the odds of making money off a photograph or illustration with watermarks that help a potential buyer identify who owns the image, but don't forget to consider the disadvantages of using watermarks before you make the decision to add them to our work [32].

6.1 Obscures Image

Worthwhile watermarks need to obscure the image just enough to make it unusable. Key areas of the illustration or photograph may end up hidden. Unless your photograph or illustration features strong color and composition, your image's appeal may suffer after the addition of a watermark as key areas are hidden beneath the watermark. Good watermarks protect the image without obscuring its appeal: they're often faint but visible enough to be intimidating [32].

6.2 Easy to Remove

Over-sized watermarks cover larger areas of an image and obscure the image's clarity. Small watermarks, on the other hand, can easily be removed with the assistance of image-editing software. To overcome these disadvantages, some people place mid-sized watermarks in places where the watermark covers nothing but an irrelevant area of an image, such as on a white background near a bottom corner. Unfortunately, this solution can't beat the thieves who will simply crop out the watermark. Great watermarks have intricate but faint detail that span a large portion of the image. Such watermarks are the hardest to remove [32].

6.3 Limited Protection

Professional watermarking services provide invisible but limited digital protection. Advanced watermarking technology that embeds ownership information into photographs or illustrations enable the use of search services to help you find incidents of unlawful use of your images. Unfortunately, professional watermarking search services may not be able to find images when they sit behind firewalls, in Flash-enabled galleries, and database-driven or password-protected websites [32].

6.4 Time Consuming

Adding watermarks to your work can be time consuming. If you are already selling large volumes of images, consider if watermarking is worth the time it takes to add them to all of your images. Unless you integrate watermarking into your work-flow, manually adding watermarks to hundreds of images may rob you of valuable time. Automating the watermarking process with a dedicated application may be worth spending money on, especially if you plan to produce, watermark and display lots of images [32].

7. Performance evaluation matric

In order to evaluate the quality performance of the watermarked images, there are some quality measures such as PSNR and MSE

- **Mean square error** (MSE):
  Mean Square Error between original image and watermarked image is calculated as follows:

$$\text{MSE} = 1/XY\left[\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j)-e(i,j))\text{^}2\right] \quad (2)$$

  Where,
  X and Y are height of the image.
  C (i, j) is the pixel value of the cover image.
  e (i, j) is the pixel value of the embed image [3 22]

- **Peak Signal to Noise Ratio (PSNR) :**
  PSNR is used to compare difference between the original and the watermarked image. Larger the PSNR value, more similar is watermarked image to the original image. This image quality metric is defined in decibels as:

$$PSNR = 10\ log10\ \frac{(255\times255)}{MSE} \quad (3)$$

  If the PSNR value is greater than 30dB then the perceptual quality is acceptable [10].

8. Conclusion

In this Paper, we have offered various aspects of digital image watermarking in terms of overview, watermarking techniques, attacks, applications, performance analysis. Apart from it a brief and comparative investigation of watermarking techniques is presented with their advantages and disadvantages. In this paper we tried to give the complete information about the digital watermarking

which will help the new researchers to get the maximum alertness in this domain.

References

[1] Lalit Kumar Saini,A Survey of Digital Watermarking Techniques and its Applications,International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014

[2] Feng-Hsing Wang, Jeng-Shyang Pan, Lakhmi C Jain, Innovations in Digital Watermarking Techniques, Springer, 2009, ISBN: 978-3-642-03186-1 (Print) 978-3-642-03187-8 (Online)

[3] Prabhishek Singh,A Survey of Digital Watermarking Techniques, Applications and Attacks,International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013

[4] Jiang Xuehua, ?Digital Watermarking and Its Application in Image Copyright Protection?, 2010 International Conference on Intelligent Computation Technology and Automation.

[5] Mahmoud El-Gayyari, ?Watermarking Techniques Spatial Domain Digital Rights Seminar ©?, Media Informatics University of Bonn Germany

[6] CHAPTER 2: LITERATURE REVIEW, Source: Internet

[7] Manpreet Kaur,A study of digital image watermarking ,IJREAS Volume 2, Issue 2 (February 2012) ISSN: 2249-3905

[8] http://ippr-practical.blogspot.in

[9] Manpreet kaur, Sonia Jindal, Sunny behal, A Study of Digital image watermarking?, Volume2, Issue 2, Feb 2012

[10] Ms.Jalpa M.Patel,A brief survey on digital image watermarking techniques ,International Journal For Technological Research In Engineering Volume 1, Issue 7, March-2014

[11] DP Kaur, J Kaur, K Deep," Digital Image Watermarking: Challanges and Approach for a Robust Alorithm", International Journal of Electronics Engineering, 1(1), 2009, pp. 95-97.

[12] Chirag Sharma, Deepak Prashar, " DWT based robust technique of watermarking applied on digital Images", International Journal of Soft Computing and Engineering (IJSCE),Volume-2,Issue-2,May 2012

[13] Lin Liu, "A Survey on Digital Watermarking Techniques

[14] Liwei Chen, Mingfu Li,"An Effective Blind Watermark Algorithm Based on the DCT", IEEE, Proceedings of the 7th World Congress Intelligent Control and Automation, June 2008, Chongquing, China.

[15] A. Hanaa , M. hadhoud, and A. Shaalan, "A Blind Spread Spectrum Wavelet Based Image Watermarking Algorithm" International Conference on Computer Engineering &Systems, pp. 251-256, 2009

[16] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, A Survey of Digital Image Watermarking Techniques?, 2005 3rd IEEE International conference on Industrial Informatics (INDIN).

[17] Xiao Jun Kang Li Jun Dong, "Study of the Robustness of Watermarking Based on Image Segmentation and DFT", IEEE International Conference on Information Engineering and Computer Science, ICIECS, 2009, pp1-4.

[18] Vaishali S. Jabadeand and Dr. Sachin R. Gengaje,"Literature Review of Wavelet Based Digital Image Watermarking Techniques", International Journal of Computer Applications, vol. 31–No.1, October 2011.

[19] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University "Watermarking with Wavelets: Simplicity Leads to Robustness", Southeastcon, IEEE, pages 587 – 592, 3-6 April 2008

[20] G. Bouridane. A, M. K. Ibrahim, Digital Image Watermarking Using Balanced Multi wavelets?, IEEE Transaction on Signal Processing 54(4), (2006), pp. 1519-1536.

[21] Cox, I.J.; Miller, M.L.; Bloom, J.A., Digital Watermarking,Morgan Kaufmann, 2001.

[22] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, A Novel Technique for Digital Image Watermarking in Spatial Domain, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[23] Mei Jiansheng, Li Sukang, "A Digital Watermarking Algorithm Based On DCT and DWT", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107

[24] Edin Muharemagic and Borko Furht A Survey of watermarking techniques and applications 2001.

[25] K. F. Tsang,A Review on Attacks, Problems and Weaknesses of Digital Watermarking and the Pixel Reallocation Attack,Security and watermarking of Multimedia COntents III, Ping Wah Wong, Edward J.Delp III, Editors, Procedding of SPIE Vol.4314(2001)@2001

[26] I.J. Cox, J. Killian, F.T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans.on Image Processing, Vol. 6, No. 12, pp.1673-87, Dec 1997.

[27] F. Hartung, J.K. Su, B. Girod, "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks", Proc. of SPIE Conf. on Security and Watermarking of Multimedia Contents, Vol. 3657, pp. 147-158, Jan 1999.

[28] M. Kutter, "Watermark Resisting to Translation, Rotation and Scaling", Proc. of SPIE Multimedia System and Applications, Vol. 3528, pp. 423-431, Nov 98.

[29] J.J.K. O'Ruanaidh, T. Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking ", Proc. of IEEE Int.Conf. on Image Processing,Vol. 1, pp.536-9, 1997.

[30] I.J. Cox, M.G. Linnartz, "Some General Methods for Tampering with Watermarks" IEEE Journal on Selected Areas in Communications,Vol. 16, No. 4, pp. 587-593, May 1998

[31] S. Craver, N. Memon, B.L. Yeo, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations,Attacks, and Implications",IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 573-586, May 1998.

[32] Kusuma Kumari B. M,A Survey of Digital Watermarking Techniques and its Applications,International Journal of Science and Research (IJSR),Volume 2 Issue 12, December 2013

[33] Vinita Gupta,A Review on Image Watermarking and Its Techniques,International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 1, January 2014

[34] G. Coatrieux, L. Lecornu, Members "A Review of digital image watermarking in health care", ,Ch. Roux, Fellow IEEE, B. Sankur, Member, IEEE