ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

A Survey of Digital Watermarking Techniques, Applications and Attacks

Prabhishek Singh, R S Chadha

Abstract— ***The expansion of the Internet has frequently increased the availability of digital data such as audio, images and videos to the public. Digital watermarking is a technology being developed to ensure and facilitate data authentication, security and copyright protection of digital media. This paper incorporate the detail study watermarking definition, concept and the main contributions in this field such as categories of watermarking process that tell which watermarking method should be used. It starts with overview, classification, features, framework, techniques, application, challenges, limitations and performance metric of watermarking and a comparative analysis of some major watermarking techniques. In the survey our prime concern is image only.***

Index Terms—**Applications, Attacks, Challenges, Techniques, Watermarking.**

I. INTRODUCTION

The term 'digital watermarking' was first appeared in 1993, when Tirkel presented two watermarking techniques to hide the watermark data in the images [1]. The success of the Internet, cost-effective and popular digital recording and storage devices, and the promise of higher bandwidth and quality of service for both wired and wireless networks have made it possible to create, replicate, transmit, and distribute digital content in an effortless way. The protection and enforcement of intellectual property rights for digital media has become an important issue [2]. Digital watermarking is that technology that provides and ensures security, data authentication and copyright protection to the digital media. Digital watermarking is the embedding of signal, secret information (i.e. Watermark) into the digital media such as image, audio and video. Later the embedded information is detected and extracted out to reveal the real owner/identity of the digital media. Watermarking is used for following reasons, Proof of Ownership (copyrights and IP protection), Copying Prevention, Broadcast Monitoring, Authentication, Data Hiding. Watermarking consists of two modules watermark embedding module and watermark detection and extraction module. Digital watermarking technology has many applications in protection, certification, distribution, anti-counterfeit of the digital media and label of the user information. It has become a very important study area in information hiding. This paper analyzes the key technologies of digital watermarking and explores the application in the digital image copyright protection. The paper is organized as follows:

- Section 2 describes the background of digital watermarking, and then we discuss the concept, classification and analysis of digital watermarking techniques according different criteria such as host signal, perceptivity, robustness, watermark type, necessary data for extraction, processing domain, applications and use of keys. It also describes the features, requirement, and architecture of watermarking and various styles of watermarks as well.
- Section 3 describes the various watermarking techniques and presents the comparative analysis of the algorithms with their advantages and disadvantages.
- Section 4 describes the watermarking applications.
- Section 5 describes the various possible attacks on the watermarks.
- Section 6 describes challenges and limitations over digital watermarking.
- Section 7 describes the various metrics used to evaluate the performance of the watermarked image.

II. DIGITAL WATERMARKING TECHNOLOGY

As an emerging technology, digital watermarking involves the ideas and theories of different subject coverage, such as signal processing, cryptography, probability theory and stochastic theory, network technology, algorithm design, and other techniques [3]. Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author's serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenario.

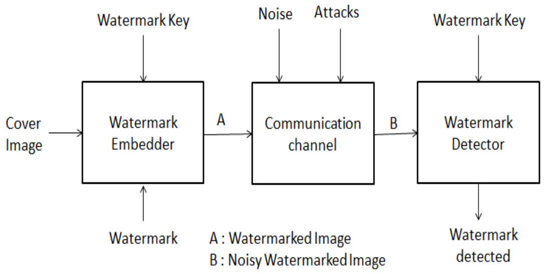

Fig 1. Digital Watermarking system

A. Classification of Digital watermarking

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

1) According to characteristics/robustness

- **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.
- **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.
- **Semi fragile:** Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise from lossy compression.

2) According to attached media/host signal

- **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.
- **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.
- **Audio watermarking*:*** This application area is one of the most popular and hot issue due to internet music, MP3.
- **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.
- **Graphic watermarking:** It embeds the watermark to 2D or 3D computer generated graphics to indicate the copyright.

3) According to perceptivity:

- **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.
- **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.

4) According to its purpose:

- **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.
- **Tampering tip watermarking:** It protects the integrity of the image content, labels the modified content and resists the usual lossy compression formats.
- **Anti-counterfeiting watermarking**: It is added to the building process of the paper notes and can be detected after printing, scanning, and other processes.
- **Anonymous mark watermarking**: It can hide important annotation of confidential data and restrict the illegal users to get confidential data.

5) According to watermark type:

- **Noise type:** Noise type has pseudo noise, Gaussian random and chaotic sequences.
- **Image type:** There are binary image, stamp, logo and label.

6) According to domain:

- **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.
- **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.

Table I. Comparison between Spatial Domain And Frequency Domain [3] [20]

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

7) According to detection process:

- **Visual watermarking**: It needs the original data in the testing course, it has stronger robustness, but its application is limited.
- **Semi blind watermarking**: It does not require an original media for detection.
- **Blind watermarking*:*** *It* does not need original data, which has wide application field, but requires a higher watermark technology.

8) According to use of keys:

- **Asymmetric watermarking:** This is technique where different keys are used for embedding and detecting the watermark.
- **Symmetric watermarking:** Here same keys are used for embedding and detecting the watermark.

B. Features of Digital watermarking

Various features of watermarking are as follows,

- **Robustness:** Robustness refers to that the watermark embedded in data has the ability of surviving after a variety of processing operations and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack.

- **Imperceptibility*:*** Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits. It can be detected by an authorized agency only. Such watermarks are used for content or author authentication and for detecting unauthorized copier.
- **Security:** A watermark system is said to be secure, if the hacker cannot remove the watermark without having full knowledge of embedding algorithm, detector and composition of watermark. A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection.
- **Verifiability:** Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.
- **Capacity and data payload*:*** Capacity of the watermarking system is defined as the maximum amount of information that can be embedded in the cover work. The number of watermark bits in a message in data payload and the maximum repetition of data payload within an image is the watermark capacity. Depending on the application some watermarking methods require a data payload exceeding 10,000 bits. A watermark may have high data capacity but low data payload.
- **Computational cost:** In order to reduce computational cost, a watermarking method should be less complex. Watermarking methods with high complex algorithms will require more software as well as hardware resources and thus incur more computational cost. Computational simplicity usually preferred in resource-limited environments like mobile devices.
- **Watermark detection reliability**: To model robust watermarking in a copyright protection scenario, we can use a watermark that consists of a pseudo-random binary sequence to represent the identity of a copyright holder. The correlation value between the identity and a correctly detected watermark is usually very high compared to the correlation value between the identity and randomly chosen watermark. In this case a graph of correlation values plotted against watermarks has a significant peak at the correctly detected watermark which corresponds to the copyright holder's identity. This is watermark detection outcome.

For a given image with watermark embedded, there are 2 possible results of its watermark detection:

✓ The successful detection of the watermark is called a true positive.

✓ The unsuccessful detection of the watermark is called a false negative.

Likewise, for a given cover image (or un-watermarked test image), there are 2 possible results of its watermark detection:

✓ The absence of watermark is called a true negative.

✓ An incorrectly detected watermark causes a false positive (a.k.a false alarm)

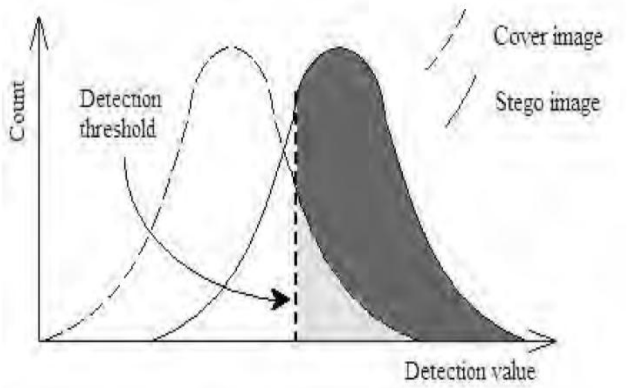

Fig 2. Distribution of Watermark Detection Values for Cover and Stego Images. The Sum Of The Lightly Shaded And Heavily Shaded Areas Is A Probability Of True Positive. [21]

- **Blind or non-blind detection of watermark**: A watermarking technique is said to be blind, if it does not require original image to recover the watermark from the watermarked image. Conversely, a watermarking technique is said to be non-blind, if it needs original image for extracting the watermark from the watermarked image. The blind technique is also referred as oblivious. The non-blind watermarking systems are more robust than blind watermarking systems due to availability of original cover image at the time of detection. However, blind or oblivious watermarking systems are more popular. The oblivious watermarking systems decrease the overhead of cost and memory for storing original images.
- **Tradeoff between performance factors:** A basic principle of watermarking is to exploit redundancy in images for embedding the watermark information. Given the fact that many of the existing image compression algorithms are not perfect, watermarking is made possible by embedding extra information in the redundant parts. In addition, enhancing watermark robustness normally requires more image distortions and increased redundancy. This causes lower imperceptibility and more likely to be removed under malicious attacks.

C. Requirements of Digital watermarking

There are a number of important characteristics that a watermark can exhibit, Jalil and Mirza (2010), Bandyopadhyay and Paul (2010). The most important properties of digital watermarking techniques are transparency, robustness, security, capacity, invert ability (reversibility) and complexity and possibility of verification. *Transparency* relates to the properties of the human sensory. A transparent watermark causes no artifacts or quality loss.

- **Robustness:** Robustness means Resistance to "blind", non-targeted modifications, or common media operations. For example the Stirmark or Mosaik tools attack the robustness of watermarking algorithms with geometrical distortions. For manipulation recognition the watermark has to be fragile to detect altered media. There are two major problems when trying to guaranty robustness; the watermark must be still present in the media after the transformation or it must be still possible for the watermark detector to detect it.

When a signal is distorted, its fidelity is only preserved if its perceptually significant regions remain intact, while perceptually insignificant regions might be drastically changed with little effect on fidelity.

- **Security:** Security describes whether the embedded watermarking information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector, except the key, and the knowledge of at least one watermarked data. Watermarking security implies that the watermark should be difficult to remove or alter without damaging the host signal. As all watermarking systems seek to protect watermark information, without loss of generality, watermarking security can be regarded as the ability to assure secrecy and integrity of the watermark information, and resist malicious attacks [5].
- **Capacity:** Capacity describes how many information bits can be embedded. It addresses also the possibility of embedding multiple watermarks in one document in parallel. Capacity requirement always struggle against two other important requirements, that is, imperceptibility and robustness (Fig 3). A higher capacity is usually obtained at the expense of either robustness strength or imperceptibility, or both.

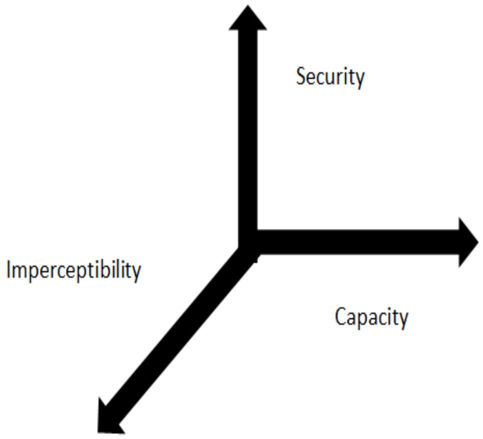

Fig 3.The Tradeoffs among Imperceptibility, Robustness, and Capacity

- **Imperceptibility**: The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. The term "imperceptible" is widely used in this case. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal, Gonzalez and Woods (2008). It is then important to develop techniques that can be used to add imperceptible or unnoticeable watermark signals in perceptually significant regions to counter the effects of signal processing.
- **Modification and Multiple Watermarks*:*** Changing a watermark can be accomplished by either removing the first watermark or then adding a new one, or Inserting a second watermark. The first alternative goes against the principle of tamper resistance, because it implies that a watermark is easily removable. Allowing multiple watermarks to coexist is the preferred solution. There is however security problem related to the use of multiple watermarks. The basis of watermarking security should lie on Kirchhoff's assumption that one should assume that the method used to encrypt the data is known to the unauthorized party. It means that watermarking security can be interpreted as encryption security leading directly to the principle that it must lie mainly in the choice of the embedded key. Allows insertion of multiple, independently detectable watermarks in an Image.
- **Invertibility:** Invertibility describes the possibility to produce the original data during the watermark retrieval. The optimization of the parameters is mutually competitive and cannot be clearly done at the same time. If we want to embed a large message, we cannot require large robustness simultaneously. A reasonable compromise is always a necessity. On the other hand, if robustness to strong distortion is an issue, the message that can be reliably hidden must not be too long.

D. Architecture of Digital watermarking

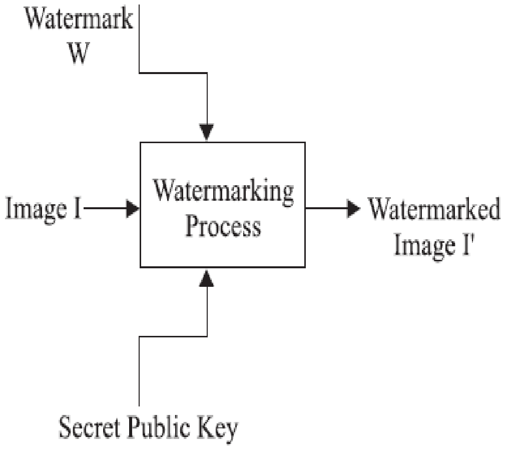

Fig 4. Simple Digital Watermarking [6]

Simple Digital watermarking is a technology in which a watermark (secret information) is hidden in the digital media using an appropriate algorithm for the authentication and identification of original owner of the product. Outcome we get is watermarked image. Simple digital watermarking technique consists of two modules watermark embedding module and watermark detection and extraction module. Watermark embedding embeds the watermark into the original image using a key. The watermark embedding module is as Fig5.

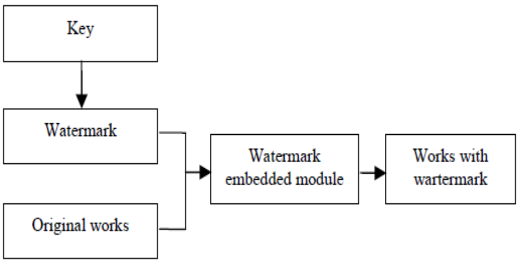

Fig 5. Watermark Embedding Module [3]

Watermark detection and extraction module is used to determine whether the data contains specified watermark or the watermark can be extracted. The watermark embedding module is as Fig 6.

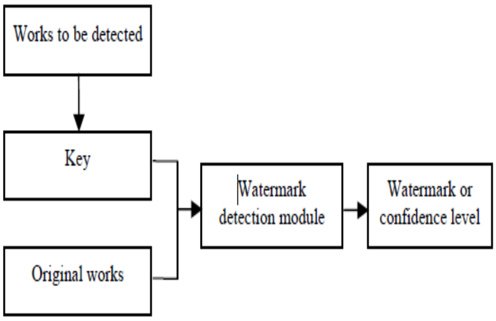

Fig 6. Watermark Detection and Extraction Module [3]

E. Styles of Robust Watermarks

There various types of styles watermarks, some of them are discussed in this survey. [10]

- **Noise Watermark:** Noise watermark is most commonly used type of robust watermark. For the reason of security and statistical undetectivity, it is demonstrated that the watermark is most secure, if it is in the form of Gaussian random sequence. To measure the similarity between original and extracted sequence, the correlation value is used to indicate the similarity.
- **Logo Watermark:** Logo is another form of robust watermark. The logo is small image pattern in binary form. It can be company logo used in commercial applications. The quality of logo image is measured by human perception. That is, it is subjective measure of verifying authenticity of the digital content.
- **Message Watermark:** Message watermark is comprised of text. Message watermark has the advantage of easy to use in comparison with noise-type watermark or logo watermark. However, the message watermark require bit error rate approaching to zero, because any bit error will cause major fault in the final result. In most cases it is required that information with at least 64 bit (or 8 ASCII character can be carried by multimedia)

III. WATERMARKING TECHNIQUES

Watermarking is the method to hide the secret information into the digital media using some strong and appropriate algorithm. Algorithm plays a vital role in watermarking as, if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can only destroy or detect the secret information if he know the algorithm otherwise it is critical to know the watermark. There are various algorithms present in the today scenario that are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain.

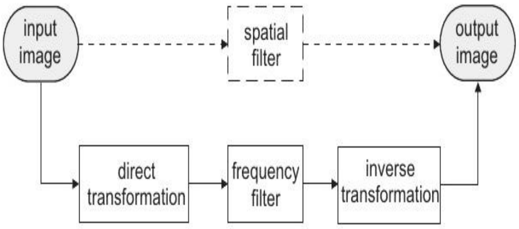

Fig 7. Brief Idea of Spatial and Frequency Domain [19]

Spatial domain: Spatial domain digital watermarking algorithms directly load the raw data into the original image [3]. 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 [10]. Some of its main algorithms are as discussed below:

Additive Watermarking: The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low [10].

Least Significant Bit: Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks.

The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image.

But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed.

Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.

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. 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.

Texture 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) [3], and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.

Patchwork Algorithm: Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems Journal, 1996[11]. 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 A 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:

- 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).

$I_w(x, y) = I(x, y) + k*W(x, y)$

Where K represent the gain factor, I_w 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.

Frequency domain: Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim 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 [13]. Some of its main algorithms are discussed below:

Discrete cosine transforms (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.

Steps in DCT Block Based Watermarking Algorithm [22]

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

Discrete wavelet transforms (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). 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 [14]. 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 [14]. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image [16]. 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 [17].

Advantages of DWT over DCT: Wavelet transform understands the HVS more closely than the DCT.

Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution. [22]

Disadvantages of DWT over DCT: Computational complexity of DWT is more compared to DCT'. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient [22]

Discrete Fourier transform (DFT): Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. 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.

Advantages of DFT over DWT and DCT: DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions. [22]

Table II. Comparisons of Different Watermarking Techniques [3] [10] [18]

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	1. Image quality gets

	increased resulting in increased robustness	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.

IV. DIGITAL WATERMARKING APPLICATIONS

- **Copyright protection:** Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.
- **Copy protection:** Digital content can be watermarked to indicate that the digital content cannot be illegally replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content.
- **Digital right management:** Digital right management (DRM) can be defined as “the description, identification, trading, protecting, monitoring, and tracking of all forms of usages over tangible and intangible assets”. It concerns the management of digital rights and the enforcement of rights digitally.
- **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.
- **Broadcast monitoring:** Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters.
- **Fingerprinting:** Fingerprints are the characteristics of an object that tend to distinguish it from other small objects. As in the applications of copyright protection, the watermark for finger printing is used to trace authorized users who violate the license agreement and distribute the copyrighted material illegally. Thus, the information embedded in the content is usually about the customer such as customer's identification number.
- **Access control:** Different payment entitles the users to have different privilege (play/copy control) on the object. It is desirable in some systems to have a copy and usage control mechanism to prevent illegal copy of the content or limit the number of times of copying. A robust watermark can be used for such purpose.
- **Medical application:** Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster [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 [8].
- **Annotation and privacy control:** Multi-bit watermarking can be used to annotate an image. For example, patient records and imaging details related to a medical image can be carefully inserted into the image. This would not only reduce storage space but also provides a tight link between the image and its details. Patient privacy is simply controlled by not keeping the sensitive information as clear text in human readable form, and the watermark can be further secured by encryption. Other usages of annotation watermarking are electronic `document indexing and automated information retrieval.
- **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.
- **Communication enhancement:** Today's smart phones are becoming the handheld computing device we carry with us 24/7 — no longer are they merely for talking or texting. More and more we look to our mobile phones to provide us with assistance, instant information, and to entertain us.
- **Content protection for audio and video content***:* Modern digital formats employed for sale or rental of commercial audio and video content to consumers-such as DVD, Blu-Ray Disc, and iTunes-incorporate content protection technologies that control access to and use of the

content and limit its unauthorized copying and redistribution. Parties seeking to engage in unauthorized distribution and copying of protected commercial music or video content must circumvent the content protection to obtain a decrypted copy of the content.

- **Content filtering:** The lean-back experience of watching television has radically changed over the last few years. Today people want to watch content in their own time and place. The proliferation of set top boxes (STB) in homes evidences this, as people want to watch video on demand or on a time-shifted schedule. Today, more than a device to watch films/series, sports or even play games, the STB has become an interactive device providing multiple services.
- **Communication of ownership and objects***:* Digital content continues to proliferate as today's consumers seek information and entertainment on their computers, mobile phones and other digital devices. In our cyber culture, digital has become a primary means of communication and expression. The combination of access and new tools enables digital content to travel faster and further than ever before as it is uploaded, dispersed, viewed, downloaded, modified and repurposed at breathtaking speed. Whether you are a global media corporation or a freelance photographer, the ability to communicate your copyright ownership and usage rights is essential.
- **Document and Image security:** Consider documents and images that are generated in support of a major product launch. Corporate communications professionals face significant challenges in managing these assets through very complex sales and marketing channels. Images and documents are distributed to remote offices, agencies, distributors, dealers and more, and must be managed to ensure confidential information is not leaked before the launch date.
- **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.
- **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.
- **Improved auditing***:* Media content of all types - television, music, movies, etc. - continues to proliferate and make its way onto many new consumer devices as well as many sites across the internet. Digital watermarking applications for auditing give all members within the value chain the ability to verify usage to support highly accurate billing and contract enforcement.

Table III. The Planning and Control Components. [9]

Application Class	Purpose of the embedded watermark	Application Scenarios
Protection of Intellectual Property Rights	Convey information about the content ownership and intellectual property rights	- Copyright Protection - Copy Protection - Fingerprinting - Signature
Content Verification	Ensures that the original digital document has not been altered, and/or helps determine the type of alteration	- Authentication - Integrity Checking
Information Hiding	Represents side channel used to carry additional information	- Broadcast Monitoring - System - Enhancement

V. WATERMARKING ATTACKS

There are various possible malicious intentional or unintentional attacks that a watermarked object is likely to subject to. The availability of wide range of image processing soft wares made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is prevent the watermark from performing its intended purpose. A brief introduction to various types of watermarking attacks is as under,

- **Removal Attack:** Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal.
- **Interference attack:** Interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging, and noise storm are some examples of this category of attacks.
- **Geometric attack:** All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.
- **Low pass filtering attack:** A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.
- **Forgery attack:** The forgery attacks that result in object insertion and deletion, scene background changes are all tantamount to substitution.
- **Security Attack:** In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. The watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged.
- **Protocol Attack:** The protocol attacks do neither aim at destroying the embedded information nor at disabling the

detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermark's implementation. Consequently, a robust watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one media into another without knowledge of the secret key.

- **Cryptographic attacks:** Cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack [7]. In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.
- **Active Attacks:** Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control for example.
- **Passive Attacks:** In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not. Cox et al (2002) suggest that, protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one want to grant.
- **Collusion Attacks:** In collusive attacks, the goal of the hacker is the same as for the active attacks but the method is slightly different. In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in fingerprinting applications *(e.g.* in the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be pretty important.
- **Image Degradation:** These type of attacks damage robust watermarks by removing parts of the image. The parts that are replaced may carry watermark information. Examples of these operations are partial cropping, row removal and column removal. Insertion of Gaussian noise also comes under this category, in which the image is degraded by adding noise controlled by its mean and its variance.
- **Image Enhancement:** These attacks are convolution operations that desynchronize the watermark information in an image. These attacks include histogram equalization, sharpening, smoothing, median filtering and contrast enhancement.
- **Image Compression:** In order to reduce the storage space and cut the cost of bandwidth required for transmitting images, images are generally compressed with JPEG and JPEG2000 compression techniques. These lossy compression methods are more harmful as compared to lossless compression methods. Lossless compression methods can recover the watermark information with inverse operation. However lossy compression techniques produce irreversible changes to the images. Therefore probability of recovering watermarked information is always very low.
- **Image Transformations:** These types of attacks are also called synchronization attacks or geometrical attacks. The famous software Stir Mark uses small local geometrical distortions to invalidate watermark detection. Geometrical attacks include rotation, scaling and translation also called RST attacks. Some researchers focus on RST robustness while designing the robust watermarking systems, because it is fundamental problem. Besides RST transforms, image transformations also include other transforms such as aspect ratio change, shearing, reaction and projection [10].

VI. CHALLENGES AND LIMITATIONS OF DIGITAL WATERMARKING

There are various technical challenges in watermarking research. The robustness and imperceptibility trade-off makes the research quite interesting. To attain imperceptibility, the watermark should be added to the high frequency components of the original signal. On the other hand, for robustness the watermark can be added to the low frequency components only. Thus, the watermarking scheme can be successful if the low frequency components of the original signal are used as the host for watermark insertion. In this section, we discuss the various technical issues related to watermarking, such as properties of the human visual system and spread-spectrum communication, which are commonly exploited for making watermarking schemes successful. [13]

A. Properties of visual signal:

Since image and videos are visual signals, it is necessary to understand the behavior of visual signals in order to find ways to hide additional information in them. Visual signals are generally recognized as amplitude plots, intensity versus space displays of image information and intensity versus space and time displays of video scenes. These waveforms reveal a lot of information about the properties of the signals. Some of the properties of visual signals are listed:

- **Non-stationary:** Non stationary property is common to all signals. Image and video signals contain a wealth of segments of flat or slowly changing intensity, as well as edges and textured regions. While the edges need to be preserved to maintain perceptual quality, the textured regions need to be judiciously used to store additional information
- **Periodicity:** There exists line to line and frame to frame periodicity in image and video signals. They are not exactly periodic but there exists redundancy between frames and lines. These redundancies are exploited in any compression scheme, and need to be considered during the watermarking process.

B. Properties of Human Visual System

The success of any watermarking scheme lies in making the best use of the human visual system (HVS). In this section, we discuss the various properties of the human visual system which are exploited in designing watermarking algorithms. Texture sensitivity: The visibility of distortion depends on the background texture. The distortion visibility is low when the background has a strong texture. In a highly textured image block, energy tends to be more evenly distributed among the different DCT coefficients. In a flat-featured portion of the image the energy is concentrated in the low frequency components of the spectrum. This indicates that in strong texture regions more watermark signal can be added.

- **Brightness sensitivity***:* The human eye is sensitive in perceiving a low intensity signal in the presence of backgrounds of different intensity. As the surrounding region intensity is increased, the relative intensity in dark areas is reduced and the sensitivity in the light areas is increased. When the mean value of the noise square is the same as that of the background, the noise square tends to be most visible against a mid-grey background. This characteristic is known as Weber's law. This means that the eye has high sensitivity at low intensity levels and greatly reduced sensitivity at high intensity levels.

VII. PERFORMANCE EVALUATION METRIC

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

The **MSE (mean square error)** is defined as average squared difference between a reference image and a distorted image. It is calculated by the formula given below

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

X and Y are height and width respectively of the image. The c (i, j) is the pixel value of the cover image and e (i, j) is the pixel value of the embed image. [18]

SNR (Signal to Noise ratio) measures the sensitivity of the imaging. It measures the signal strength relative to the background noise. It is calculated by the formula given below, [23]

$$\text{SNR}_{\text{dB}} = 10\log_{10}\left(\frac{P_{\text{signal}}}{P_{\text{noise}}}\right)$$

The PSNR (peak signal to noise ratio) is used to determine the degradation in the embedded image with respect to the host image. It is calculated by the formula as

$$\text{PSNR} = 10\log_{10}(L*L/MSE)$$

L is the peak signal value of the cover image which is equal to 255 for 8 bit images. [18]

The **BER (bit error ratio)** is the ratio that describes how many bits received in error over the number of the total bits received. It is calculated by comparing bit values of embed and cover image.

$$\text{BER} = P/\ (H*W)$$

H and W are height and width of the watermarked image. P is the count number initialized to zero and it increments by one if there is any bit difference between cover and embed image. [18]

VIII. CONCLUSION

In this paper we have presented various aspects for digital watermarking like overview, framework, techniques, applications, challenges and limitations. Apart from it a brief and comparative analysis of watermarking techniques is presented with their advantages and disadvantages which can help the new researchers in related areas. We also tried to classify the digital watermarking in all the known aspects like robustness, host signal, perceptivity, purpose, watermark type, domain, detection process and use of keys. In this paper we tried to give the complete information about the digital watermarking which will help the new researchers to get the maximum knowledge in 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] Christine I. Podilchuk, Edward J. Delp, "Digital watermarking: Algorithms and applications", IEEE Signal processing Magazine, July 2001.

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

[4] Ensaf Hussein, Mohamed A. Belal, "Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey", IJERT, ISSN: 2278-0118, Vol. 1 Issue 7, September-2012.

[5] C.-T. Li and F.M. Yang., "One-dimensional Neighborhood Forming Strategy for Fragile Watermarking". In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.

[6] Rakesh Ahuja, S S Bedi, Himanshu Agarwal, "A Survey of Digital Watermarking Scheme", MIT International Journal of Computer Science and Information Technology, Vol.2, No. 1, Jan. 2012, pp.(52-59)

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

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

[9] Jahnvi Sen, A.M. Sen, K. Hemachandran," AN ALGORITHM FOR DIGITAL WATERMARKING OF STILL IMAGES FOR COPYRIGHT PROTECTION", Jahnvi Sen et al / Indian Journal of Computer Science and Engineering IJCSE).

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

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

[12] www.scisstudyguides.addr.com

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

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

[15] D. Kundur, D. Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication", in proceeding of the IEEE, (1999), pp. 1167-1180.

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

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

[18] 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.

[19] http://www.digimarc.com.

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

[21] Chaw-Seng WOOS, "Digital Image Watermarking Methods for Copyright Protection and Authentication".

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

[23] http://en.wikipedia.org/wiki/Signal_to_noise_ratio_(imaging)

AUTHOR'S PROFILE

Mr. Prabhishek Singh received his B.Tech in CSE from G.B.T.U Lucknow, Uttar Pradesh, India in 2010.Currently, he is doing M.Tech in CSE from C-DAC Noida(Affiliated to G.G.S.I.P.U New Delhi), India. He is working on the project "**Digital Image Watermarking by Patchwork Method using Image Segmentation**". His interest areas are Digital Image Processing, Operating Systems, and DBMS.

Mr. Ramneet Singh Chadha is an Assistant.Prof, MTech Head and currently working as Project Manager, in Health Informatics group. He has more than 12 years of domain expertise in Health care domain and has been closely involved in Design, Development and Implementation of e-Sushrut HMIS Software, since his joining C-DAC in 1997. He has interest in interoperability of hospitals for setting up NHIN using HL7 standards; cloud computing and telemedicine and other research area is health domain