

Introduction

1.1 Overview of the research topic:

The revolutions and advent in internet technology has resulted in many new opportunities for creating and delivering the contents in digital form with increasing use transmitted information's via internet, we need to protect information's such as: image, audio, video files and so on. We discuss in this research how to protect image your by adding watermarks to them. The Purpose is, to prevent every person who might be using your image without your permission.

Digital image watermarking is one of the most widely used techniques for protection of ownership rights of digital images. Appeared on banknotes and important documents with the aim to protect them against forgery.

There are many Techniques that applied to the field of digital watermarking this increase needs in watermarking methods appear as a result of a growing number of attacks against watermarking systems.

A digital watermark could be used either source based or destination based. From the application point of view, source based watermarks are used for authentication or ownership identification.

According to the type of document, watermarking techniques can be divided into four categories: they are text watermarking, image watermarking, audio watermarking and video watermarking.

Right now, digital watermarking is an active and leading area of research.

1.2 Background:

The term ‘digital watermarking’ first appeared in 1993, when (Tirkel) presented two watermarking techniques to hide the watermark data in the images. The success of the Internet digital storage devices and quality of service it possible to create, transmit, and distribute digital content in an easy way.

The growth of e-commerce applications in the World Wide Web also requires the need to increase the security of data communications over the internet. To provide security to these applications and the protection and enforcement of intellectual property rights for digital media, data encryption and information hiding techniques were introduced & developed. Digital watermarking is a technology that provides and ensures security, data authentication and copyright protection to the digital media.

Digital Watermarking is the process of embedding data called a watermark (also known as Digital Signature or Tag or Label) into the digital media (such as text, image, audio and video) such that watermark can be detected or extracted later to make an assertion about the object. For example, information about copyrights, ownership, timestamps, and the legitimate receiver could be embedded. Digital watermarking by itself prevent copying, modification, and re-distribution of documents.

However, if encryption and copy protection fail, watermarking allows the document to be traced back to its rightful owner of unauthorized use. Digital watermarking Enters in many areas including signal processing, telecommunications, cryptography, Medicine, and law. Watermarking is used for Proof of Ownership (copyrights and protection), Copying Prevention, Broadcast Monitoring, Authentication and Data Hiding.

Images make up a major component of multimedia content. Examples of images are digital arts, illustrative diagrams, and cultural heritage paintings in digitized form and digital photographs. Advances in computing hardware, software, and networks have created threats to copyright protection and content integrity. For instance, images can be copied, modified, and distributed easily. Digital watermarking is a potentially good tool in enabling content protection. Encryption can offer confidentiality and integrity in content protection, and the decrypted content can be further protected using digital watermarks.

The watermarking process embeds a signal into the image without significantly degrading its visual quality. Then the image can be made public or sent to the end user. Later, the detected watermark can be used for the purposes of copyright protection and content authentication.

Copyright protection concerns the positive identification of content ownership in order to protect the rights of the owner. Robust watermarks can be used in copyright protection because they are persistently associated with an image. Attempts to remove the watermark should result in severe degradation of the image's visual quality. The detection of a watermark in an image can be used to identify the copyright holder.

1.3 Problem statement:

The motivation for taking up “Digital Watermarking in Images” as topic for this research is a new field of security and important in verifying from digital information scattered wide on the internet. Protection of digital multimedia content has become an increasingly important issue for content owners. Watermarking is identified as a major means to achieve copyright protection. Digital watermarking gives real owner the ability to check if a file is an unauthorized copy or if it has been modified.

Within the development of digital watermarking technique, methods of watermarking attacks have been developed for deleting or modifying to improve illegal copying. In this research We will use technique is developed for hiding digital watermarking into a image in a way that satisfied hiding which includes every part of image, to protect it proposed to resolve this so that a watermark is hidden in the image as a token of ownership. But the intelligent attacker performed various attacks on the image to destroy the watermark this motivated us to think on the robust techniques which resist various attacks.

We decided to work on watermarking techniques we found that there was a scope of improvement in these techniques we will use technique Discrete Wavelet Transform (DWT).

An important issue arises for the protection of the rights of all participants it has been recognized and current laws of copyright protections are inadequate for dealing with digital data.

Therefore it was necessary to solve this problem and develop protection mechanisms.

1.4 Research Objectives:

Driven by the urgent need to protect the digital image content that is being widely and wildly distributed and shared through the Internet by an ever-increasing number of users the field of digital watermarking has witnessed an extremely fast-growing development since its inception. The main purpose of digital watermarking, information embedding and data hiding systems is to embed auxiliary information.

Copyright protection concerns the positive identification of content ownership in order to protect the rights of the owner. Robust watermarks can be used in copyright protection because they are persistently associated with an image. Attempts to remove the watermark should result in severe degradation of the image's visual quality. The detection of a watermark in an image can be used to identify the copyright holder. On the other hand content authentication is the validation of content integrity.

Digital watermarking hides in images the information necessary for ownership identity to offer copyright Protection and authentication.

Copyright Protection: for the protection of the intellectual property, the data Owner can embed a watermark representing copyright information in the data.

The embedded watermark can be used as a proof, e.g. in a court if someone Intentionally infringed the copyrights.

The main objective of this thesis is:-

- 1-Protect images by adding watermarks to them.
- 2-To provide protection copyright and ownership.
- 3-Protect images from fraud.
- 4-understand techniques authentication and protection digital image.

1.5 Methodology:

There are many ways to protect images, watermarking is probably the most effective and it's simple to use.

- Implement it used Matlab is the software that we will use to represent the system.
- An DWT Techniques is the Technique that will use to embedding and extraction watermark
- Mean Square error (MSE), Peak Signal to Noise Ratio (PSNR), the Parameters that will use to measure the quality of the image.

1.6 Research scope:

Research activities in digital image watermarking have become more specialized. Therefore, it is important to identify the focus of study. In this thesis, investigate of robust the watermark, semi-fragile watermarking, and hybrid methods. In addition, we also examine hybrid methods that combine the advantages of robust and semi-fragile watermarks For example, a watermark embedded in an image can be used to provide information web-based.

The printed image can be captured using a camera-phone, and the detected watermark is sent to a web server in order to retrieve extra information associated with the image. This technology could be useful in linking advertisements in printed magazines and time-sensitive materials on web servers. This strategy offers cross-media promotional coverage and content updates. The areas that contribute to the development of digital watermarking include the following:

A) Information and Communication Theory.

B) Signal Processing.

C) Digital image Processing.

Each of these areas deals with a particular aspect of the digital watermarking problem we also need to consider trade-off between watermark properties that have conflicting characteristics.

1.7 Contribution:

The research process started with a thorough literature survey on image watermarking methods for copyright protection and content authentication.

Our research work has the following contributions the major outcomes of this research are:

- Study and understand the digital watermarking.
- The development method and Techniques of a watermarking.
- We have performed a complete survey on the watermarking technologies.
- To increase the fidelity and quality of the watermarked image.
- We compare the proposed Techniques with the existing scheme in different aspects and discuss the advantages and the disadvantages of our Techniques.

1.8 Thesis out line:

This research is organized as 5 chapters:

- Chapter (1) overview of the research topic and problem statement and research objectives.
- Chapter (2) digital watermarking and properties of digital watermarks and Application of watermarking and watermarking techniques.
- Chapter (3) Methodology and Algorithm Performance.
- Chapter (4) Simulation Environments and Flow chart for this system.
- Finally, Chapter (5) Conclusion and Recommendation.

2.1 Introduction:

Due to enhancement of information technology distribution of digital data is become very easy. Increasing in development, increases security threads of data it is important issue to protect multimedia data from many attacks such as counterfeiting, piracy and malicious maniple. To provide solution to many attacks number of mechanism used, digital watermarking is one of them. Watermark-It is a label, a tag, an information container which insert into multimedia data to make original data secure from illegal manipulation and distribution. It can be visible or invisible [5].

With the widespread distribution of digital information over the World Wide Web (WWW) the protection of intellectual property rights has become increasingly important. These information, which include still images, video, audio, or text are stored and transmitted in a digital format. Information stored in digital format can be easily copied without loss of quality and efficiently distributed. Because of easy reproduction, retransmission and even manipulation, it allows a pirate (a person or organization) to violate the copyright of real owner. The design of techniques for preserving the ownership of digital information is in the basic of the development of future multimedia services.

2.2 Digital watermarking:

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. The outcome of this is the watermarked image [6].

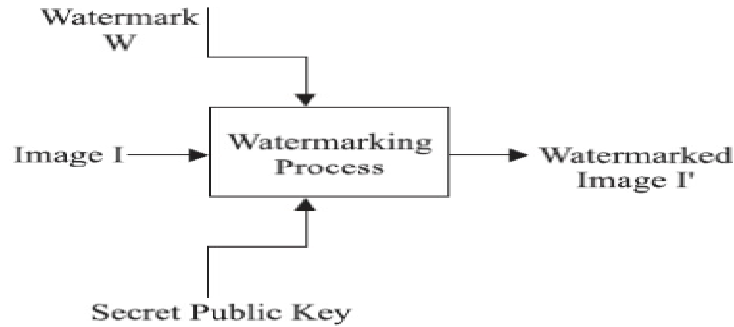


Fig 2.1: Simple Digital Watermarking

Watermarking is a key process in the protecting copyright ownership of electronic data including image, videos, audio.....etc.

2.3 Watermarking process:

Digital watermarking is a very developing field and used in various applications which have been proved to be successful. The digital watermarking has been applied in a number of image processing techniques. The aim of every application is to providing security of the digital content.

Every digital watermarking technique includes two algorithms: one as the embedding algorithm and other as the detecting algorithm. These two processes are same for all the type of watermarking techniques. Figure (2) shows the watermark embedding process in which the watermark is embedded in the cover image by using the embedding algorithm. And Figure(3) shows the watermark detection process in which the embedded watermark is recovered by using the detection algorithm.

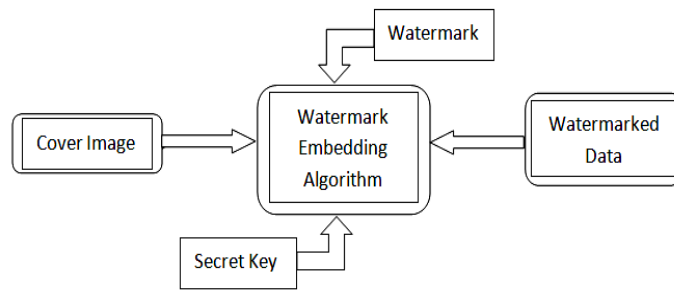


Fig2.2: Watermark Embedding Process

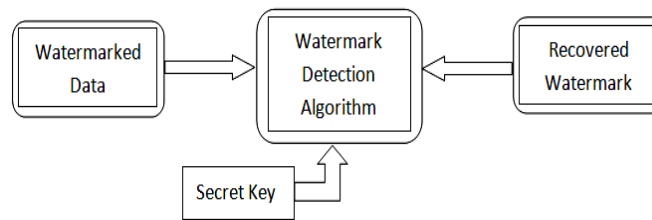


Fig2.3 Watermark Detection Process

2.4 Classification of watermarking:

Watermarking techniques can be classified into the following four categories according to the type of the multimedia document to be watermarked:

- Text Watermarking: Watermark is embedding into text file.
- Image Watermarking: Watermark is embedding into image.
- Audio Watermarking: Watermark is embedding into audio file.
- Video Watermarking: Watermark is embedding into video file.

2.5 Digital watermarks are of three types as follows:

- Visible watermark.
- Invisible watermark.
- Dual watermark.

The visible watermark appears visible to a casual viewer on a careful inspection.

Invisible-robust watermark is so embedded that alterations made to the pixel. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image causes the watermark destruction, or alteration.

The dual watermark is a combination of the visible and the invisible watermarks. In this type of watermarks an invisible watermark is used as a backup for the visible watermark [7].

Watermarking is either “visible” or “invisible” of ownership or authenticity has been in the form of stamps, seals, signatures or classical watermarks.

Digital watermarking is classified into various types this classification is based on several criteria all the classifications are described in following table:

Table (2.1) Types of watermarking basis of different Criteria

S.no	Criteria	Classification
1	Watermark Type	<ul style="list-style-type: none"> ➤ Image Watermarking. ➤ Text Watermarking. ➤ Audio Watermarking. ➤ Video Watermarking.
2	Robustness	<ul style="list-style-type: none"> ➤ Fragile: Easily Manipulated. ➤ Semi-Fragile: Resist from some type of Attacks. ➤ Robust: not affected from attack.
3	Domain	<ul style="list-style-type: none"> ➤ Spatial: LSB. ➤ Frequency: DWT, DCT, DFT.
4	Perceptivity	<ul style="list-style-type: none"> ➤ Visible Watermarking: Channel logo. ➤ Invisible Watermarking: like Steganography. ➤ Dual watermark.

2.6 Importance Digital Watermarks:

Today storing information and data such as image video and audio in digital formats is very common. For many people transferring digital files via the internet is a daily activity. Owing to the rapid development of digital technology and the wide spread use of the internet, accompanying this development more serious problems.

There are few approaches designed for protecting data and securing systems. One of them is data encryption (cryptography). Based on conventional

cryptographic system, parts of the data may be protected from an unauthorized person by applying any of existing cryptographic algorithms. Only a person who possesses appropriate key (or keys) can decrypt the encrypted data. The drawback of this data protection strategy is that once such a data is decrypted by a pirate, there is no way to protect the data and track the illegal distribution. Also it is impossible legally to prove the ownership. The next approach to protect the intellectual property rights is watermarking. Watermarking is a technique for embedding hidden data that attaches copyright protection information to digital information.

This provides an indication of ownership of the digital data on the other hand the watermarking requires that the hidden message should be robust to attempts aimed at removing it. In the case of copyright protection the copyright information should resist any modifications by pirates intending to remove it [8].

As is well known, due to the nature of digital information it is easy to make lossless copies from the original digital source to modify the content and to transfer the copies rapidly over the internet. Therefore the demands of copyright protection ownership demonstration and verifications for digital data are becoming more important among the solutions for these problems digital watermarking.

There are many kinds of watermarking techniques each of them provides different features and function which can be employed for different purpose for instance for verification a sender of a digital article can put before sending it . When the article is received an attempt is made to extract the hidden watermark.

Discuss Properties and applications of digital watermarking they will highlight the importance of digital watermarking.

2.7 Properties of Digital Watermarks:

Watermarking systems can be characterized by a number of defining properties in this section we highlight **6** of them. The relative importance of each property is dependent on the requirements of the application and the role the watermark will play. In fact, even the interpretation of a watermark property can vary with the application [9].

We begin by discussing a number of properties typically associated with a watermark embedding process:

2.7.1 Robustness: Watermark robustness is one of the major characteristics that influence the performance and applications of digital image watermark.

Robustness refers to the ability to detect the watermark after common signal processing operations. Watermark should be robust able to withstand compression, printing and scanning and many other operations.

Watermark robustness is one of the major characteristics that influence the performance and applications of digital image watermarks.

Watermarks can be categorized into three major groups based on their robustness: robust, fragile, and semi-fragile watermarks. Robust watermarks should be detected [10].

2.7.2 Fidelity: Watermarking is a process that alters an original image to add a message to it; therefore it inevitably affects the image's quality. We want to keep the image's quality to a minimum, so no obvious difference in the image's fidelity can be noticed.

2.7.3 Embedding Effectiveness: this is the important property. So probability of detection immediately after embedding this implies that a

watermarking system might have an effectiveness of less than 100%, 100% effectiveness is always desirable.

2.7.4 The payload size: Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload.

2.7.5 Security: Security of a watermark is the ability of the watermark to resist malicious attacks. These attacks include intentional operations of watermark insertion, modification, removal.

A hostile attack is any process specifically intended to thwart the watermark's purpose [10].

Unauthorized parties should not be able to read or alter the watermark.

Ideally, the watermark should not even be detectable by unauthorized parties.

2.7.6 Imperceptibility: The watermarked image should look like same as the original image to the normal eye. The viewer cannot detect that watermark is embedd.

To preserve the quality of the marked document, the watermark should not noticeably distort the original document.

Ideally, the original the performance of a given watermarking system can be evaluated on the basis of a set of properties. The relative importance of these properties depends on the application for which the system is designed.

2.8 Application of watermarking:

Recent years the phenomenal growth of the internet has highlighted the need for the mechanism to protect ownership of digital media. Digital Watermarking is a technique that provides a solution to the longstanding

problems faced with copyrighting digital data. Watermarking technologies is applied in every digital media where security and owner identification is needed. A few most common applications are listed.

2.8.1 Owner Identification:

The protection and enforcement of intellectual property rights for digital media has become an important issue.

Under law any original Work automatically holds copyright if copyright holders wanted to distribute their Works without losing any rights they had to include a copyright notice in every distributed copy.

2.8.2 Broadcast Monitoring:

Watermarking is an obvious alternative method of coding identification information for active monitoring.

Broadcast monitoring by embedding a watermark in commercial advertisements, an automated monitoring system can verify whether the Advertisements are broadcasted as contracted. Broadcast monitoring can protect not only the commercials but also the valuable TV products.

Nevertheless, there are a number of companies that provide watermark-based Broadcast monitoring services [8].

2.8.3 Proof of Ownership:

It is enticing to try to use watermarks not just to identify copyright ownership but to actually prove ownership because it can be so easily forged.

2.8.4 Content Authentication:

It is becoming easier and easier to tamper with digital Works in ways that are Difficult to detect For example, two image modifications made image is the original image other is the modified version. If this image were a critical piece of evidence in a legal case or police investigation, this form of tampering might pose a serious problem the same problem exists with audio and video.

2.8.5 Transaction Tracking:

In the literature on transaction tracking, the person responsible for misuse of a Work is sometimes referred to as a traitor we use the term adversary to describe anyone who attempts to remove, disable, or forge a watermark for the purpose of circumventing its original purpose.

Transaction tracking is more often called fingerprinting, as each copy of a Work can be uniquely identified by the watermark a human fingerprint that uniquely identifies a person. However, fingerprinting already refers to the detection and recognition of human fingerprints.

There are few technologies for transaction tracking For example, highly sensitive business documents, such as business plans, is sometimes printed on backgrounds Records are then kept about who have which copy. These marks are often referred to as “watermarks” [8].

2.8.6 Medical safety:

Watermarking technology has recently evolved in medical image watermarking as it can be used to hide the patients' information and then extract the information by the owner using certain private key.

Embedding the date and the patient's name in medical images could be Safety Patient Data [11].

2.8.7 Fingerprinting:

To trace the source of illegal copies, the owner can use the fingerprinting technique. In this case, the owner can embed different watermarks in the copies of the data that are supplied to different customers. Fingerprinting can be compared to embedding a serial number that is related to the customer's identity in the data. It enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third parties.

2.9 Watermarking Techniques:

Watermarking is the method used to hide the secret information into the digital media using some strong and appropriate algorithm. Algorithm plays a vital role in watermarking because 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 today's scenario that are used to hide the information. Those algorithms come into two domains Digital watermarking contains various techniques for

protecting the digital content. The entire digital image watermarking techniques always works in **two** domains:

- Spatial Domain.
- Transform domain.

2.9.1 Spatial Domain Watermarking:

The spatial domain techniques works directly on pixels. It embeds the watermark by modifying the pixels value. Most commonly used spatial domain techniques for example LSB.

The spatial domain represents the image in the form of pixels. The spatial domain watermarking embeds the watermark by modifying the values of some selected pixels.

The strength of the spatial domain watermarking is:

- Simplicity.
- Uncomplicated.
- Less time consuming.

The spatial domain watermarking is easier and its computing speed is high than transform domain but it is less robust against attacks. The spatial domain techniques can be easily applied to any image. The most important method of spatial domain is Lest Significant Bit (LSB) algorithm [13].

Techniques are based on direct manipulation of pixels in an image. Some of its algorithms are as discussed below:

One simple method that is not robust to the LSB encoding. LSB encoding is very simple and has been used for a variety of purposes. In this method the least significant bit of every component is replaced by the watermark information bit. This method can store quite some information, but the amount of information that can be embedded [10].

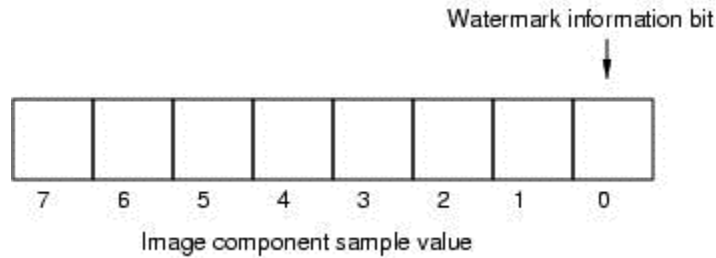


Fig 2.4: shows LSB embedded

2.9.2 Frequency Domain Watermarking:

In order to produce high quality image in the frequency or transform domain technique by first transmute the real image into the frequency domain by using DCT, DFT and DWT. It is applied to the selected frequencies of the real image because high signals will be lost during compression or scaling.

2.9.2.1 Discrete Cosine Transform (DCT):

Discrete Cosine Transform (DCT) used for the signal processing. It transforms a signal from the spatial domain to the frequency domain. DCT is applied in many fields like data compression, pattern recognition and every field of image processing. DWT watermarking is more robust as compared to the spatial domain watermarking techniques.

In DCT, for embedding the watermark information, we divide the image into different frequency bands. In Figure (5) FL denotes the lowest frequency component of the block, while FH denotes the higher frequency component and FM denotes the middle frequency component which is chosen as the embedding region. The Discrete cosine transform achieves good robustness against various attacks [13].

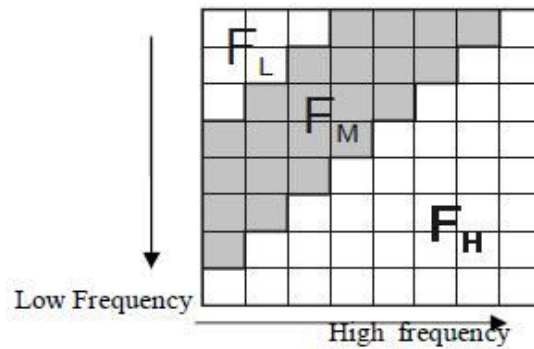


Fig 2.5: Discrete Cosine Transform

2.9.2.2 Discrete Fourier Transform (DFT):

Discrete Fourier Transform (DFT) offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT decomposes an image in sine and cosine form.

Depends on the mathematical equations is the development of the DWT, which we will use in this research.

2.9.2.3 Discrete wavelet transforms (DWT):

The Discrete Wavelet Transform (DWT) is a very useful tool for signal processing and image analysis especially in multi resolution representation. In DWT signals are decomposed into different components in the frequency domain. 1-D DWT Decomposes an input sequence into two components the average component and the detail component by calculations with a low-pass filter and a high-pass filter. Two dimensional discrete wavelet transform (2-D DWT) decomposes an input image into four sub-bands, one average Component (LL) and three detail components (LH, HL, LH ,HH). In image processing, the multi resolution of 2-D DWT has been employed to detect edges of an original image [15].

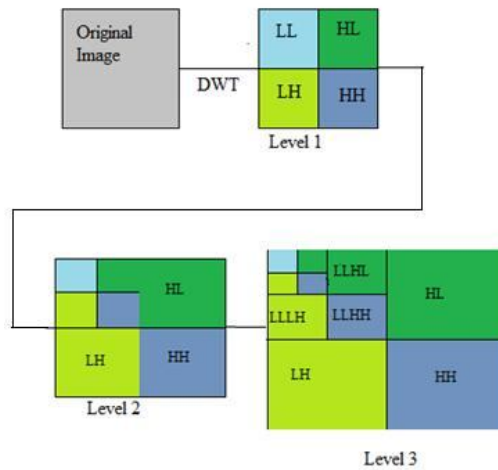


Fig 2.6: Discrete wavelet transforms

Table(2.2) Comparisons of Different Watermarking Techniques

Algorithm	Advantages	Disadvantages
LSB	<ol style="list-style-type: none"> 1. Easy to implement and understand. 2. Image quality of High. 	<ol style="list-style-type: none"> 1. It lacks basic robustness 2. Vulnerable to noise 3. Vulnerable to cropping, scaling.
DWT	<ol style="list-style-type: none"> 1. The watermark will not be removed by any kind of attack. 2. Higher compression. 	<ol style="list-style-type: none"> 1. Cost of computing may be higher. 2. Longer compression time.
DCT	<ol style="list-style-type: none"> 1. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected. 	<ol style="list-style-type: none"> 1. Block DCT destroys the properties of the system. 2. Certain higher frequency components tend to be suppressed during the quantization step.
DFT	<ol style="list-style-type: none"> 1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions. 	<ol style="list-style-type: none"> 1. Complex implementation 2. Cost of computing may be higher.

2.10 The important issues that arise in the study of digital watermarking techniques are [8]:

➤ ***Capacity :***

What is the optimum way to embed and then later extract this information?

➤ ***Robustness:***

How do we embed and retrieve data such that it would survive malicious or accidental attempts at removal?

➤ ***Security:***

How do we determine that the information embedded has not been tampered forged or even removed?

2.11 Literature review and previous studies:

2.11.1 Mohamed Ali HAJJAJI 2011: They present a new approach for watermarking of medical image that we are trying to adapt to telemedicine. This approach is intended to insert a set of data in a medical image. These data should be imperceptible and robust to various attacks. It's containing the signature of the original image, the data specific to the patient and his diagnostic. The purpose of the watermarking method is to check the integrity and preservation of the confidentiality of patient data in a network sharing. This approach is based on the use the LSB (least significant bits) of the image. Proposed watermarking of medical image, in which a set of numbers or data is inserted in a medical image. The watermarking method is based on the least significant bits (LSBs) in order to check the integrity and confidentiality of medical information and to maintain confidentiality for patient and hospital data. For 10% compression rate the watermark is successfully recovered.

The watermarking of image is an application in the medical image, on particular in the telemedicine domain. Indeed, given the significance and growth experienced by the practice of telemedicine, the watermarking may be proposed for contribute to the security of medical images Shared on the Internet.

They are interested in inserting a delicate watermarking whose objectives are to verify the integrity of the medical image and preserve the confidentiality of patient data.

This method is perfectly suited to medical imaging because it benefits from the use of least significant bits (LSBs) of the image, allowing you to insert the patient's own information while keeping a quality of the watermarked image [12].

2.11.2 Puneet Kr Sharma and Rajni 2012: The concept of Image watermarking mainly came into existence in 1990s because of the widespread of the Internet. At that time an invisible watermark message was inserted into a image which is to be transferred such that the invisible message will survive intended or unintended attacks. The first example of a technology similar to digital watermarking is a patent filed in 1954.

The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format. The information/logo are embedded in image is called a digital image watermark. The Information/logo where the watermark is to be embedded is called the image. The rapid advancement of internet has made it easier to send the data/image accurate and faster to the destination. But this advantage is also accompanied

With the disadvantage of modifying and misusing the valuable information through intercepting proposed image watermarking & different security issues. To hide logo (secret image) into the cover image they used LSB algorithm. LSB each of the pixel of the cover image is replaced by the bits of the secret image. Then and LSB of each pixel of the cover image is replaced by the bits of the secret image.

In order to transfer the data/image to the intended user at destination without any alterations or modifications there are many approaches like Cryptography.

Watermarking and Steganography The presents the general overview of image watermarking and different security issues. In this paper, Image Watermarking using Least Significant Bit (LSB) algorithm has been used for embedding the message/logo into the image. This work has been implemented through JAVA [13].

2.11.3 Preeti Parashar Preeti Parashar and Rajeev Kumar Singh 2014 :

A Survey Digital Image Watermarking Technique Digital image processing is a rapidly developing area with various raising applications in computer science and engineering. It is very import field for the research work because its techniques are used in almost all kinds of tasks like human computer interface, medical visualization, image enhancement, Law enforcement, artistic effects, image restoration and digital watermarking for security purpose. Digital image processing has many beneficial Properties over the image processing.

Digital watermarking is very useful method for providing security to the digital media on the internet technology. In this paper, survey of different techniques based on spatial domain (LSB) and the transform domain (DCT, DWT, and DFT). This survey analyses the limitations and strengths of the watermarking methods.

Digital watermarking is still a challenging research field with many interesting problems like it does not prevent copying or distribution and also cannot survive in every possible attack. One future research pointer is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio [14].

