Seminar Report

**on**

**DIGITAL WATERMARKING**

**Submitted By**

**PUSHPAK HIRODE**

**SHARAYU DANGE**

**GAYATRI KAJE**

Seventh Semester

B.E.(Electronics and Telecommunication Engineering)

**Guided by**

# PROF. N.S.WADHE



**Department of Electronics and Telecommunication Engineering,**

**Prof. Ram Meghe Institute of Technology & Research, Badnera - Amravati**

**2021-2022**

**CERTIFICATE**

This is to certify that the seminar report entitled

# DIGITAL WATERMARKING

is a bonafide work and it is submitted to the Sant Gadge Baba Amravati University, Amravati

By

## Pushpak Hirode

## Sharayu Dange

## Gayatri Kaje

Seventh Semester B.E.(Electronics and Telecommunication

Engineering ) in the partial fulfillment of the requirement for the degree of Bachelor of Engineering in Electronics and Telecommunication

Engineering, during the academic year 2021-2022 under my guidance.

Prof. N.S.WADHE Dr. S. M. Deshmukh

Guide Head,

Department of EXTC Engg. Department of EXTC Engg.

PRM Institute Of Technology & Research, PRM Institute Of Technology & Research,

Badnera Badnera



**Department of Electronic and Telecommunication Enginnering,**

**Prof. Ram Meghe Institute of Technology & Research, Badnera- Amravati.**

**2021-2022**

**ACKNOWLEDGEMENT**

I would like to express our deep and sincere thanks to Dr. A. P. Bodkhe Sir, Principal and Dr. S. M. Deshmukh Sir, Head, Electronic and Telecommunication Engineering Department for their tremendous support and valuable guidance. I would like to express our deep sense of gratitude and whole hearted thanks to our Guide Prof. N. S .Wadhe Sir for his keen interest, co-operation and continuous encouragement without which it was not possible for us to complete this project work. I would be deviating from our duty if I fail to disseminate about the valuable time and suggestions that Prof. N. S .Wadhe Sir, Project in charge has imparted.

Pushpak Hirode

Sharayu Dange

Gayatri Kaje

**ABSTRACT**

The ease of reproduction, distribution, and manipulation of digital documents creates problems for authorized parties that wish to prevent illegal use of such document. To this end, digital watermarking has been proposed as a last line of defense. A digital watermark is an imperceptible, robust, secure message embedded directly into a document. The watermark is imperceptible both perceptually and statistically. Robustness means that the watermark cannot be removed or modified unless the

document is altered to the point of no value. The watermark is secure if unauthorized parties cannot erase or modify it. Current watermarking schemes may be viewed as spread-spectrum communications systems, which transmit a message redundantly using a low-amplitude, pseudonoise carrier signal. An example highlights the basic mechanisms and properties of spread spectrum and their relation to watermarking. Finally, specific issues in watermarking of text, images, and video.

Keyword :- digital watermarking data hiding copyright protection spread-spectrum communications

Table Of Content:

### 1. Introduction

**1.1 Objective**

**1.2 Literature Review**

**1.3 Research Methodology**

**2. Proposed work**

### 3. Types of watermark

**4. Properties of Watermark**

**5. Application of Watermark**

**6. Adavantage of Watermark**

**7. Disadvantage Of Watermark**

**8. Expected Outcomes**

### 9. References

**1 . Introduction**

Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible.

A digital watermark is a message which is embedded into digital content (video, images or text) that can be detected or extracted later. Moreover, in image the actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. Watermarking is the insertion of imperceptible and inseparable information into the host data for data security & integrity.

With the increasing use of the internet, copyright protection for the multimedia data has turned into a vital issue. For reliable communication the security of the data is the prime concern. Traditionally the cryptographic techniques were used for providing the security to the information but this theory has its own limitation. So to resolve the problem of the traditional technique the analyst has been focusing on the study of the digital watermarking technology. It increases the security of the data and protects the information from unauthorized access. Watermark information can be patent information, authentication information in order to determine the copyright owner of the digital works, it also certify the reliability and probity of the multimedia works .

A digital watermark is insertion of an impalpable signal into information, like sound, video and pictures, for an assortment of purposes, including inscribing and copyright control. It is basically used for the identification of the ownership of the copyright of an image. Digital watermarking is a code that is embedded in the image .it is very similar to the steganography as in both the information is embedded inside the cover message with less or no degradation of the cover – object. In steganographic systems the large amount of data is embedded which results in the secure data transmission without the degradation of the cover objects and in the watermarking systems the large amount of the data is embed that can’t be extracted or diversified without making the cover object entirely unusable .Many image watermarking techniques are used for process of watermarking techniques like DCT, DWT, LSB etc.

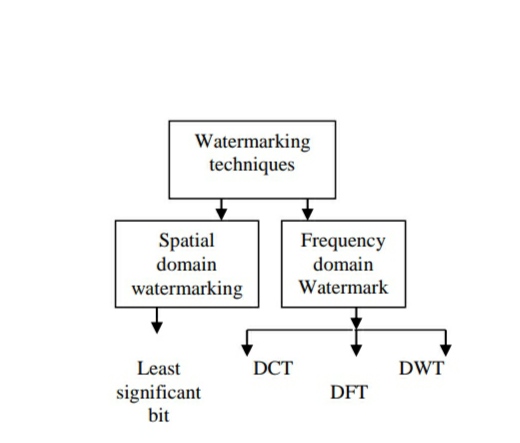
**1.2 Objective**

Digital watermarking hides, in digital images, the information necessary for ownership identity to offer copyright Protection and authentication. Robustness, even if recognized as a key property of the digital watermarking, is not considered enough to prove the ownership of the image. The aim of inversion attacks is to create ambiguities about the authorship of an image. To thwart inversion attacks with otherwise robust watermarking schemes, non-invertibility of watermarking has often been stressed. Digital watermarking is applied to protect the copyright of the digital media which unlike the analog media can be stored, duplicated, and distributed without loss of fidelity. Unauthorized copy of digital documents has been a subject of concern for many years especially with respect to their authorship claims. Digital watermarking, by hiding certain information in the original data provides a solution digital watermarking technology can effectively compensate for the deficiencies of the security and protection application of traditional information security technology. Digital watermarking prevents illegal duplicating, interpolating and distributing the digital content technically.

**1.2 . Literature Review**

* In First survey learn to Comparison of Digital Watermarking with Other Techniques of Data Hiding”, , the author name is, K.Sridhar, Dr. Syed Abdul Sattar , Dr. M Chandra Mohan International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (1) , 2014, 350-353
* In second survey learn the paper title is ,“Performance Comparison of Digital Image Watermarking Techniques, the author name is Namita Chandrakar, Jaspal Bagga A Survey”, International Journal of Computer Applications Technology and Research Volume 2– Issue 2, 126 – 130, 2013
* In third survey learn the paper title is A Survey of Digital Watermarking Techniques, Applications and Attacks, Author name is Prabhishek Singh, R S Chadha International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013

**1.3 Research Methodology**



Digital watermarking comprise of various watermarking techniques for the protection of the data .The techniques of watermarking are generally classified into two fields. Watermarking techniques are divided into two categories.

1) Spatial domain watermarking: In this type of watermarking the information is added by changing the pixel values of the carrier signal .least significant bit is one of technique of the spatial domain watermarking.

• Least significant bit: - in this the watermark is added in the pixel of the image . the pixel of the images is accessed and the information which is to send is inserted in the pixel. This is an method for providing security to the data that is to transmitted.

2) Frequency Domain watermarking:-In this type of watermarking the information is embedded into the frequency coefficient of the carrier signal. It is more robust, and its capacity of hiding the information is more. Fourier transforms (FT), Discrete cosine transform (DCT), Discrete wavelet transform (DWT ) etc are some of the technique of frequency Domain watermarking.

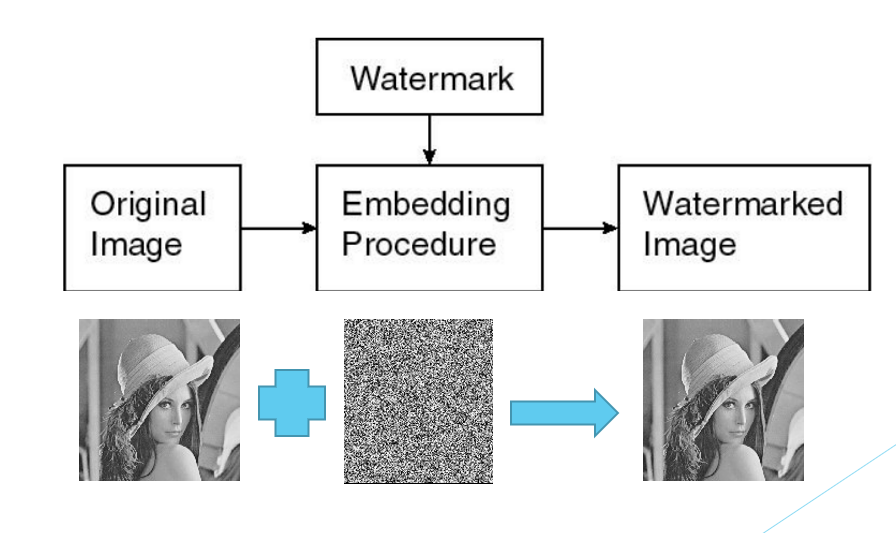
• Discrete cosine transform (DCT):- in discrete cosine transform an image is broken into the different frequency bands that are high, medium and low frequency bands. It transforms a signal from the spatial domain to the frequency domain. The watermark is embedded into these band according to the choice made. DCT is applied in many fields like data compression, pattern recognition and every field of image processing. DCT is a real transform with better computational efficiency and also gives a better performance in the bit rate reduction.

• Discrete fourier transform (DFT) :- A discrete fourier transform is performed on the digital data and a magnitude domain of the discrete fourier transform is completed. The water mark is embedded into selected frequency bands of the computed magnitude of the discrete fourier transform, thereby creating a watermarked magnitude domain. The selected frequency bands comprise one or more middle frequency bands, and the middle frequency bands comprise a band of circular rings of the magnitude domain. An inverse Discrete Fourier Transform is performed on the watermarked magnitude domain to reconstruct the digital data with the embedded watermark.

• Discrete wavelet transform (DWT) :- In discrete wavelet transform image sis divided into subbands of different resolution. On the arrival of the image the decomposition of an image can be done at different level using series of low pass and high pass filter. Due to its spatial localization and multi resolution technique DWT is used in the digital watermarking. it give better visual image quality , localization and is highly robust technique .

**2. PROPOSED WORK:**

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark .For visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. Fig 1.1. Watermark and image The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals.

Figure shows the general watermarking embedding procedure. In an original image with the help of embedding procedure watermark is embedded and then we get a watermarked image. The most common example of watermark is an Indian curreny. 

### 3.Types of watermark

Digital watermarks are of four types:

• Visible

• Invisible

• Public

• Fragile

A visible watermark typically consists of a conspicuously visible message or a company logo indicating the ownership of the image. Any removal or tampering with the logo would break the copyright agreement. Another way is to write the copyright notice and other information into an extra couple of lines within the image file. The extra lines can be removed from the image, without detriment to the image quality and content, but this again would break the copyright agreement of the image. A visible watermark was added to the image to create this image.



The watermark is a repeating image of a bird in flight. Visible watermarks often look as if they were "embossed" onto the original image, as illustrated here.

**An invisible watermarked** image appears very similar to the original. The existence of an invisible watermark can only be determined using an appropriate watermark extraction or detection algorithm. It can be detected by an authorized agency only. Such watermarks are used for content and/or author authentication and for detecting unauthorized copier.



To insert the invisible watermark, we first supplied a special password, or a "key," for security. The key may be used to recover the message contained in the invisible watermark, and to determine whether the image was altered since the invisible watermark was inserted.

**Public watermark** such a watermark can be read or retrieved by anyone using the specialized algorithm. In this sense, public watermarks are not secure.

**Fragile watermarks** are also known as tamperproof watermarks. Such watermarks are destroyed by data manipulation. Fragile watermark is a mark which is (highly) sensitive to a modification .A fragile watermarking scheme should be able to detect any change in the signal and identify where it has taken place and possibly what the signal was before modification. It serves at proving the authenticity of a document.

**4 .PROPERTIES OF WATERMARK:**

The characteristics of a watermarking algorithm is normally tied to the application is designed for. The most important properties of any digital watermarking techniques are robustness, security, imperceptibility, complexity, and verification.

The following merely explain the words used in the context of watermarking. **Imperceptibility:-**In watermarking, we traditionally seek high fidelity, i.e. the watermarked work must look or sounds like the original. Whether or not this is a good goal is a different discussion. Imperceptibility means the watermark is not seen by the human visual system. **Robustness:-** By "robust" we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, just to enumerate some. Robustness is defined as if the watermark can be detected after media (normal) operations such as filtering, lossy compression, color correction, or geometric modifications. In some cases the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent. It is more a property and not a requirement of watermarking. The watermark should be able to survive any reasonable processing inflicted on the carrier (carrier here refers to the content being watermarked).

**Security:-**The watermarked image should not reveal any clues of the presence of the watermark, with respect to un-authorized detection, or (statistical) indefectibility or unsuspicious (not the same as imperceptibility). Security means the embedded watermark cannot be removed beyond reliable detection by targeted attacks.

**Complexity** is described as the effort and time required for watermark embedding and retrieval. **Verification** is a procedure where by there is a private key or public key function .

**Capacity:** Image watermarking capacity is an evaluation of how much information can be hidden with in a digital image. Watermarking capacity is determined by the statistical model used for the host image, by the distortion constraints on the data hider and the attacker, and by the information available to the data hider, to the attacker, and to the decoder.

**Fast embedding and/or retrieval** The speed of a watermark embedding algorithm is important for applications where documents are marked “on-the-fly” (i.e., when they are distributed). The large bandwidth necessary for video also requires fast embedding methods. However, since ownership disputes will likely take weeks or months to resolve, a watermark recovery algorithm may emphasize reliable detection over speed.

No reference to original document For some applications, it is necessary to recover the watermark without requiring the original, unmarked document (which would otherwise be stored in a secure archive). Multiple watermarks It may also be desirable to embed multiple watermarks in a document. For example, an image might be marked with a unique watermark each time it is downloaded.

**Unambiguity** A watermark must convey unambiguous information about the rightful owner of a copyright, point of distribution, etc.This requirement is a cryptographic and protocol issue and not covered in this paper. Of these properties, robustness, imperceptibility, and security are usually the most important. When speaking of robustness, we often talk about attacks on a watermark. An attack is an operation on the marked document that, intentionally or not, may degrade the watermark and make the watermark harder to detect. For text documents, an attack might consist of photocopying. For images and video, compression(e.g., JPEG or MPEG), filtering, cropping, resizing, and other signal processing manipulations (even printing and rescanning) must not destroy the watermark.

**5 .APPLICATION OF WATERMARK**

The first applications that came to mind were related to copyright protection of digital media. In the past duplicating art work was quite complicated and required a high level of expertise for the counterfeit to look like the original. However, in the digital world this is not true. Now it is possible for almost anyone to duplicate or manipulate digital data and not lose data quality. Similar to the process when artists creatively signed their paintings with a brush to claim copyrights, artists of today can watermark their work by hiding their name within the image. Hence, the embedded watermark permits identification of the owner of the work.There are a number of possible applications for digital watermarking technologies and this number is increasing rapidly.

**Security:** In the field of data security, watermarks may be used for certification, authentication, and conditional access. Certification is an important issue for official documents, such as identity cards or passports. Example on the left of a protected identity card. The identity number "123456789" is written in clear text on the card and hidden as a digital watermark in the identity photo. Therefore switching or manipulating the identity photo will be detected. Digital watermarking permits linking information on documents. That means that key information is written twice on the document. For instance, the name of a passport owner is normally printed in clear text. But it would also www.studymafia.org be hidden as an invisible watermark in the passport photo. If anyone tries to tamper with the passport by replacing the photo it would be possible to detect the change by scanning the passport and verifying the name hidden in the photo.

**Tampering with images:** Another application is the authentication of image content. The goal of this application is to detect any alterations and modifications in an image. The three pictures below illustrate this application. The picture on the left shows an original photo of a car that has been protected with a watermarking technology. In the center, the same picture is shown but with a small modification: the numbers on the license plate have been changed. The picture on the right shows the photo after running the digital watermark detection program on the tampered photo. The tampered areas are indicated in white. We can clearly see that the detected area corresponds to the modifications applied to the original photo. Using digital watermarks for integrity verification: the protected image is the image (a) above; a modified image is obtained by swapping the numbers 9 and 4 of the number plate (b); digital watermarking technology allows detecting and highlights the modified areas, as shown on (c).

**Copy prevention or control** : Watermarks can also be used for copy prevention and control. For example, in a closed system where the multimedia content needs special hardware for copying and/or viewing, a digital watermark can be inserted indicating the number of copies that are permitted. Every time a copy is made the watermark can be modified by the hardware and after a point the hardware would not create further copies of the data. An example of such a system is the Digital Versatile Disc (DVD).

**Owner Identification** :

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

**Copy Protection**: Illegal copying is also prevent by watermarking with copy protect bit. This protection requires copying devices to be integrated with the watermark detecting circuitry. **Broadcast Monitoring** Broadcasting of TV channels and radio news is also monitoring by watermarking. It is generally done with the Paid media like sports broadcast or news broadcast. **Medical applications** Medical media and documents are also digitally verified, having the information of patient and the visiting doctors. These watermarks can be both visible and invisible. This watermarking helps doctors and medical applications to verify that the reports are not edited by illegal means.

**Data Authentication** Authentication is the process of identify that the received content or data should be exact as it was sent. There should be no tampering done with it. So for that purpose sender embedded the digital watermark with the host data and it would be extracted at the receivers end and verified. Example are CRC (cyclic redundancy check) or parity check.

**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.

**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. 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.

**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.

**6 .Advantages of Watermarking**

* Digital Watermarking allows embedding of arbitrary information (the

watermark) into digital media (such as video or images) by applying

imperceptible, systematic alterations to the media data.

* Higher level of security: Security and confidentiality of the embedded

information is provided by a secret key. Without this key the

watermark cannot be accessed or modified. Watermarks can be

designed in such a way that the embedded information is still

retrievable even after the carrier medium changed.

* The advantage of digital watermarking is that the product of the

embedding process is still a digital medium. Customers can do

everything with a marked medium that they can do with an unmarked

one. Watermarked media can be played or copied without any

restrictions

* Digital Watermarking is non-restrictive – only misuse is detectable

and traceable.

* Easy to implement and understand.
* Low degradation of image quality.
* High perceptual transparency.
* Gain factor can be increased resulting in increased robustness.
* High level of robustness against most type of attacks.
* This method hides data within the continuous random texture patterns of a picture.
* 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.
* Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception.
* DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions

**7.Disadvantages of watermarking**

Digital watermarking is a recent research field; therefore its intrinsic limits are not well understood yet. On the other hand, more insight into the technical possibility of satisfying the requirements imposed by practical applications is needed, if the practical possibility of using watermarking for copyright protection is to be evaluated. In the following, some of the most common limits shared by digital watermarking schemes are described.

* Visible watermark can be easily removed.
* A watermarking algorithm which is really robust does not exist yet. In

the image case, robustness is still an open issue. More specifically,

resistance to geometric manipulations such as cropping is recognized

as a very difficult goal to achieve in a computationally efficient way.

* Owners can erase the mark: virtually all the watermarking schemes

proposed so far are reversible according to the definition previously

given.

In other words, by knowing the exact content of the watermark, and

the algorithms used to embed and retrieve it, it is always possible to

make it unreadable without any significant degradation of the data.

**8 .EXPECTED OUTCOMES**

* As Described Recent Development In The Digital Water Marking Of Images In Which The Water Marking Technique Is Invisible.
* Digital Water Marking Is Rapidly Evolving Area Of Research And Development.
* Digital Watermarking Technology Can Provide New Way To Protect The Copyright Of Multimedia Information And To Ensure The Safe Use Of Multimedia Information.
* The study of the watermark technology has become active since mid-1990s, and some technologies are already adopted in practical applications as a product or as proprietary services for enterprises.
* Although this is a relatively new technology area, it quickly becomes a practical and effective solution in some application areas, and has great potential for some other areas as well.
* The key to the successful implementation is to understand the advantages and the limitations of the watermark technology, and to use the watermark technology as a complimentary element to the existing security elements.

### 9. References

1. K.Sridhar, Dr. Syed Abdul Sattar , Dr. M Chandra Mohan,” Comparison of Digital Watermarking with Other Techniques of Data Hiding”, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (1) , 2014, 350-353
2. Namita Chandrakar, Jaspal Bagga,“Performance Comparison of Digital Image Watermarking Techniques: A Survey”, International Journal of Computer Applications Technology and Research Volume 2– Issue 2, 126 - 130, 2013
3. Prabhishek Singh, R S Chadha,“A Survey of Digital Watermarking Techniques, Applications and Attacks”,International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013