NEW HORIZON COLLEGE OF ENGINEERING

AUTONOMOUS COLLEGE Permanently Affiliated to VTU, Approved by AICTE & UGC
Accredited by NAAC with 'A' Grade

Mini Project Report On

"DIGITAL WATERMARKING"

Submitted in partial fulfilment for the award of degree

Bachelor of Engineering

In

Electronics and Communication

BY

GUNTUPALLI SOWMYA (1NH18EC714)

INDRAJA CHIRUGUDU (1NH18EC716)

KABILAN.K (1NH18EC721)

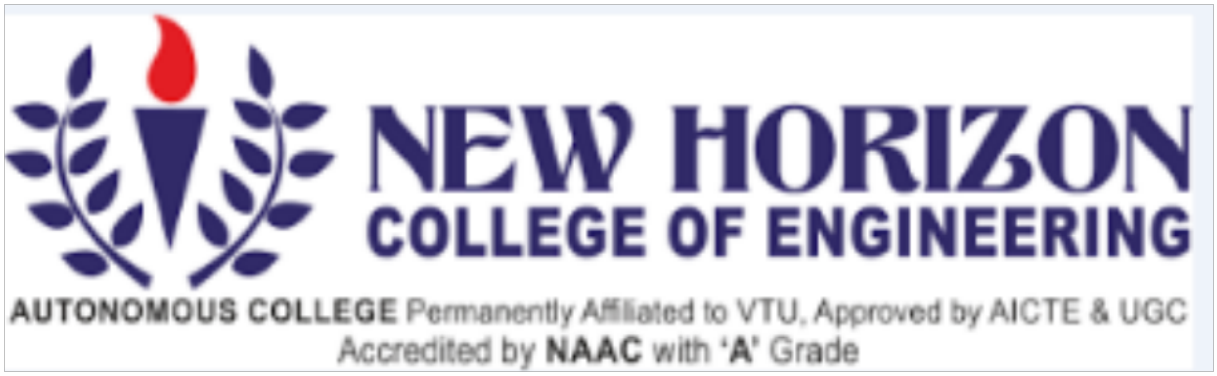
CHANDRASHEKHARAIAH M.M (1NH18EC709)

UNDER THE GUIDANCE OF:

Mr. PUVIRAJAN

Department of Electronics and Communication Engineering

New Horizon College of Engineering



CERTIFICATE

Certified that the mini-project entitled "**DIGITAL WATERMARKING**" is carried out by **GUNTUPALLI SOWMYA** bearing **USN:1NH18EC714, INDRAJA CHIRUGUDU** bearing **USN:1NH18EC716, KABILAN.K** bearing **USN:1NH18EC721, CHANDRASHEKHARAIAH M.M** bearing **USN:1NH18EC709** students of **NEW HORIZON COLLEGE OF ENGINEERING,BENGALURU**,in partial fulfilment for the award of Bachelor of Engineering in Electronics and Communication of the Visvesvaraya Technological University,Belgavi during the year **2020-2021**

It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the department library. The mini project report has been approved as it satisfies the academic requirements in respect of the mini project work prescribed for the said degree.

Signature of the HOD	Signature of the Guide
Dr. Sanjeev Sharma	Mr. Puvirajan
Professor & HOD	Assistant professor
Dept. of ECE	Dept. of ECE
NHCE, Bengaluru	NHCE, Bengaluru

EXTERNAL VIVA

Name of the Examiners	**Signature with date**
1.	
2.	

ACKNOWLEDGEMENT

The satisfaction that accompany the successful completion of any task would be , but impossible without the mention of the people who made it possible, whose constant guidance and encouragement helped us to succeed.

We thank **Dr.Mohan Manghnani**, Chairman of **New Horizon Educational Institution,** for providing necessary infrastructure and creating good environment.

We also record here the constant encouragement and facilities extended to us by **Dr.Manjunatha**, Principal,NHCE and **Dr.Sanjeev Sharma**, head of the department of Electronics and Communication Engineering .We extend sincere gratitude to them.

We sincerely acknowledge the encouragement,timely help and guidance to us by our beloved **Mr.Puvirajan** to complete the project within stipulated time successfully.

Finally, a note thanks to the teaching and non-teaching staff of electronics and communication department for their co-operation extended to us, who helped us directly or indirectly in this successful completion of mini project.

CHANDRASHEKHARAIAH H.M	**1NH18EC709**
KABILAN.K	**1NH18EC721**
GUNTUPALLI SOWMYA	**1NH18EC714**
INDRAJA CHIRUGUDU	**1NH18EC716**

ABSTRACT

Digital domain offers various advantages over analogue like as high-quality editing, perfection in copying etc. So, this is more preferable now. It causes the large-scale unauthorised copying of music, book, film & software etc. so for giving protection from unauthorised copying we are using a unique mythology named DIGITAL WATER MARKING.

A Robust Watermark is more resilient to the tempering/attacks that multimedia object (Image, Video, and Audio) had to face like compression, image cropping, image flipping, image rotation to name a few.

Among the various information hiding technique, we have chosen digital water marking. To send secret information embedded in carrier multimedia object we use that method. The message may be text, audio, video or image. The hiding object may be visible or invisible. So, our goal is to provide an algorithm to increase the imperceptibility, robustness and data capacity for the digital water marking

CONTENTS

List of Figures

CHAPTER 1
INTRODUCTION

The internet is an excellent sales and distribution channel for digital assets, but copyright and content management can be challenged. These days, digital images can be used every-where with or without consent. Images that are leaked or misused can hurt marketing efforts, brand image or ultimately sales. And intellectually property assets can be detached from your copyright information, so guarding brands and intellectual property assets is essential.

Watermarking solutions let you add extra layer of protection to your digital images.

WHAT IS DIGITAL WATER MARKING?

Digital water marking means hiding message related to a digital signal like (image, song, video).digital watermarking is an extension of this concept in the digital world. Digital water marking may be visible in which case their use two fold one is discourage unauthorized usage and second is act advertisement. Digital watermarking works by the hiding information within digital data, that it cannot be detected without any special software with aim of making sure that hidden data is present in all copies of the data that are made legally or otherwise, never the less of attempts to remove it.

There are many types of digital information of data like:

i) Digital audio
ii) Digital image
iii) Digital video

A watermark is pattern of bits inserted into a digital image, audio or video file that identifies the files copyright information (author, rights, etc.). the name “watermark” is derived from the faintly visible marks imprinted on organisation stationary.

Unlike printed watermarks, which are intended to be somewhat visible (like the very light compass stamp watermarking this report), digital watermarks are designed to be completely invisible, or in the case of audio clips, inaudible.

In addition, the bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. And finally, a digital watermark must be robust enough to survive changes to the file its embedded in.

Digital watermarking works by concealing information within digital data, such that it cannot be detected without special software with the purpose of making sure the concealed data is present in all copies of the data that are made weather legally or otherwise, regardless of attempts to damage/remove it.

HISTORY OF WATERMARKING

The paper watermark first appeared in 1282 in Italy. It all started by adding a thin wire to the paper mould which was introduced a transparent mark within the paper (making the paper identifiable or to be used as trademark). The meaning and purpose of the earliest watermarks are uncertain. They may have been used for practical functions such as identifying the moulds on which sheets of papers were made, or as trademarks to identify the paper maker. On the other hand, they may have represented mystical signs, or might simply have served as decoration. In the eighteenth century, the watermark on paper had become functional in Europe and America. They were used as trademarks, to record the date that the paper was manufactured and to indicate the originality.

At that time the word watermark began to be used to identify the antifraud measures on money and other documents. The word watermark was first used at the end of the eighteenth century. In 1779, the first bank note forgery was attempted by John Mathison. Counterfeiting prompted advances in watermarking technology. William Congreve, an Englishman, invented a technique for making colour watermarks by inserting dyed material into the middle of the paper during papermaking. The resulting marks must have been extremely difficult to forge, because the Bank of England itself declined to use them on the grounds that they were too difficult to make. A more practical technology was invented by another Englishman, William Henry Smith. This replaced the fine wire patterns used to make earlier marks with a sort of shallow relief sculpture, pressed into the paper pattern. The resulting variation on the surface of the pattern produced beautiful watermarks with varying shades of grey. This is the basic technique used today for the face of President Jackson on the $20 paper note. The word watermark may have been acquired from the German term wassermarke, which means watermark in English. The interpretation of the word watermark is probably a reference to the effect of water on the paper. An example watermarking in early history is the imperceptible messages about the objects in which they are embedded. Another example of watermarking is in the field of music. A U.S. patent (1961) describes a new invention for preventing piracy. The watermark was implemented by inserting an identification code in the music by intermittently applying a narrow notch filter centred at 1 kHz. The absence of energy at this frequency indicated to a decryption code either a dot or a dash. The identification signal used the Morse code. This technology is similar to the digital methods used in the present day.

Digital watermarking gradually evolved until it was accepted as a form of copyright protection. In 1979, Szepanski described a machine-detectable pattern that could be placed on documents for anti-counterfeiting purposes. Nine years later, researchers described a method for embedding an identification code in an audio signal. In 1988, researchers first used the term digital watermark. In the early 1990s the term digital watermarking gained universal acceptability. In 1996, the first Information Hiding Workshop (IHW) was held, which included digital watermarking as one of its primary topics. Then more conferences specifically to security and watermarking of multimedia

contents were devoted in 1999. During this time many organizations began considering watermarking technology for inclusion in various standards.

The Copy Protection Technical Working Group (CPTWG) tested watermarking systems for protection of video on DVD disks. Also the protection of music and sound systems was introduced by the Secure Digital Music Initiative (SDMI). The advanced MPEG standards were also created by the International Organization for Standardization (ISO). Several companies were involved in watermark technology and intellectual property protection, including sounds, images and video. In the area of image watermarking, for example, Dig marc used the embedded watermark and detection technology with Adobe's Photoshop. In the late 1990s watermarked products became generally available.

PROPERTIES OF DIGITAL WATERMARKING

Digital image watermarking concerns to solve some issues properly, thus, this paper highlights the main requirements of watermarked image as following:

Robustness: The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning and printing, lossy compression, translation, scaling, and rotation, and other operations like digital to analog (D/A), analog to digital (A/D) conversions, cutting, image enhancement. In addition, not all watermarking algorithms have the same level of robustness, some techniques are robust against some manipulation operations, however, they fail against other stronger attacks. Moreover, it's not always desirable for watermark to be robust, in some cases it's desired for the watermark to be fragile. Therefore, the robustness can be classified as following:

- **Robust:** The watermark is designed to be able to survive against incidental and intentional attacks. This kind of watermarking can be used in broadcast monitoring, copyright protection, fingerprinting, and copy control.

- **Fragile:** The watermark in this type is designed to be destroyed at any kind of modification, to detect any illegal manipulation, even slight changes, involving incidental and intentional attacks. Fragile watermarks are mainly used in content authentication and integrity verification. They use blind detection type, as it will be discussed in Detection Types. In addition, the implementation of fragile techniques is easier than the implementation of robust ones.

- **Semi-fragile**: The watermark in this type is robust against incidental modifications, but fragile against malicious attacks and it is used for image authentication.

Imperceptibility: Imperceptibility (also known as Invisibility and Fidelity) is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image. In other words, the watermarked image should look similar to the original image, and the watermark must be invisible in spite of occurrence of small degradation in image contrast or brightness. However, the challenge is that imperceptibility could be achieved, but the robustness and the capacity will be reduced, and vice versa, imperceptibility may be sacrificed by increasing the

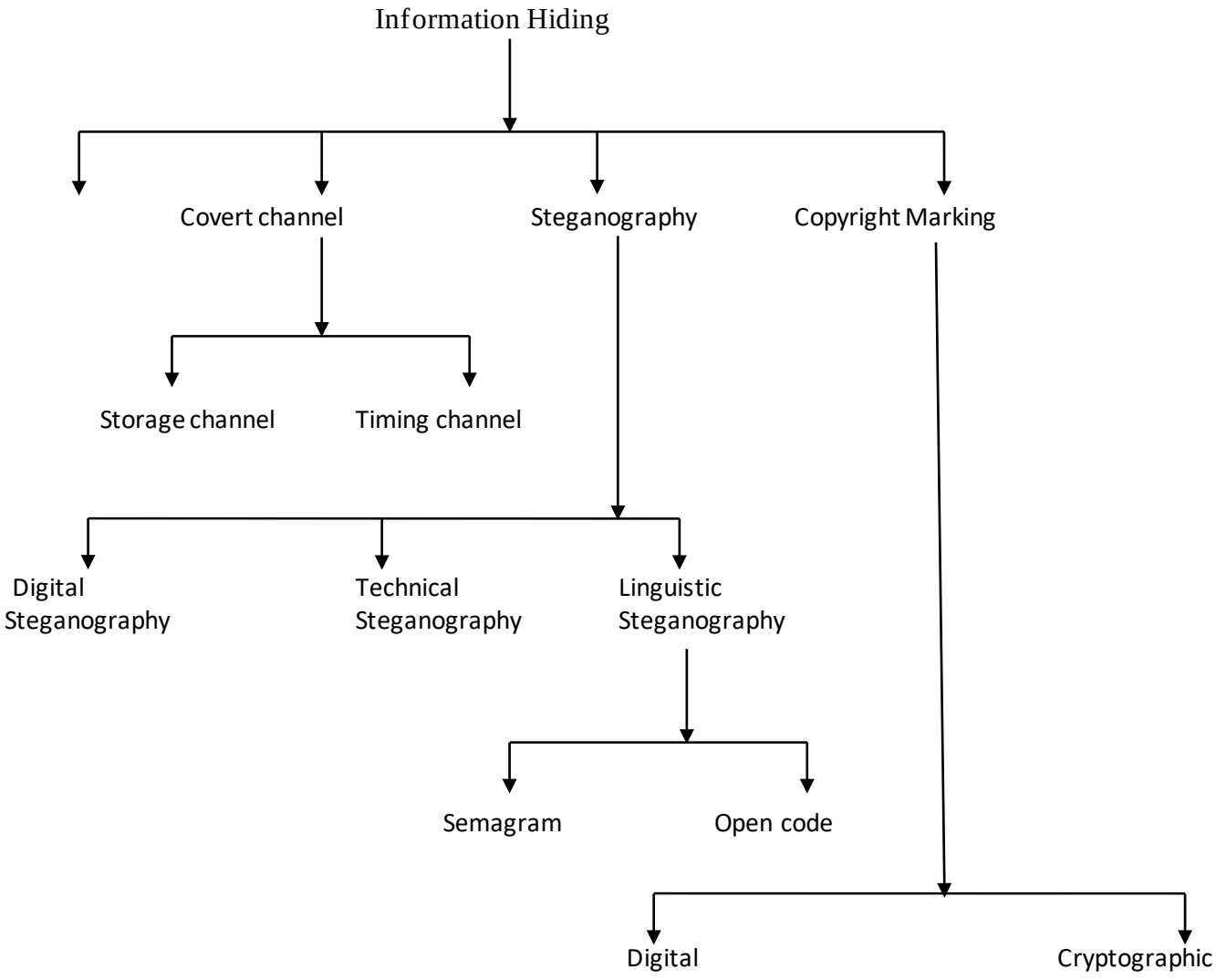
robustness and the capacity. Moreover, the watermark not always desired to be invisible, sometimes, it is preferred to have visible watermark into the image.

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

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

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

CLASSIFICATION OF INFORMATION HIDING TECHNIQUE



- **ANONYMITY:**

Anonymity means namelessly or having a pseudo name. It is a study of finding ways to hide the content (i.e. the sender and the recipients) of a message. We will not explain much more on this topic. Because our goal is reach to the watermarking technology.

- **COVERT CHANNEL:**

A covert channel is hidden from the access control mechanism operating system that cannot be detected of controlled by the hard ware based security mechanism.

Covert channel can be used for a single system as well as for a network also. It is of two types – Storage Channels and Timing Channels, whether storage channels are more commonly used than the other one. The main drawback of this information hiding scheme is the low Signal-to-Noise ratio, low data rates and it can often be detected by monitoring the system performance.

- **STEGANOGRAPHY:**

Greek word **`Stegano'** means covered or protected and **`Graphia'** means writing. Stegaaphy is the art or practice of concealing a secret information, in form of a message or image or file within another message, image or file.

As said before steganography is of three types- Technical steganography, Linguistic steganography, Digital steganography.

The examples given in the section of history of information hiding, gives an idea about the **technical steganography**.

- **OPEN CODE:**

use illusions or code word. ` Hypnerapomachia Poliphili' is a suitable example of open code steganography is also described in history portion.

- **SEMAGRAM:** is a secret code which is not in written form like musical notations.

Now come to the recent trade of steganography- **Digital steganography**. Electric communication may include steganography coding inside of a transport layer such as a document, or image or protocol. This technique is named as the digital steganography.

Difference between Cryptography, Steganography and Watermarking –

Cryptography	Steganography	Watermarking
The message itself converted into a distinct and unreadable form It needs a secret transmission Data quantity does not matter. It hides the content of the message actually. The message is transmitted being encrypted, cover is not required. It is for point to point communication purpose.	The message is made imperceptible in a cover signal. Secret transmission is not required Data quantity should be controlled as it decreases the imperceptibility. It conceals the existence of the message. The message may have nothing to do with the cover. Its purpose mainly points to point also.	The message is made robust as top priority. Secret transmission is not required Data quantity should be controlled as it decreases the robustness. It prevents the cover document from any types of unauthorized or illegal attempts. It carries the authenticity or information or copyright of the cover object. It provides generally one-to-many scheme.

IMPORTANCE OF WATERMARKING

The availability of personal computers and easy access to the internet has lead to a significant increase in the downloading of digital media files. These digital files can be pictures, music, videos and other documents. The internet became user friendly with the introduction of the first widely used web browser in November 1993. The internet is an excellent distribution system for digital media because it is inexpensive and allows convenient downloading and sharing between individuals and organizations. Therefore, copying and modifying these files and documents have become very popular. The illegal copying of some types of media has been a subject of concern for many years. As a result, an urgent solution for copyright protection and authentication is needed. Digital watermarking is an effective solution to protect intellectual properties and copyrights by hiding information such as logos, signatures or text into multimedia data such as images, videos, or audio files. However, content owners (especially large Hollywood studios and music labels) also see a high risk of piracy. In the past, using analogue devices posed a lower risk than with digital media; copying an analogue file allows results in a degradation of the quality. However, with digital media recording devices, songs and movies can be produced with no degradation whatsoever in quality, since the data are a stream of 1's and 0's.

Using digital devices and connecting them to the internet, people can record and distribute copyrightprotected material without return to the legal content owners, nor pay them for their efforts. Legitimate property owners started seeking a qualified method to protect their rights. Cryptography is probably the most common method of protecting digital content. By using this technology, products are encrypted before sell, and only people who purchased these have the decryption key to fully access the encrypted files. The encrypted files can also be made available via the Internet. Unfortunately, sellers cannot monitor how a legitimate customer handles the content after decryption. Once the original copy is sold, a pirate can actually purchase the product, use the decryption key to obtain unprotected copy content, then reproduce multiple copies for illegal distribution.

So cryptography provides a limited measure of protection; once the decrypted content reaches the customer there will be no further protection. Therefore, there is still a need for further protection of content, even after it is decrypted. Watermarking is a promising technology that can be used to fulfil the owner's copyright protection. In digital watermarking, the information is hided inside the contents. Digital watermarking can survive different kinds of attacks, include compression, digital to analogue conversion, and file format changes. A watermark can be designed to survive all of these processes. Watermarking has been considered for many copy prevention and copyright protection applications. In copy prevention, the watermark may be used to inform software or hardware devices that copying should be restricted. In copyright protection applications,

the watermark may be used to identify the copyright holder and ensure proper payment of royalties. Although copy prevention and copyright protection have been major driving forces behind research in the watermarking field, there are a number of other applications for which watermarking has been used or suggested. These include broadcast monitoring, transaction tracking, and authentication. Other applications that require still image watermarking include medical images, satellite images, and image captured by mobile phone cameras.

WATERMARKING MODELS

There are several ways in which we can model a watermarking process. These can be broadly classified in one of two groups. The first group contains models which are based on a communication-based view of watermarking and the second group contains models based on a geometric view of watermarking. In the rest of this essay, I only refer to image watermarking because I only concentrated on images during the development of example watermarking systems.

Communication-based models:

Communication-based models describe watermarking in a way very similar to the traditional models of communication systems. Watermarking is in fact a process of communicating a message from the watermarking embedder to the watermarking receiver. Therefore, it makes sense to use the models of secure communication to model this process. In a general secure communication model we would have the sender on one side, which would encode a message using some kind of encoding key to prevent eavesdroppers to decode the message if the message was intercepted during transmission. Then the message would be transmitted on a communications channel, which would add some noise to the noise to the encoded message. The resulting noisy message would be received at the other end of the transmission by the receiver, which would try to decode it using a decoding key, to get the original message back. This process can be seen in the Standard model of a communications channel with key-based encoding in general, communication-based watermarking models can be further divided into two sub-categories. The first uses side-information to enhance the process of watermarking and the second does not use side-information at all. The term side information refers to any auxiliary information except the input message itself, that can be used to better encode or decode it. The best example of this is the image used to carry the message, which can be used to provide useful information to enhance the correct detection of the message at the receiver.

Geometric models:

It is often useful to think of watermarking in geometric terms. In this type of model, images, watermarked and unwatermarked, can be viewed as high-dimensional vectors, in what is called the media space. This is also a high-dimensional space that contains all possible images of all dimensions. For example, a 512 X 512 image would be described as a 262144 elements vector in a 262144-dimensional space. Geometric models can be very useful to better visualize the watermarking process using a number of regions based on the desirable properties of watermarking. One of these regions is the embedding region, which is the region that contains all the possible images resulting from the embedding of a message inside an unwatermarked image using some watermark embedding algorithm. Another very important region is the detection region, which is the

region containing all the possible images from which a watermark can be successfully extracted using a watermark detection algorithm. Lastly, the region of acceptable fidelity contains all the possible images resulting from the embedding of a message into an unwatermarked image, which essentially look identical to the original image. The embedding region for a given watermarking system should ideally lie inside the intersection of the detection region and the region of acceptable fidelity, in order to produce successfully detected watermarks that do not alter the image quality very much. Here we can see that if mean square error (MSE) is used as a measure of fidelity, the region of acceptable fidelity would be an ndimensional sphere centred on the original unwatermarked image (co), with a radius defined by the largest MSE we are willing to accept for images with acceptable fidelity. The detection region for a detection algorithm based on linear correlation would be defined as a half space, based on the threshold used to decide whether an image has a watermark embedded or not. Note that the diagram is merely a projection of an ndimensional space into a 2d space. The region of acceptable fidelity (defined by MSE) and the detection region (defined by linear correlation) When thinking about complex watermarking systems, it is sometimes more useful to consider a projection of the media space into a possibly lower-dimension marking space in which the watermarking then takes place as usual. This projection can be handled more easily by computers because of the smaller number of vector elements and can be possibly expressed by block-based watermarking algorithms which separate images into blocks instead of operating on a pixel basis.

CHAPTER 2
LITRATURE SURVEY

1. In 1996 I.J. Cox et al. introduced a frequency domain water mark scheme using spread-spectrum technique. The intentions of the scheme were to insert watermarking into the particular spectral components of the signal which are perceptually most significant.by calculating the DCT of the entire image, the most significant regions are marked out. Then the watermark (here, used as sequence of real numbers with a normal distribution N (0, 1) and having a zero mean and 1 variance) is inserted into the DCT domain of the marked position of the general signal processing and geometric distraction. To make it imperceptible in any frequency beam cox et al.spread it over brod band.but the drawback scheme is that it wants the original image for its extraction. More ever, author did not clarify whether it is roboust again photocopying attack or not.

   Another human visual system based watermarking technology was prepared by kim et al in 1999.but here instead of DCT wavelet transform was used. Here the energy of each wavelet bands have been calculated and according to this the number of watermark sequence changes proportionally. The changing rate of a sinusoidal pattern per subtended visual angle (unit-cycle per degree is the estimation of image characteristics as well as the visual weight of watermarking in each wavelet transfer band.

2. A spatial domain invisible digital watermarking technique was proposed by R.B walfagang and E.J.delp in 1997.here the watermark was a combination of two dimensional blocks of a long row-by-row m-sequence ,having the same size of the image.in this scheme additionally the author used a testing paradigm with different ranges using which the authentically of the image could br determined.

3. I.J. Cox was followed by W.Zhu et al. with a little difference in the algorithm.in 1999 Zhu et al.developed this watermarking algorithm inserting the watermarking in wavelet coefficient and the watermark which

CHAPTER 3
TECHNOLOGY USED

The water mark technique is invented as well as fruitful in information hiding scheme because we don't have a perfect visual system to detect a slight change and to distinguish it from the original one.

Basically it is the procedure to embed an information (called watermark) into an object (known as host image or cover object) in such a way that modification will not be allowed. It mainly consists of two steps.

i) Watermark embedding process
ii) Watermark extracting process.

Embedding or encoding:

In the time of embedding a watermark, it is desired to achieve the maximum robustness as well as energy. To maximize the signal energy designer should try to decrease the error rate. Here an encoder function (FE) embeds the watermark (W) into an image (IO) and produces the watermarked image (IW). The general block diagram of a basic watermark embedding system is shown in Figure 1.

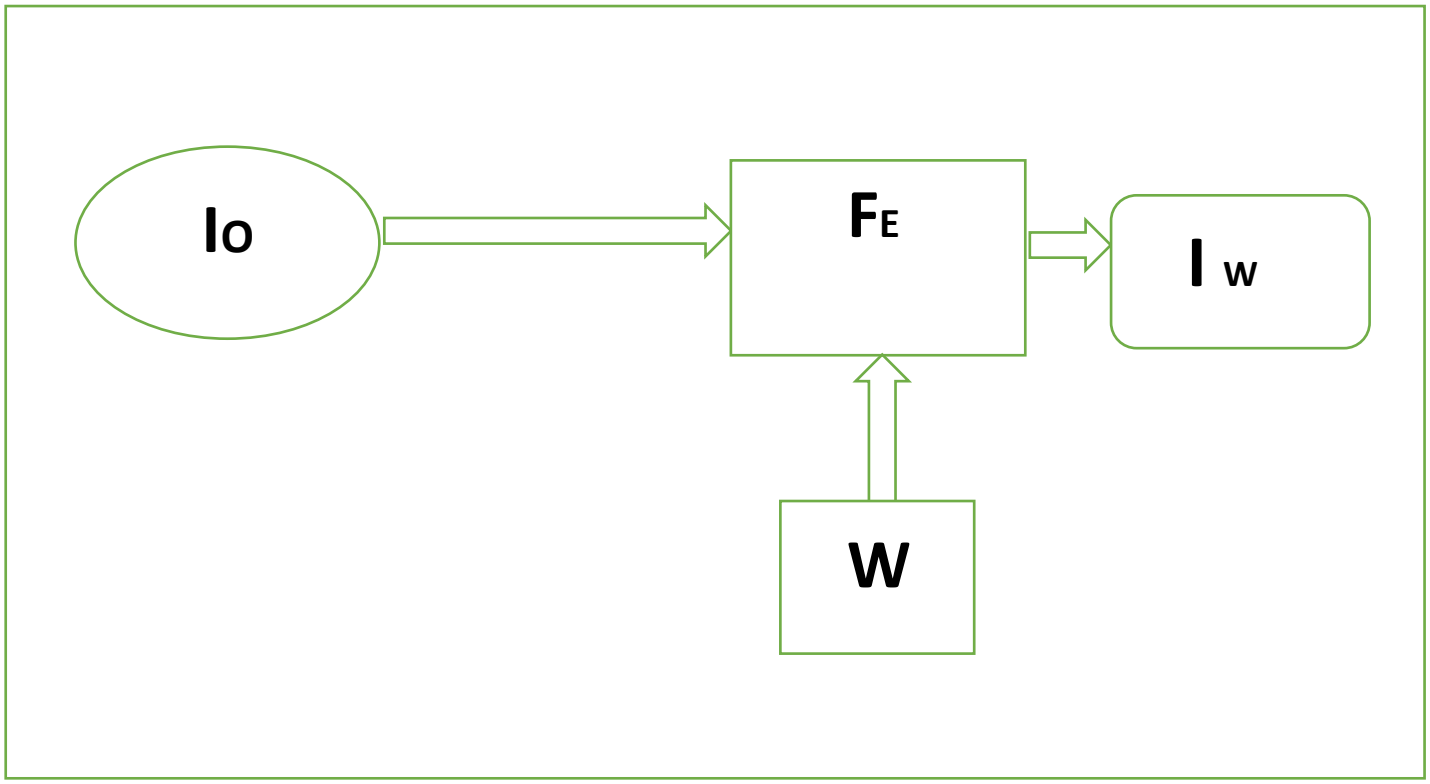


Figure 1 : Block diagram of watermark embedding system

Extracting or decoding:

The purpose of the extraction of an image is to determine the water mark. In this procedure the original image (IO) is given to the input extracting function (FD) and as another input the received image i.e. the watermarked image (IR) is applied. As an output of the decoder, a watermark (W') is obtained. Then to check whether the watermark is original or not, W' is compared to the original watermark (W) through a comparator function (FC) applying a certain threshold value. In fig.2 the extracting process of a watermark is shown in Figure 2.

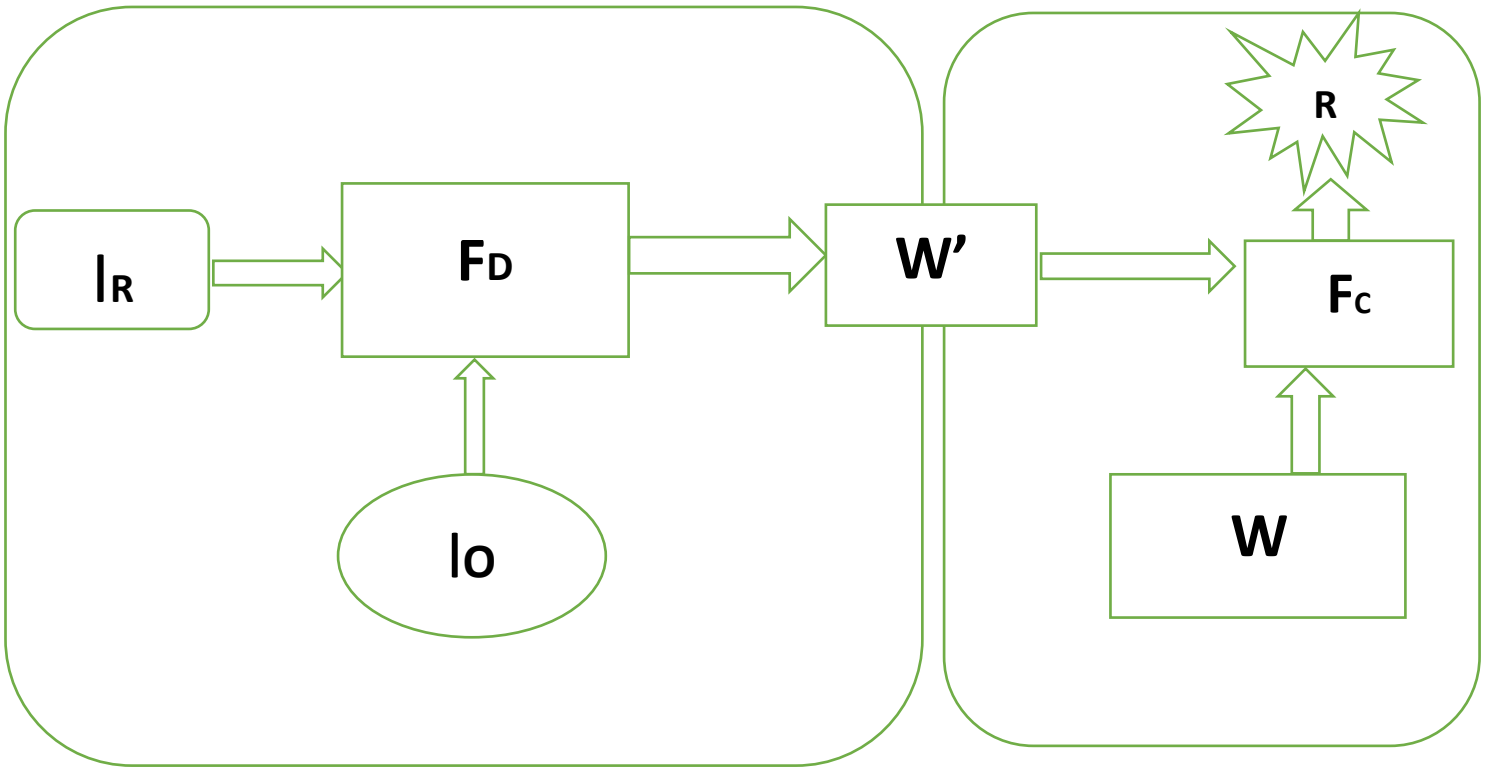


Figure 2: Block diagram of watermark extracting

CHAPTER 4

PROPOSED METHODOLOGY

For information hiding, various techniques are there. But as a copyright protection mechanism, we have chosen Digital Watermarking for some several facilities mainly,

i) Watermark is imperceptible so that the cover will not be detracted in the aesthetic sense.
ii) The watermark and the cover into which it is embedded are inseparable (Even if the after conversion of the cover into another file format, the watermark is not being eliminated or destructed).

We have to generate such a watermarking algorithm which provides better robustness, imperceptibility and data capacity. Although the above three features cannot be increased all at a time. Because, as discussed robustness means the property for which an information embedded in an object will try to remain unchanged. So if data quantity increased it will be harder to make them robust. Again it is also difficult to make a larger amount of data imperceptible. The property robustness also opposes to imperceptibility. A relative characteristic of these three main property of digital watermarking is shown in Figure 3.

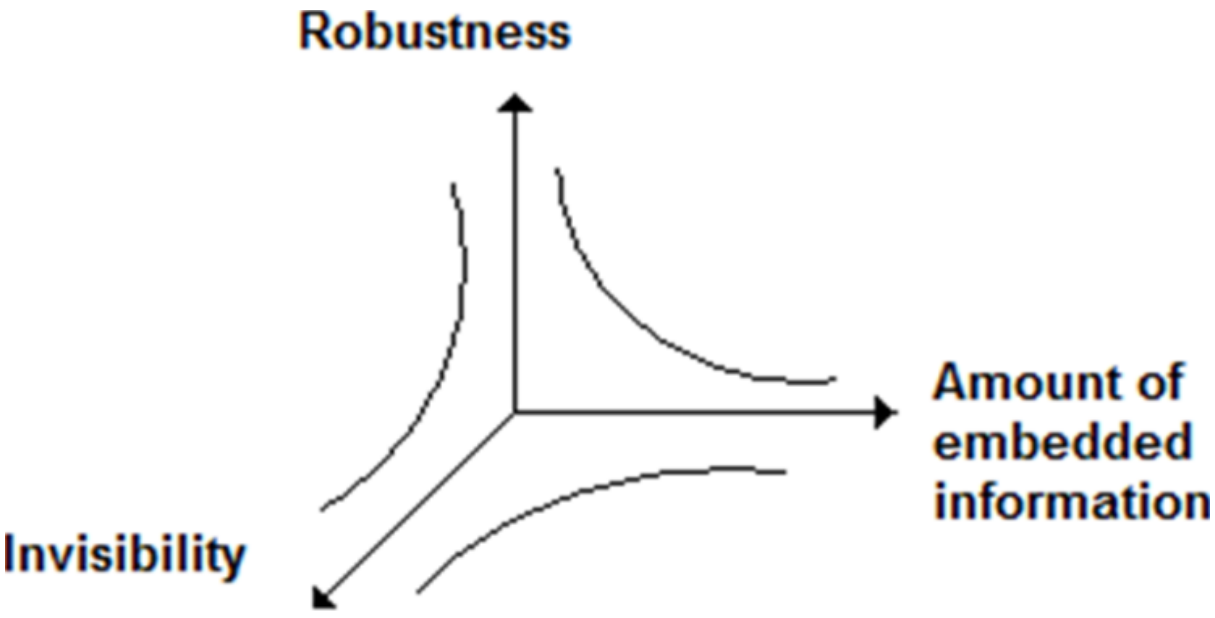


Figure 3. Relationship between Robustness, Imperceptibility, Data Capacity

So, we have to make an algorithm (having balanced robustness, imperceptibility and data capacity) to prove that it is a better approach by compare it to the others.

The proposed work consists of

1. Invisible Watermarking

2. Spatial Domain Analysis

3. Increasing of Robustness, Imperceptibility and Data Capacity

It is done using 2 basic operations:

1. **Saliency Mapping:** It works based on the visual saliency i.e. the portion of any image is mostly observed by human eye, and we should not enter the watermark into these places to increase the Robustness and Imperceptibility of the image.

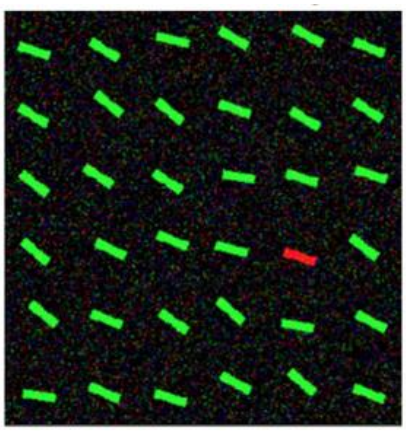


Figure 4

One item in the array of items strongly pops-out and effortlessly and immediately attracts attention. Many studies have suggested that in simple displays like this, no scanning occurs: Attention is immediately drawn to the salient item, no matter how many other items (called distractors) are present in the display. This suggests that the image is processed in parallel (all at once) to determine saliency at every location and to orient towards the most salient location.

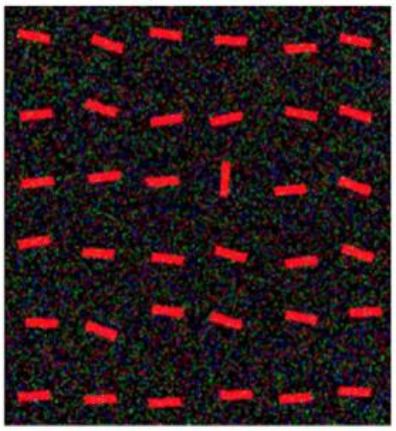


Figure 5

In this display, the vertical bar is visually salient. Comparing this example to the previous one suggests that local visual properties of a given item do not determine how perceptually salient this item will be; rather, looking at a given item within its surrounding context is crucial. Compare, for example, the red bar in the top-left corner of this image to the salient bar in the image above: both bars are red, roughly horizontal, and they both have very similar local appearances. Yet the one in the top-left corner here has low saliency and attention is much more strongly attracted to the more salient vertical bar, while the red bar in the above image is highly salient.

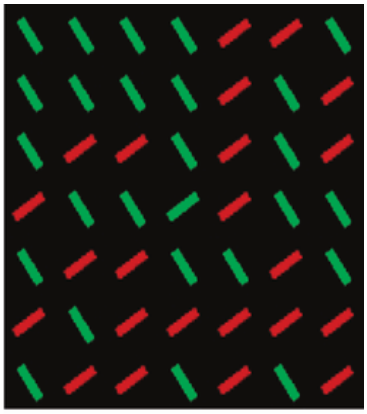
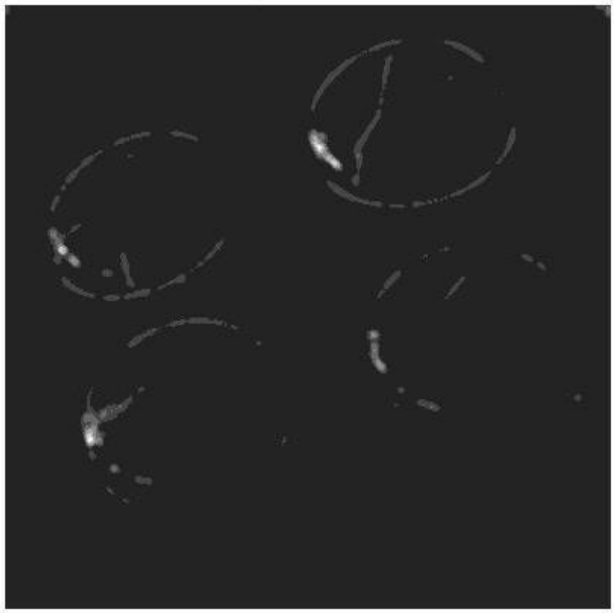


Figure 6

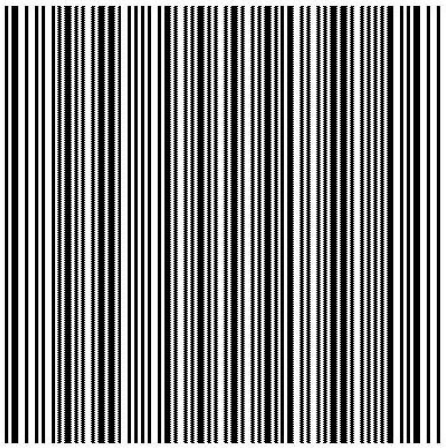
In this display, there is again one bar that is unique and different from all the other ones. However, by design and through judicious choice of distracting items, there is little saliency to guide you towards the target bar (why that is will be discussed in the following section). The target is a so-called conjunction target: is the only red and vertical bar. Because saliency does not help you direct attention towards potentially interesting items in the display, you find yourself scanning the image, seemingly at random, looking for something interesting

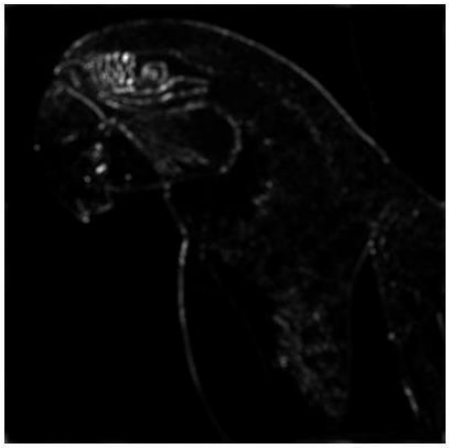
2. Hiding Capacity Map (HCM): This technique divides the whole image into some portions based on Saliency and JND to guide the user where to enter the most bits of the watermark and where to enter less no of bits of the watermark.

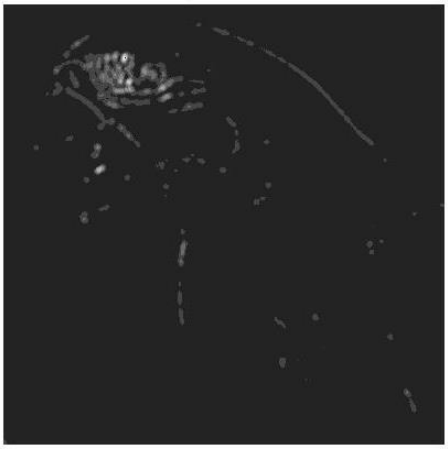


CHAPTER 5

RESULT OBTAINED







CHAPTER 6
FEATURE SCOPE

- The robustness can be measured.
- If needed, algorithm can be modified to increase robustness.
- A detailed comparison study with respect to other algorithm can be done.
- work with 3-D images can be done.
- Watermarking process can also be done with text or audio files.
- More Statistical Parameters can be analysed.

APPLICATION

- **Copyright Protection:** The most distinct application of digital watermarking is copyright protection. As lots of multimedia objects are exchanged over insecure network every time, the copyright protection has become a vital issue. Because for availability of the images through internet, these will be used without payment of royalty. So, watermark acting as an ownership mark can restrain the redistribution of the object.

- **Content Protection:** If a content (like library manuscript) stamped with a robust and visible watermark, it will indicate the ownership original. So, the content can be made available through the internet and be distributed more freely and publicly.

- **Content Labelling**: Watermark may carry more information about the object like quality, manufacturer's description etc. This is known as content labelling.

- **Authentication:** In some applications like ATM cards, ID cards, Credit cards etc., the ownership of the contain has to be verified. This quarry can be solved by embedding a watermark and in addition by providing the owner with a private key to access the message.

- **Evidence of Ownership:** Invisible watermarking may also use in copyright protection. Here it plays a roll of ownership evidence. That means the seller's watermark in the object proves that the public object is property of the seller not produced illegally or without payment of royalties by copying or editing the object.

- **Misappropriation Detection:** It may occur that someone bought a fee generating object from a license owner and sell these objects in cheap or free of cost, keeping of the revenue license owner. This type of fraudulent business can be restrained by invisible watermarking.

- **Tamper Detection**: By using the Fragile Watermarks any type of tampering on the object where the water mark was embedded, can be detected. Because, it tampering happened, the watermark will be degenerated or distorted.

- **Trustworthy Detection:** Invisible watermarking may also use in a trustworthy camera to indicate the images have been originally captured by the camera not produced by editing

or falsifying any scene. Actually at the time of capturing a picture an invisible watermark is embedded into the picture.

- **Digital Fingerprinting:** To justify the owner of as content, or to detect any alternation of object store in a digital library, it is used. Because for each party or object there should be a unique fingerprint.

- **Broadcast Monitoring:** It mainly helps the advertising companies to verify whether the advertisement broadcasted on T.V. or Radio appeared for the right duration or not.

- Source Tracking is another application of Digital Watermarking.

CHAPTER 7
REFERENCE

[1] H. Barlow. Possible Principles Underlying the Transformation of Sensory Messages. Sensory Communication, pages 217–234, 1961.

[2] H. Egeth, R. Virzi, and H. Garbart. Searching for Conjunctively Defined Targets. Journal of Experimental psychology: Human Perception and Performance, 10(1):32–39, 1984.

[3] R. Fergus, P. Perona, and A. Zisserman. Object class recognition by unsupervised scale-invariant learning. Proc. CVPR,2, 2003.

[4] J. Gluckman. Order Whitening of Natural Images. Proc.CVPR, 2, 2005.

[5] J. Intriligator and P. Cavanagh. The Spatial Resolution of Visual Attention. Cognitive Psychology, 43(3):171–216, 2001. [6] L. Itti and C. Koch. A Saliency-Based SearchMechanism for Overt and Covert Shifts of Visual Attention. Vision Research, 40(10-12):1489–1506, 2000.

[7] L. Itti and C. Koch. Computational Modelling of Visual Attention. Nature Reviews Neuroscience, 2(3):194–203, 2001. [8] L. Itti, C. Koch, E. Niebur, et al. A Model of Saliency-Based Visual Attention for Rapid Scene Analysis. IEEETransactions on Pattern Analysis and Machine Intelligence,20(11):1254–1259, 1998.

[9] C. Koch and T. Poggio. Predicting the VisualWorld: Silence is Golden. Nature Neuroscience, 2(1):9– 10, 1999.

[10] D. Martin, C. Fowlkes, D. Tal, and J. Malik. A Database of Human Segmented Natural Images and its Application to Evaluating Segmentation Algorithms and Measuring Ecological Statistics. Proc. ICCV, 2, 2001.

[11] A. Oliva and A. Torralba. Modeling the Shape of the Scene: A Holistic Representation of the Spatial Envelope. International Journal of Computer Vision, 42(3):145–175, 2001.

[12] A. Oliva, A. Torralba, and P. Schyns. Hybrid Images. ACM Transactions on Graphics (TOG), 25(3):527–532, 2006. [13] R. Rensink. Seeing, sensing, and scrutinizing. Vision Research, 40(10-12):1469–87, 2000.

[14] R. Rensink and J. Enns. Preemption Effects in Visual Search: Evidence for Low-Level Grouping. Psychological Review,102(1):101–130, 1995.

[15] R. Rensink, J. ORegan, and J. Clark. To See or not to See: The Need for Attention to Perceive Changes in Scenes. Psychological Science, 8(5):368–373, 1997

APPENDIX

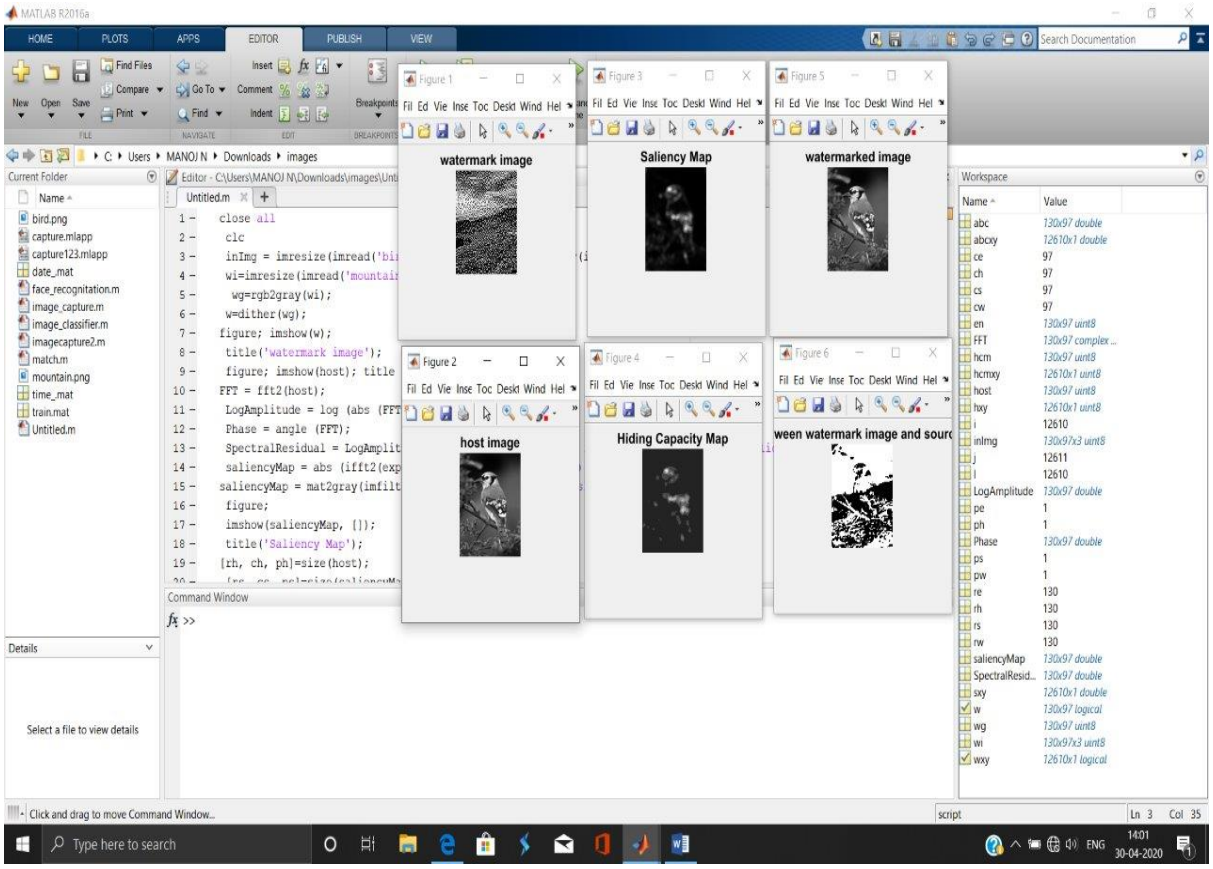
MATLAB CODE

```
close all
 clc
 inlmg = imresize(imread('mountain.png'),0.5);  host=rgb2gray(inlmg);
 wi=imresize(imread('bird.png'),0.5);
  wg=rgb2gray(wi);
 w=dither(wg);
figure; imshow(w);
 title('watermark image');
 figure; imshow(host); title ('host image');
FFT = fft2(host);
 LogAmplitude = log (abs (FFT));
 Phase = angle (FFT);
 Spectral Residual = LogAmplitude - imfilter(LogAmplitude, fspecial('average', 3), 'replicate');
 saliency Map = abs (ifft2(exp(Spectral Residual + 1i*Phase))).^(2);
saliencyMap = mat2gray(imfilter(saliencyMap, fspecial('disk', 3)));
 figure;
 imshow(saliencyMap, []);
 title('Saliency Map');
[rh, ch, ph]=size(host);
 [rs, cs, ps]=size(saliencyMap);
 [rw, cw, pw]=size(w);
hxy=reshape(host,rh*ch*ph,1);
sxy=reshape(saliencyMap,rs*cs*ps,1);
wxy=reshape(w,rw*cw*pw,1);
abc=zeros(rh,ch,ph);  abcxy=reshape(abc,rh*ch*ph,1);
```

```
for l=1:1:rs*cs*ps
 if 0<=sxy(l) && sxy(l)<0.15
  abcxy(l)= 35;
elseif 0.15<=sxy(l) && sxy(l)<0.3
abcxy(l)= 70;
 elseif 0.3<=sxy(l) && sxy(l)<0.45
 abcxy(l)= 105;
  elseif 0.45<=sxy(l) && sxy(l)<0.6
 abcxy(l)= 140;
 elseif 0.6<=sxy(l) && sxy(l)<0.75
 abcxy(l)= 175;
elseif 0.75<=sxy(l) && sxy(l)<0.9
 abcxy(l)= 210;
 elseif 0.9<=sxy(l) && sxy(l)<1
 abcxy(l)= 255;    end
end
hcm=reshape(uint8(abcxy),rh,ch,ph);
figure;
imshow(hcm);
title('Hiding Capacity Map');
[re, ce, pe]=size(hcm);
hcmxy=reshape(hcm,re*ce*pe,1);
j=1;
for i=1:1:re*ce*pe
if hcmxy(i)==63 && j<= rw*cw*pw
hxy(i)= bitset(hxy(i),3,wxy(j));
hxy(i)= bitset(hxy(i),4,wxy(j));
hxy(i)= bitset(hxy(i),5,wxy(j));
hxy(i)= bitset(hxy(i),6,wxy(j));
elseif hcmxy(i)==126  && j<= rw*cw*pw
```

```
  hxy(i)= bitset(hxy(i),3,wxy(j));
  hxy(i)= bitset(hxy(i),4,wxy(j));
 hxy(i)= bitset(hxy(i),5,wxy(j));
 elseif hcmxy(i)==189 && j<= rw*cw*pw
  hxy(i)= bitset(hxy(i),3,wxy(j));
  hxy(i)= bitset(hxy(i),4,wxy(j));
 elseif hcmxy(i)==255 && j<= rw*cw*pw
 hxy(i)= bitset(hxy(i),3,wxy(j));
 end
 j=j+1;
 end
 en=reshape(hxy,rh,ch,ph);
figure;
imshow(en);
title ('watermarked image');
figure;
 imshow(abs(wg-en)*100);
title('diff between watermark image and source image');
```

RESULT FOR THE CODE



PROPOSED ALGORITHM

1. Read the input image.

2. Convert this input image into grey code/grey image.

3. Resize this grey image.

4. Illustrate the difference between the black & white section where the difference is not noticeable.

5. Fourier transform of the source image.

6. Logarithmic value of absolute FT for each pixel.

7. Define the phase of each pixel for same FT value.

8. Calculate the Spectral Residual.

9. Find the Saliency Map of the original image.

10. Calculate the dimension for host, saliency map and host image.

11. Convert these three images into one dimension.

12. Create a blank image of dimension of source image.

13. Use ‘for loop’ for define the value difference for each pixel into the blank image.

14. Determine the corresponding HCM.

15. Now use another ‘for loop’ for bit set for the corresponding values of those pixel (2, 3, 4, 5).

16. Reshape the image into row, column and phase.

MAT LAB FUNCTIONS

A = imread(filename, fmt) reads a grayscale or colour image from the file specified by the string filename. If the file is not in the current folder, or in a folder on the MATLAB® path, specify the full pathname.

The text string fmt specifies the format of the file by its standard file extension. For example, specify 'gif' for Graphics Interchange Format files. To see a list of supported formats, with their file extensions, use the imformats function. If imread cannot find a file named filename, it looks for a file named filename.fmt.

The return value A is an array containing the image data. If the file contains a grayscale image, A is an M-by-N array. If the file contains a TrueColor image, A is an M-by-N-by-3 array.

I = rgb2gray(RGB): converts the TrueColor image RGB to the grayscale intensity image I. rgb2gray converts RGB images to grayscale by eliminating the hue and saturation information while retaining the luminance.

BW = dither(I): converts the grayscale image in the matrix I to the binary (black and white) image BW by dithering.

subplot(m,n,p): divides the current figure into an m-by-n grid and creates an axes in the grid position specified by p. MATLAB® numbers its grids by row, such that the first grid is the first column of the first row, the second grid is the second column of the first row, and so on.

imshow(I): displays the image I in a Handle Graphics® figure, where I is a grayscale, RGB (TrueColor), or binary image. For binary images, imshow displays pixels with the value 0 (zero) as black and 1 as white.

Y = fft2(X):returns the two-dimensional discrete Fourier transform (DFT) of X. The DFT is computed with a fast Fourier transform (FFT) algorithm. The result, Y, is the same size as X.

If the dimensionality of X is greater than 2, the fft2 function returns the 2-D DFT for each higher dimensional slice of X. For example, if size(X) = [100 100 3], then fft2 computes the DFT of X(:,:,1), X(:,:,2) and X(:,:,3).

B = imfilter(A,h) filters the multidimensional array A with the multidimensional filter h. The array A can be logical or a no sparse numeric array of any class and dimension. The result B has the same size and class as A.

h = fspecial('average', hsize) returns an averaging filter h of size hsize. The argument hsize can be a vector specifying the number of rows and columns in h, or it can be a scalar, in which case h is a square matrix. The default value for hsize is [3 3].

I = mat2gray(A, [amin amax]) converts the matrix A to the intensity image I. The returned matrix I contains values in the range 0.0 (black) to 1.0 (full intensity or white). amin and amax are the values in A that correspond to 0.0 and 1.0 in I. Values less than amin become 0.0, and values greater than amax become 1.0.

[r c p]=size() returns the size of row vector, column vector and no of planes of the input image.

B = reshape(A,m,n) or B = reshape(A,[m n]) returns the m-by-n matrix B whose elements are taken column-wise from A. An error results if A does not have m*n elements

CONCLUSION

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.