

# **WAVELET BASED IMAGE WATERMARKING USING ARITHMETIC CODING**

Enrollment No. - 101267

Name of Student - Prachi Arora

Name of Supervisor - Mr. Amit kumar Singh



Submitted in partial fulfillment of the Degree of  
Bachelor of Technology

**DEPARTMENT OF COMPUTER SCIENCE  
JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY  
WAKNAGHAT**

## TABLE OF CONTENTS

<b>Chapter No.</b>	<b>Topics</b>	<b>Page No.</b>
	Certificate from the Supervisor	IV
	Acknowledgement	V
	Summary	VI
Chapter-1	1 Digital Image Watermarking	1
	1.0 Data Hiding: Introduction	1
	1.0.1 History of Data Hiding	1
	1.0.2 Need Of Data Hiding	1-2
	1.0.3 Data hiding Techniques	2-3
	1.1 Watermarking	3-4
	1.2 Definition of Watermarking	4
	1.3 Principle of Watermarking	4-5
	1.4 Characteristics of watermarks	5
	1.4.1 Imperceptibility	5
	1.4.2 Robustness	6
	1.4.3 Tamper-resistance	6
	1.4.4 Key Restrictions	6
	1.4.5 Capacity or Data Payload	6
	1.4.6 Computational cost	6
	1.4.7 Modification and multiple watermarks	6
	1.4.8 Security	7
	1.4.9 Effectiveness	7
	1.5 Applications Of Watermarking	7
	1.5.1 Copyright Protection	7
	1.5.2 Authentication	7
	1.5.3 Broadcast Monitoring	7
	1.5.4 Content Labeling	7
	1.5.5 Tamper Detection	7
	1.5.6 Digital Fingerprinting	8
	1.5.7 Content protection	8
	1.5.8 Medical	8
	1.6 Types Of Watermarking	8
	1.6.1 Visible	8
	1.6.2 Invisible	8
	1.6.2.1 Robust Watermarks	8

1.6.2.2	Fragile Watermarks	9
1.6.2.3	Public and Private Watermark	9
1.7	Classification Of Watermarking	9
1.7.1	Text watermarking	9
1.7.2	Image Watermarking	9-10
1.7.3	Audio Watermarking	10
1.7.4	Video Watermarking	10-11
1.8	Techniques or Schemes of Watermarking	11
1.8.1	Spatial Domain Techniques	11
1.8.1.1	Least Significant Bit Coding (LSB)	11
1.8.2	Frequency Domain techniques	11
1.8.2.1	Discrete cosine transform (DCT) based technique:	11-12
1.8.2.1.1	DCT –I	12
1.8.2.1.2	DCT –II	12-14
1.8.2.1.3	Basic Steps	14-15
1.8.2.1.4	Block Diagram	15
1.8.2.2	Wavelet Transform based Watermarking	15-16
1.9	Attacks on Watermarks	16
1.9.1	Basic	16
1.9.2	Robustness	16
1.9.3	Presentation	16-17
1.9.4	Interpretation	17
1.9.5	Implementation	17
1.9.6	Removal	17-18
1.9.7	Geometrical	18
1.9.8	Cryptographic	18
1.9.9	Active & Passive	18
1.9.10	Forgery	18
1.9.11	Collusion	19
1.9.12	Distortive	19
1.10	Performance Metrics	19
1.10.1	PSNR (Peak signal to noise ratio)	19
1.10.2	MSE (Mean square error)	19-20
1.10.3	NCC (Normalized cross correlation)	20
1.10.4	BER (bit error rate)	20
1.11	Image Compression	20
1.11.1	Image compression process	21
1.11.2	Image Compression Techniques	21

	1.11.2.1	Lossless compression technique	21
	1.11.2.1.1	Run length encoding	22
	1.11.2.1.2	Huffman encoding:	22
	1.11.2.1.3	Arithmetic encoding	22-24
	1.11.2.2	Lossy compression technique	24
	1.11.2.2.1	Transformation Coding	24
	1.11.2.2.2	Vector Quantization	25
	1.11.2.2.3	Fractal Coding	25
	1.11.2.2.4	Block truncation coding	25
	1.11.2.2.5	Sub band coding	25
Chapter 2	2	Literature Review	26
	2.0	Literature Survey	26-31
Chapter 3	3	Proposed Method for Image Watermarking using Arithmetic Coding	32
	3.0	Proposed algorithm	32
	3.0.1	Embedding	32
	3.0.2	Extraction	32
	3.1	Block Diagrams	33
	3.1.1	Watermark Embedding	33
	3.1.2	Watermark Extraction	33
Chapter 4:		Experiment and Results	34
	4.0	Results	34-37
	4.1	Conclusion and future Direction	37
		Reference	38-39
		Appendix	40-46

## CERTIFICATE

This is to certify that the work titled “**Wavelet based Image Watermarking using Arithmetic Coding**” submitted by “**Prachi Arora**” in partial fulfillment for the award of degree of B.Tech of Jaypee University of Information Technology, Waknaghat has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor .....  
Name of Supervisor      Mr. Amit Kumar Singh  
Designation                Assistant Professor  
Date                                .....

## **ACKNOWLEDGEMENT**

I take this opportunity to express my profound gratitude and deep regards to my guide **Mr. Amit Kumar Singh**, Assistant Professor, Dept of CSE and ICT for his exemplary guidance, monitoring and constant encouragement throughout the work on this project. Without his blessing, help and guidance this project could not have been completed.

I would like to express my special gratitude and thanks to **Prof. Dr. Satya Prakash Ghreera**, Head of Dept. of CSE and ICT for his kind co-operation and encouragement.

Last but not the least I express my warm thanks to my respected parents and all my friends for their support and their constructive suggestions, which enabled me to bring improvements in my project.

Signature of the student .....  
Name of Student Prachi Arora  
Date .....

## SUMMARY

The recent growth in computer networks, and more specifically, the World Wide Web, has allowed multimedia data such as images to be easily distributed over the Internet. However, many publishers may be reluctant to show their work on the Internet due to a lack of security. The data which is distributed can be replicated easily without error, putting the rights of their owners at risk. Digital watermarks have been proposed as a way to tackle this issue. A digital watermark is an invisible signature embedded inside an image to show authenticity and ownership. An effective digital watermark should be perceptually invisible to prevent obstruction of the original image. It should be statistically invisible to prevent detection, and it should also be robust to many image manipulations, such as filtering, additive noise, and compression.

In this project a watermarking algorithm is implemented for digital images using discrete wavelet transform (DWT) and arithmetic coding. The watermark which is a string of characters is compressed using arithmetic coding because of its high coding efficiency. This compressed watermark is then embedded into the host cover image. The various performance factors like peak signal to noise ratio (PSNR) are analyzed by changing the sub band decomposition level, gain factor etc and applying different attacks which gives different results on different values.

---

Signature of Student

Name:

Date:

---

Signature of Supervisor

Name:

Date:

# **CHAPTER 1: DIGITAL IMAGE WATERMARKING**

## **1.0 DATA HIDING: INTRODUCTION**

Data hiding is referred to as a process to hide messages such as images, videos, maps, text, etc into cover media imperceptibly. That is data hiding links two sets of data, a set of embedded data and another set of cover media data. The relationship between these two sets of data characterizes different applications. For instance in covert communications, the hidden data may often be irrelevant to cover media. In authentication, however, the embedded data is closely related to the cover media.

### **1.0.1 HISTORY OF DATA HIDING**

It is often thought that communications may be secured by encrypting the traffic, but this is not really true in practice. The history teaches that is better hiding messages rather than enciphering them, because it arouses less suspicion. This preference persists in many operational contexts till up this day: an encrypted e-mail message between an employee of a defence contractor and the embassy of a hostile power, for example, may have obvious implications. So the study of communications security includes not just encryption but also traffic security, whose essence lies in hiding information. Data information hiding is a multidisciplinary discipline that combines image and signal processing with cryptography, communication theory, coding theory, signal compression, and the theory of visual and audio perception. First techniques included invisible ink, secret writing using chemicals, templates laid over text messages, microdots, changing letter/word/line/paragraph spacing, changing fonts. Images, video, and audio files provide sufficient redundancy for effective data hiding. Postscript files, PDF files, and HTML can also be used for non-robust data hiding to a limited extent. Executable files, provide very little space for data hiding fonts.

### **1.0.2 NEED OF DATA HIDING**

Two important uses of data hiding in digital media are to provide proof of the copyright, and assurance of content integrity. Even if that signal is subjected to manipulation such as degrading by filtering, resampling, cropping, or lossy data compression the data should stay hidden in the



host signal. Other applications of data hiding, such as the inclusion of augmentation data, need not be invariant to detection or removal, since these data are there for the benefit of both the author and the content consumer. The need of data hiding is in the following mentioned fields.

- Covert communication using images (secret message is hidden in a carrier image).
- Ownership of digital images, authentication and copyright.
- Data integrity, fraud detection, self-correcting images.
- Traitor-tracing (fingerprinting video-tapes).
- Adding captions to images, additional information, such as subtitles, to video, embedding subtitles or audio tracks to video (video-in-video).
- Intelligent browsers, automatic copyright information, viewing a movie in a given rated version.
- Copy control (secondary protection for DVD).

### 1.0.3 DATA HIDING TECHNIQUES

Data hiding can be mainly divided into three processes - cryptography, steganography and watermarking.

**Cryptography** is the process of converting information to an unintelligible form i.e. scrambling the messages so that only the authorized person with the key can decipher it. Cryptography is defined as the art and science of secret writing. As many advances were made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods were designed to offer better security than what cryptography could offer. This led to the discovery of steganography and watermarking.

**Steganography** is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker. The importance of steganography was recently reconsidered by governments with regard to Internet security. The purpose of Stenography is to conceal the message such that the very existence of the hidden is 'camouflaged'. In stenography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

**Watermarking** is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a

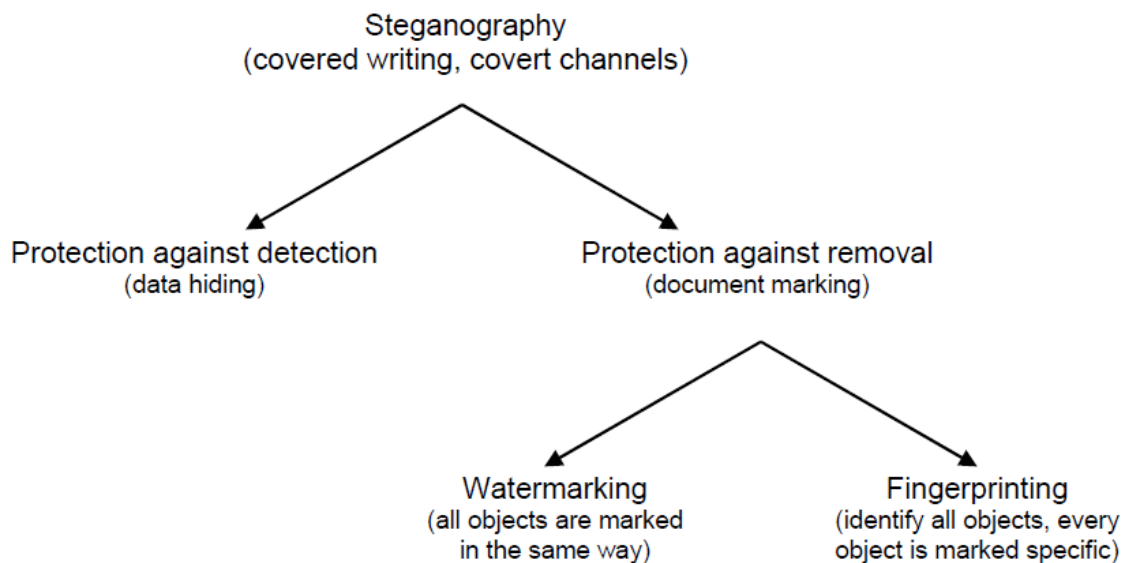
message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Steganography mainly aims for imperceptibility to human senses whereas digital watermarking tries to control the robustness as top priority. Watermarking focuses mainly on the protection of intellectual property rights and the authentication of digital media.

## 1.1 WATERMARKING

The history of watermark dates back to the 13th century. Watermarks were used to indicate the paper brand and the mill that produced it in Italy. By the 18th century watermarks began to be used as anti- counterfeiting measures on money and other documents and in 1995 interest in digital watermarking began to mushroom. Intense research has been carried out in this field for the past few years which has led to the discovery of various algorithms. Throughout this report some of these techniques are discussed and one such technique is implemented.

A **digital watermark** is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication.

Watermarking is closely related to Steganography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication. Figure 1.1 explains how watermarking is derived from Steganography.



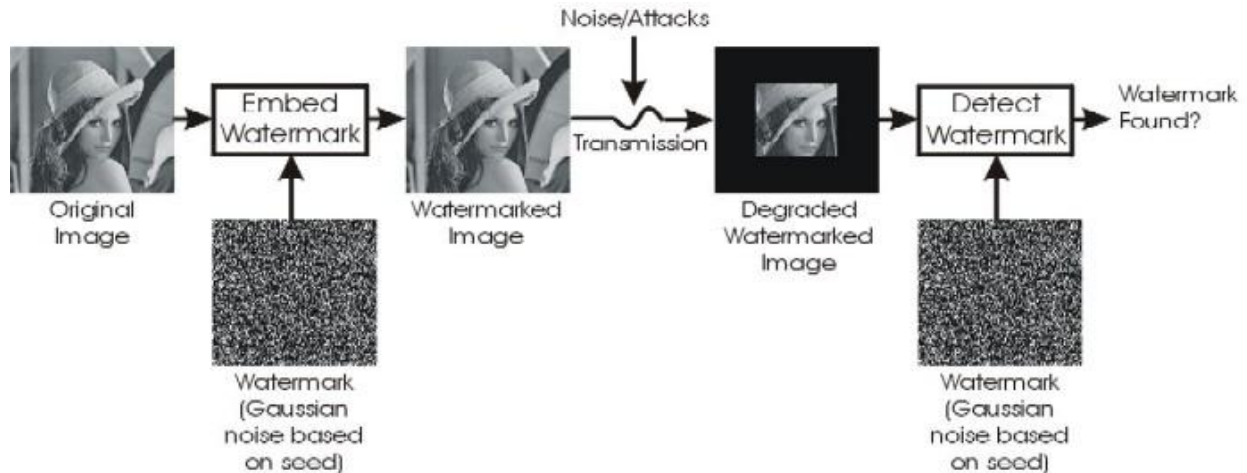
**Figure 1.1: Types of steganography**

## **1.2 DEFINITION OF WATERMARKING**

Digital watermarking is the method of embedding a digital signal (audio, video or image) with information which cannot be removed easily.

## **1.3 PRINCIPLE OF WATERMARKING**

There are three steps involved in the watermarking system, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored. Any modification through this transmission is an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If no modification was made during this transmission the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding is done by manipulating the content of the digital data, which means the information is carried with the signal itself and not embedded in the frame around the data. Figure 2 shows the basic block diagram of watermarking process.



**Fig.1.2 Watermarking block diagram**

There are various embedding techniques currently available, using one of them the desired watermark is embedded in the original image. The watermark is retrieved from the watermarked image by passing it through a decoder in which usually a reverse process to that employed during the embedding stage is applied. The different techniques differ in the way in which it embeds the watermark on to the cover object. In order to prevent illegal access to the watermark a secret key is used during the embedding and the extraction process.

## 1.4 CHARACTERISTICS OF WATERMARKS

There are various important characteristics that watermarks have:

**1.4.1 Imperceptibility:** It is the characteristic of hiding a watermark so that it is not noticeable to the viewer and it should not degrade the visual quality of the image. If visible distortions are introduced in the image, it creates suspicion and makes life easy for the attacker. Also the commercial value of the image is degraded. A closely related term is fidelity.

**1.4.2 Robustness:** Music, images and video signals may undergo many types of distortions. For example, an image might be contrast enhanced and colors might be altered somewhat, or an audio signal might have its bass frequencies amplified. In general, a watermark must be robust to transformations that include common signal distortions as well as digital-to-analog and analog-

to-digital conversion and lossy compression. Moreover, for images and video, it is important that the watermark survive geometric distortions such as translation, scaling and cropping.

**1.4.3 Tamper-resistance:** Watermarks are often required to be resistant to signal processing that is solely intended to remove them, in addition to being robust against the signal distortions that occur in normal processing. This property is referred to as tamper- resistance.

**1.4.4 Key Restrictions:** an important distinguishing characteristic is the level of restriction placed on the ability to read a watermark. Watermarks in which the key is available to a very large level of detectors is called as “unrestricted key” watermarks and those in which keys are kept secret by one or a small number of detectors are called as “restricted-key ” watermarks.

**1.4.5 Capacity or Data Payload:** Data payload of a watermark is the amount of information it contains. As with any method of storing data, this can be expressed as a number of bits, which indicates the number of distinct watermarks that might be inserted into a signal. If the watermark contains  $N$  bits the there are  $2^N$  different possible watermarks.

**1.4.6 Computational cost:** As with any technology intended for commercial use, the computational cost of inserting and detecting watermarks is important. This is particularly true when watermarks need to be inserted or detected in real-time video or audio.

**1.4.7 Modification and multiple watermarks:** In some circumstances, it is desirable to alter the watermark after insertion. For example, in the case of digital video discs, a disc may be watermarked to allow only a single copy. Once this copy has been made, it is then necessary to alter the watermark on the original disc to prohibit further copies. Changing a watermark can be accomplished by either (i) removing the .rst watermark and then adding a new one or (ii) inserting a second watermark such that both are readable, but one overrides the other.

**1.4.8 Security:** it is the ability of watermark to resist malicious attacks. These attacks include intentional operations of watermark insertion, modification, removal and estimation which aim at defeating the purpose of the watermarks.

**1.4.9 Effectiveness:** It is perhaps the most important property of a watermark. Effectiveness is the probability that the message in a watermarked image will be correctly detected. We ideally need this probability to be 1.

## **1.5 APPLICATIONS OF WATERMARKING**

**1.5.1 Copyright Protection:** This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Digital watermarking can be used to identify and protect copyright ownership.

**1.5.2 Authentication:** Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.

**1.5.3 Broadcast Monitoring:** As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.

**1.5.4 Content Labeling:** Watermarks can be used to give more information about the cover object. This process is named content labeling.

**1.5.5 Tamper Detection:** Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

**1.5.6 Digital Fingerprinting:** This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.

**1.5.7 Content protection:** In this process the content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.

**1.5.8 Medical:** Due to security issues in management of medical information, the watermarking techniques are used in medicals to complete the existing measures for protecting medical images. It has become an important issue in medical image security, confidentiality and integrity.

## **1.6 TYPES OF WATERMARKING**

On the basis of human perception the watermarks are of two types Visible and Invisible

### **1.6.1 Visible**

The watermark is visible which can be a text or a logo used to identify the owner. Visible watermarks change the signal altogether such that the watermarked signal is totally different from the actual signal.

### **1.6.2 Invisible**

The watermark is embedded into the image in such a way that it cannot be perceived by human eye. It is used to protect the image authentication and prevent it from being copied. Invisible watermark can be further divided into three types,

#### **1.6.2.1 Robust Watermarks**

Invisible watermark cannot be manipulated without disturbing the host signal. This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks.

#### **1.6.2.2 Fragile Watermarks**

These watermarks are very sensitive. They can be destroyed easily with slight modifications in the watermarked signal. They are designed with very low robustness. They are used to check the integrity of objects.

### **1.6.2.3 Public and Private Watermark**

They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original image is not known during the detection process then it is called a public or a blind watermark and if the original image is known it is called a non blind watermark or a private watermark.

## **1.7 CLASSIFICATIONS OF WATERMARKING**

On the basis of the type of the document watermarking can be classified as Text, Image, Audio, and Video.

### **1.7.1 Text watermarking:**

Digital watermarking provides authentication and copyright protection for multimedia contents over the internet. Text is one of the most important medium traveling over the internet hence it needs to be protected. Text watermarking techniques that have been developed in past protects the text from illegal copying, forgery, and prevents copyright violations. Text watermarking is an approach for text document copyright protection. Watermarking ensures that a text document carries secret message containing copyright information so that copyright infringed can be recognized. Text watermarking is a process to embed a watermark into text document .

### **1.7.2 Image Watermarking:**

As the increasing of the electronic publishing, the data distribution is becoming faster, and requiring less effort to make copies. One of the major challenges is that of discouraging unauthorized copying and distributing electronic documents. In order to trace the unauthorized copies, it has been suggested to sign the image with a signature or copyright message. Such message must be secretly embedded and no visible difference between the coded image and the original image could be perceived. Besides, a robust signature coding approach should survive several possible attacks, such as image processing and lossy image compression. Fragile watermarking is a technique to insert a signal or logo for image authentication. The signature will be altered when the host image is manipulated. An effective authentication scheme must be able to determine whether an image is altered or not, able to locate any alteration made on the



image, able to integrate authentication data with host image and the embedded authentication data should be invisible under normal viewing conditions.

### **1.7.3 Audio Watermarking**

An audio watermark is a unique electronic identifier embedded in an audio signal, typically used to identify ownership of copyright. One of the most secure techniques of audio watermarking is spread spectrum audio watermarking (SSW). In SSW, a narrow-band signal is transmitted over a much larger bandwidth such that the signal energy presented in any signal frequency is undetectable. Thus the watermark is spread over many frequency bands so that the energy in one band is undetectable. An interesting feature of this watermarking technique is that destroying it requires noise of high amplitude to be added to all frequency bands. SSW is a robust watermarking technique because, to eliminate it, the attack must affect all possible frequency bands with modifications of considerable strength. This creates visible defects in the data. Spreading spectrum is done by a pseudo noise (PN) sequence. In conventional SSW approaches, the receiver must know the PN sequence used at the transmitter as well as the location of the watermark in the watermarked signal for detecting hidden information. This is a high security feature, since any unauthorized user who does not have access to this information cannot detect any hidden information. Detection of the PN sequence is the key factor for detection of hidden information from SSW. Although PN sequence detection is possible by using heuristic approaches such as evolutionary algorithms, the high computational cost of this task can make it impractical.

### **1.7.4 Video Watermarking**

Watermarks are used to introduce an invisible signal into a video to ease the detection of illegal copies. This technique is widely used by photographers. Placing a watermark on a video such that it is easily seen by an audience allows the content creator to detect easily whether the image has been copied. The limitation of watermarks is that if the original image is not watermarked, then it is not possible to know whether other images are copies. Video watermarking involves embedding cryptographic information derived from frames of digital video into the video itself. Ideally, a user viewing the video cannot perceive a difference between the original, unmarked video and the marked video, but a watermark extraction application can read the watermark and

obtain the embedded information. Because the watermark is part of the video, rather than part of the file format, this technology works independently of the video file format.

## **1.8 TECHNIQUES OR SCHEMES OF WATERMARKING**

### **1.8.1 Spatial Domain Techniques**

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression.

#### **1.8.1.1 Least Significant Bit Coding (LSB)**

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component.

### **1.8.2 Frequency Domain techniques:**

#### **1.8.2.1 Discrete cosine transform (DCT) based technique:**

Discrete cosine transform (DCT): It is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to set of n coefficients. A linear combination of n known basis vectors weighted with the n coefficients will result in the original vector. The known basis vectors of transforms from this class are “sinusoidal“, which means that they can be represented by sinus shaped waves or, in other words, they are strongly localized in the frequency spectrum. Therefore one speaks about transformation to the frequency domain. The most popular member of this class is the Discrete Fourier Transformation (DFT). The difference between DCT and DFT is that DFT applies to complex numbers, while DCT uses just real numbers. For real input data with even symmetry

DCT and DFT are equivalent. There are eight different variants of DCT. There is a very slight modification between these eight variants.

### 1.8.2.1.1 DCT –I

In JPEG compression the input data are two-dimensional, presented in 8x8 blocks. There's a need of using two-dimensional DCT. Since each dimension can be handled separately, the two-dimensional DCT follows straightforward form the one-dimensional DCT. A one-dimensional DCT is performed along the rows and then along the columns, or vice versa. The formula used for one-dimensional DCT:

$$F(u) = C(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2N}\right]$$

where  $u=0,1,\dots,N-1$

$$C(u) = \sqrt{\frac{1}{N}} \text{ when } u=0 \quad C(u) = \sqrt{\frac{2}{N}} \text{ when } u \neq 0$$

### 1.8.2.1.2 DCT –II

The formula used for two-dimensional DCT:

$$F(u, v) = C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x, y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2M}\right]$$

where  $u=0,1,\dots,N-1$   $v=0,1,\dots,M-1$

$$C(u), C(v) = \sqrt{\frac{1}{N}} \text{ when } u, v=0 \quad C(u), C(v) = \sqrt{\frac{2}{N}} \text{ when } u, v \neq 0$$

Applying these formulas directly requires much computational resources therefore an implementation in hardware can be very efficient.

The figure below shows example of 8x8 blocks before DCT.

75	76	75	75	69	66	77	71
73	74	73	74	63	64	68	69
69	68	71	72	67	58	48	41
59	55	56	52	47	40	24	9
51	50	45	41	33	22	7	-5
43	37	32	24	15	5	-6	-25
29	21	9	-2	-10	-21	-44	-69
9	-4	-17	-35	-52	-61	-57	-35

After Discrete Cosine Transform the block has following values:

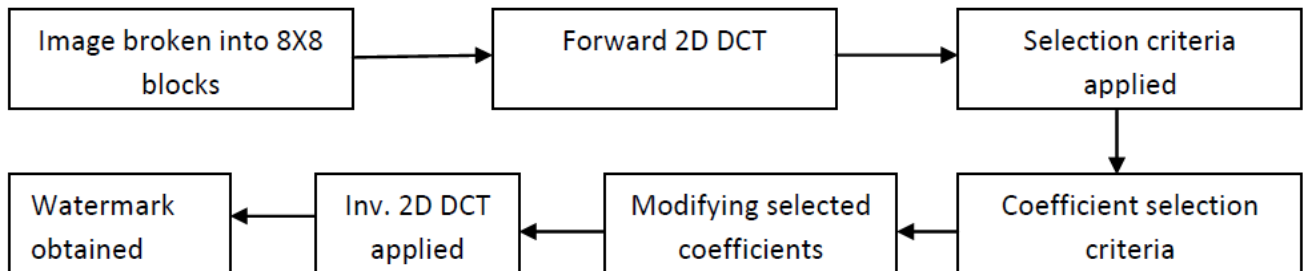
251	118	-13	6	-2	6	-1	0
279	-68	-8	-7	-1	4	-4	-1
-51	-14	34	-14	5	0	-1	0
27	5	-10	8	-7	4	-5	1
-22	-7	14	-9	4	-2	1	1
-3	15	-18	15	-6	2	-1	2
7	-9	6	-6	4	0	0	2
3	7	-9	3	0	-2	-1	0

As you can see only small amount of low frequency elements dominates over the rest of the coefficients. It allows reducing data during next stages of JPEG compression. The main advantage of DCT which makes it attractive for watermarking is its energy compaction property. This property divides the image into distinct frequency bands which makes it easy to embed the watermark in the desired area of the image. Most of the energy in the DCT domain is concentrated in the low frequencies. As is known low frequencies are perceived very well by human eye, hence the chances of the watermark being perceptible is high where as high frequencies are prone to attacks such as compression and scaling. So, a tradeoff has to be made.

### 1.8.2.1.3 Basic Steps:

1. The image is segmented into non-overlapping blocks of 8x8.
2. Forward DCT is applied to each of the block.
3. Selection criteria are then applied.
4. This is followed by applying coefficient selection criteria.
5. Embed watermark by modifying the selected coefficients.
6. Inverse DCT is applied to obtain the final watermarked image.

### 1.8.2.1.4 Block Diagram:



**Fig.1.3 Block diagram of watermarking steps using DCT**

### 1.8.2.2 Wavelet Transform based Watermarking

The Fourier transform is an analysis of global frequency content in the signal. There are applications in digital image processing wherein we need the localized frequency components. This can be done by using the Short Time Fourier Transform. This is similar to the concept of using windowing functions. The windowed transform is given as

$$F(\omega, \alpha) = \int_{-\infty}^{\infty} f(x)g(x - \alpha) e^{-j\omega x} dx$$

Where ‘w’ denotes the frequency and ‘alpha’ denotes the position of the window.

This equation transforms the signal f(x) in a small window around ‘alpha’. The STFT is then performed on the signal and local information is extracted. The wavelet transform based watermarking technique divides the image into four sidebands – a low resolution approximation of the tile component and the component’s horizontal, vertical and diagonal frequency characteristics. The process can then be repeated iteratively to produce N scale transform.



**Fig.1.4 Wavelet based transforms**

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the human visual system (HVS) as compared to the DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, and HH}. Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on

image quality. One of the most straightforward techniques is to use embedding technique similar to that used in the DCT,

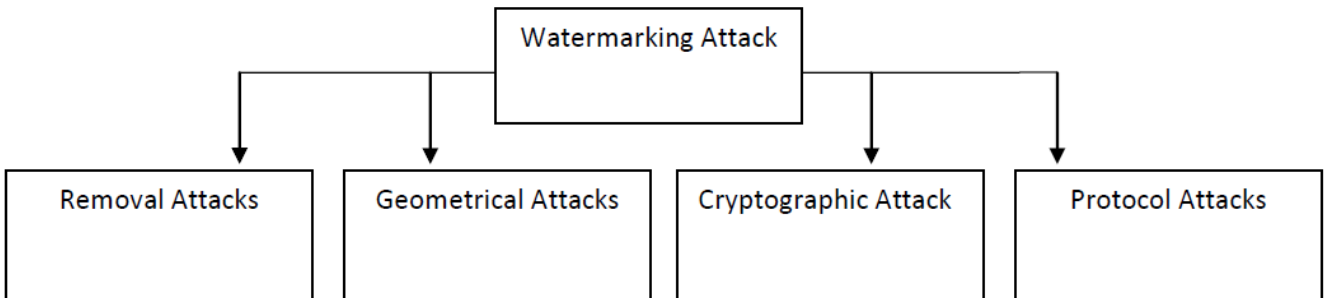
$$I_{w_{u,v}} = \begin{cases} W_i + \alpha |W_i| x_i, & u, v \in HL, LH \\ W_i & u, v \in LL, HH \end{cases}$$

In the Wavelet Domain where  $W_i$  denotes the coefficient of the transformed image,  $x_i$  the bit of the watermark to be embedded, and  $\alpha$  a scaling factor. To detect the watermark the same process as that used in DCT is implemented. Furthermore, as the embedding uses the values of the transformed value in embedded, the embedding process should be rather adaptive; storing the majority of the watermark in the larger coefficients. This method provides resistance to JPEG compression, cropping, and other types of attacks.

### 1.9 ATTACKS ON WATERMARK

In watermarking terminology, an “attack” is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. Digital watermarking is not as secure as data encryption. Therefore, digital watermarking is not immune to hacker attacks. An important aspect of any watermarking scheme is its robustness against attacks. A watermark is robust if it cannot be impaired without also rendering the attacked data useless. An attack succeeds in defeating a watermarking scheme if it impairs the watermark beyond acceptable limits while maintaining the perceptual quality of the attacked data.

Watermarking attacks are broadly divided into the following categories:



**Fig 1.5 Types of Watermark Attacks**

### **1.9.1 Basic**

In basic attack, the attacker takes advantage of the limitations in design of the embedding technique. As the name suggests the attack is very basic and can be easily resolved.

### **1.9.2 Robustness**

This may include removal attacks where the attacker aims at removal of the watermark from the cover data. Also the attacker may try to diminish the data.

### **1.9.3 Presentation**

These attacks modify the content of the file in order to prevent the detection of the watermark. The mosaic attack takes advantage of size requirements for embedding a watermark. By splitting the marked file into small sections, the mark detection can be confused. Many web browsers will draw images together with no visible split enabling the full image to be effectively restored while hiding the mark. If the minimum size for embedding the mark is small enough the mosaic attack is not practical. This attack can defeat web crawlers which download pictures from the Internet and check them for the presence of a watermark.

### **1.9.4 Interpretation**

These attacks find a situation where ownership certification is prevented. They rely on misinterpretation the data to comply with ownership certification.

### **1.9.5 Implementation**

This method Attacks the detection software. A marking system can provide more opportunities for attack than the marking technique itself. If the mark detection software is vulnerable it may be possible for attackers to deceive it.

### **1.9.6 Removal**

This category includes de-noising, lossy compression, quantization, demodulation, collusion and averaging attacks. Removes watermark from cover signal.



Removal Attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm i.e. without the key used for watermark embedding. Sophisticated removal attacks try to impair the embedded watermark as much as possible while keeping the quality of the attacked document high enough. These include demodulation, collusion and lossy compression.

### **1.9.7 Geometrical**

In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained. However, the complexity of the required synchronization process might be too great to be practical. However, most recent watermarking methods survive these attacks due to the use of special synchronization techniques. Robustness to global affine transformations is more or less a solved issue. Therefore, pixels are locally shifted, scaled, and rotated without significant visual distortion. However, it is worth noting that some recent methods are able to resist this attack.

### **1.9.8 Cryptographic**

If the image is watermarked such that it needs a key to decipher, brute force attacks are used for exhaustive search to find the key to decipher. These are called cryptographic attacks. Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks.

### **1.9.9 Active & Passive**

Attacker removes or spoils the watermark. Attacker just identifies the watermark and does not damage it.

### **1.9.10 Forgery**

Attacker forges new watermark and replaces the old one with the new one. The original watermarked image is replaced by the attacker which may look like the original image but is not the original data, thereby misleading the end receiver.

### 1.9.11 Collusion

In this type of attack the attacker decodes different copies with different watermarks and joins them to make one single watermark. In such a case, a successful attack can be achieved by averaging all copies or taking only small parts from each different copy.

### 1.9.12 Distortive

Attacker applies distortive transformation to make the watermark undetectable by any other person & making it unreadable by the end receiver.

## 1.10 PERFORMANCE METRICS

The performance metric is used to determine the behavior, quality and performance of the watermarked image. In this, the watermarked image is compared with the cover image and then its quality is determined.

### 1.10.1 PSNR (PEAK SIGNAL TO NOISE RATIO)

The PSNR (peak signal to noise ratio) is used to determine the degradation in the embedded image with respect to the host image. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image [21]. The higher the PSNR, the better the quality of the compressed or reconstructed image.

It is calculated by the formula as

$$\text{PSNR} = 10 \log_{10}(L^2/MSE)$$

L is the peak signal value of the cover image

### 1.10.2 MSE (MEAN SQUARED ERROR)

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

$$MSE = \frac{1}{XY} \sum_{i=1}^X \sum_{j=1}^Y (c(i,j) - e(i,j))^2$$

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

### 1.10.3 NCC (NORMALISED CROSS CORRELATION)

Normalized correlation describes the similarity between extracted watermark and the original watermark signal [21].

$$NCC = \frac{\sum_{i=1}^M \sum_{j=1}^N w(i,j)w'(i,j)}{\sum_{i=1}^M \sum_{j=1}^N w(i,j)^2}$$

Where  $w(i,j)$  and  $w'(i,j)$  represent the original watermark image and extracted watermark image respectively.

### 1.10.4 BER (BIT ERROR RATE)

Bit error rate is used to quantify a channel carrying data by counting the rate of errors in a data string. It is a key parameter used in accessing the system. When data is embedded into the image, there is a possibility of error being introduced into a watermarked image. As a result, it is necessary to assess the performance and quality of the watermarked image, and bit error rate, BER, provides an ideal way in which this can be achieved [21].

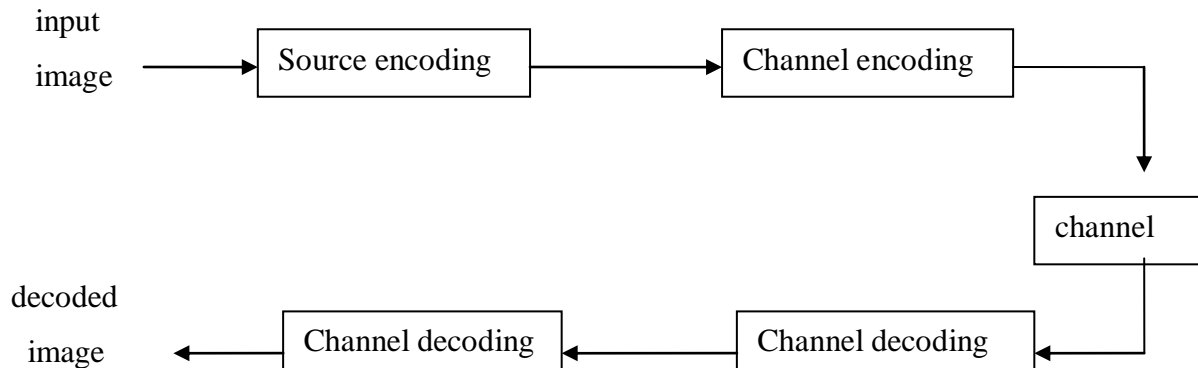
$$\text{Bit Error Rate, BER} = \frac{\text{Number of errors}}{\text{Total number of bits sent}}$$

## 1.11 IMAGE COMPRESSION

Image compression addresses the problem of reducing the amount of data required to represent a digital image which is a major issue of today with the transfer requirements over the internet. The image compression is a conversion from higher dimensional space to lower dimensional space. The image compression plays an important role in multimedia application such as storage and transmission. The basic rule of image compression is to represent an image with minimum number of bits of accepted image quality. In most of application high quality image data require

large amount of storage space and transmission bandwidth. So with the compression schemes we can compress the information so that storage space and transmission time can be reduced.

### 1.11.1 Image compression process



The goal of source coding is efficient conversion of source data into a sequence of bits. The source codes reduce the entropy (measure of information content) which means decrease in the average number of bits required to represent the image.

The purpose of channel encoder is to protect the communication system against noise and other transmission error in the channel.

### 1.11.2 Image Compression Techniques

The image compression techniques are broadly classified into two categories depending whether or not an exact replica of the original image could be reconstructed using the compressed image .

These are:

1. Lossless technique
2. Lossy technique

#### 1.11.2.1 Lossless compression technique

In lossless compression techniques, the original image can be perfectly recovered from the compressed (encoded) image. These are also called noiseless since they do not add noise to the signal (image). Lossless compression is preferred in case of medical images but the compression ratio is less.

$$\text{Compression Ratio} = \frac{\text{output file size}}{\text{input}}$$

Following techniques are included in lossless compression:

**1.11.2.1.1. Run length encoding :** This is a very simple compression method used for sequential data. It is very useful in case of repetitive data. The term run is used to indicate the repetition of symbol while the term run length is used to represent the number of repeated symbol. So the run length coding replaces sequences of identical symbols (pixels) ,called runs by shorter symbols.

**1.11.2.1.2. Huffman encoding:** This is a general technique for coding symbols based on their statistical occurrence frequencies (probabilities). The pixels in the image are treated as symbols. The Huffman coding scheme maps one symbol to one code word. The symbols that occur more frequently are assigned a smaller number of bits, while the symbols that occur less frequently are assigned a relatively larger number of bits. Most image coding standards use lossy techniques in the earlier stages of compression and use Huffman coding as the final step.

**1.11.2.1.3. Arithmetic encoding:** The Huffman coding scheme encode one symbol one symbol at a time and each symbol translates into an integer number of bits so failed to achieve optimal efficiency. The Huffman coding assigns variable length code to a fixed group of symbols. Arithmetic code assigns variable length code to a variable group of symbols. In this all the symbols in the message are considered together to assign a single arithmetic code.

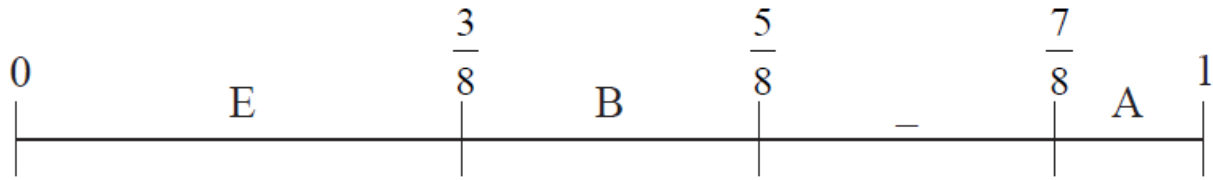
Example:

Given string: BE\_A\_BEE compress it using arithmetic coding.

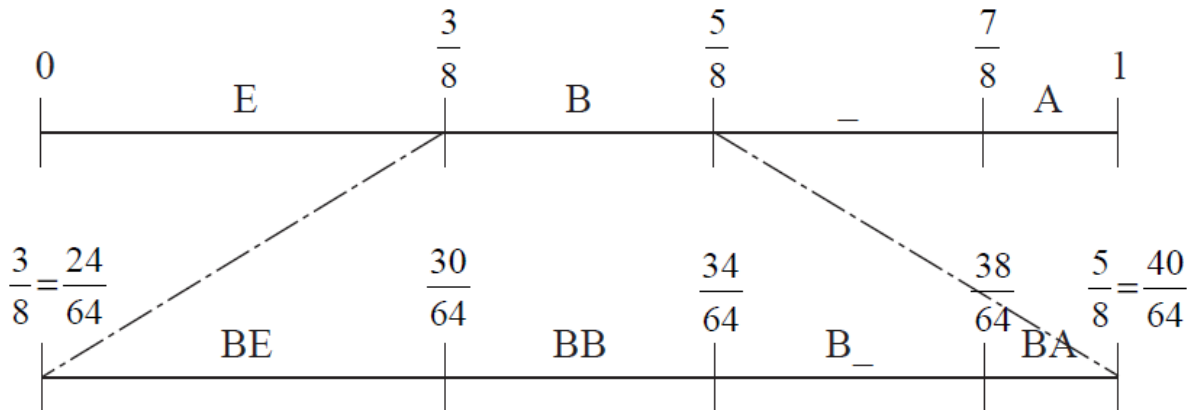
Firstly, calculate the frequency counts for the different letter

E	B	_	A
-----			
3	2	2	1

Then we encode the string by dividing up the interval [0,1] and allocate each letter an interval whose size depends on how often it occurs in the string.



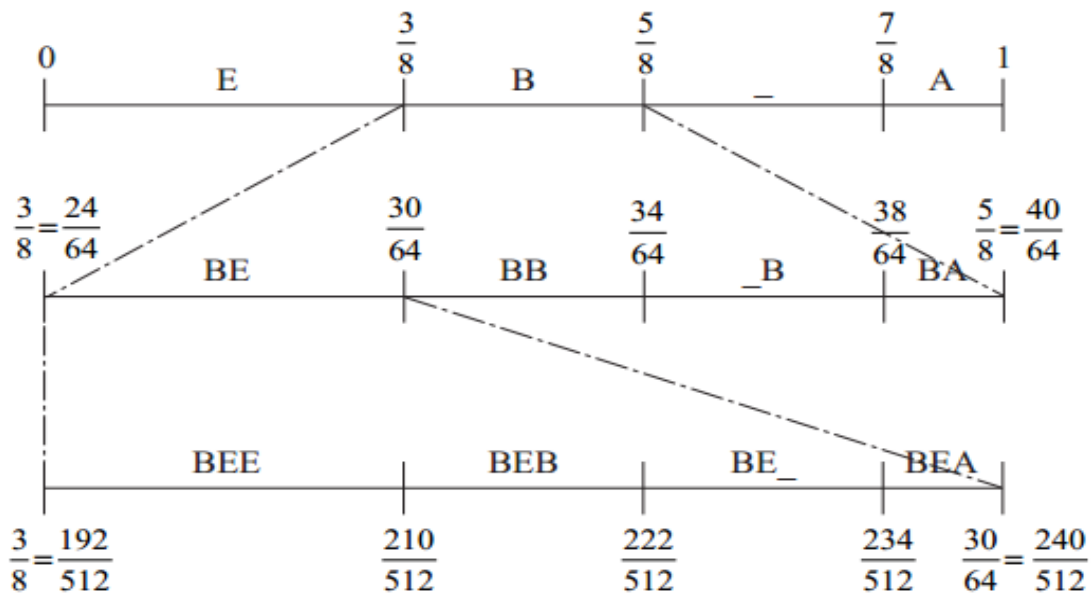
Our string starts with a 'b', so we take the 'B' interval and divide it up again in the same way.



The boundary between 'BE' and 'BB' is  $\frac{3}{8}$  of the way along the interval, which is itself  $\frac{2}{8}$  long and starts at  $\frac{3}{8}$ . So the boundary is  $\frac{30}{64}$ . Similarly the boundary between 'BB' and 'B\_' is  $\frac{34}{64}$ .

The second letter in the message is 'E', so now we subdivide the 'E' interval in the same way.

We carry on through the message.



And continuing in this way we obtain,

$$\frac{7653888}{16777216} \qquad \qquad \qquad \frac{7654320}{16777216}$$

BE\_A\_BEE

So, we represent the message as any number in the interval

$$\left[ \frac{7653888}{16777216}, \frac{7654320}{16777216} \right)$$

However, we cannot send number like  $7654320/16777216$  easily using a computer. Computer use binary numbers- a system where all the numbers are made up of 0s and 1s. so it is converted into binary to be sent and stored in a computer.

### 1.11.2.2 Lossy compression technique

Lossy schemes provide much higher compression ratios than lossless schemes. Lossy schemes are widely used since the quality of the reconstructed images is adequate for most applications .By this scheme, the decompressed image is not identical to the original image, but reasonably close to it. Lossy compression techniques includes following schemes:

**1.11.2.2.1. Transformation Coding:** In this coding scheme, transforms such as DFT (Discrete Fourier Transform) and DCT (Discrete Cosine Transform) are used to change the pixels in the original image into frequency domain coefficients (called transform coefficients).These coefficients have several desirable properties. One is the energy compaction property that results in most of the energy of the original data being concentrated in only a few of the significant transform coefficients. This is the basis of achieving the compression. Only those few significant coefficients are selected and the remaining are discarded. The selected coefficients are considered for further quantization and entropy encoding. DCT coding has been the most common approach to transform coding. It is also adopted in the JPEG image compression standard.

**1.11.2.2.2 Vector Quantization:** The basic idea in this technique is to develop a dictionary of fixed-size vectors, called code vectors. A vector is usually a block of pixel values. A given image is then partitioned into non-overlapping blocks (vectors) called image vectors. Then for each in the dictionary is determined and its index in the dictionary is used as the encoding of the original image vector. Thus, each image is represented by a sequence of indices that can be further entropy coded.

**1.11.2.2.3 Fractal Coding:** The essential idea here is to decompose the image into segments by using standard image processing techniques such as color separation, edge detection, and spectrum and texture analysis. Then each segment is looked up in a library of fractals. The library actually contains codes called iterated function system (IFS) codes, which are compact sets of numbers. Using a systematic procedure, a set of codes for a given image are determined, such that when the IFS codes are applied to a suitable set of image blocks yield an image that is a very close approximation of the original. This scheme is highly effective for compressing images that have good regularity and self-similarity.

**1.11.2.2.4 Block truncation coding:** In this scheme, the image is divided into non overlapping blocks of pixels. For each block, threshold and reconstruction values are determined. The threshold is usually the mean of the pixel values in the block. Then a bitmap of the block is derived by replacing all pixels whose values are greater than or equal (less than) to the threshold by a 1 (0). Then for each segment (group of 1s and 0s) in the bitmap, the reconstruction value is determined. This is the average of the values of the corresponding pixels in the original block.

**1.11.2.2.5 Sub band coding:** In this scheme, the image is analyzed to produce the components containing frequencies in well-defined bands, the sub bands. Subsequently, quantization and coding is applied to each of the bands. The advantage of this scheme is that the quantization and coding well suited for each of the sub bands can be designed separately.



## Chapter 2: LITERATURE REVIEW

### 2.0 LITERATURE SURVEY

Before getting into the details of the proposed algorithm variety of researchers and scholars have proposed their working research materials on watermarking that employees different techniques such as techniques like Singular Value Decomposition, Discrete Cosine Transform, Discrete Wavelet Transform and a combination of spatial domain and transform domain techniques etc. The researches on various techniques by different researchers are briefly described below.

Guorong Xuan et al.[1] has proposed a data hiding algorithm based on Integer Wavelet transform a. After the hidden data have been extracted, the original image can be recovered without any distortion from the marked image. This algorithm hides the data and the overhead data representing the bookkeeping information into a middle bit-plane of the integer wavelet coefficients in high frequency sub bands. High frequency sub bands is chosen to have a high PSNR value. In the chosen bit-plane(s) of the high frequency sub bands, the arithmetic coding is chosen to losslessly compress binary 0s and 1s because of its high coding efficiency and thus the cover image can embed much more data as compared with the existing distortionless data hiding techniques. The imperceptibility requirement is thus satisfied. The secret key is used to make the hidden data remaining in secret even after the algorithm is known to the public. The image histogram modification is used to prevent grayscales from possible overflowing. The algorithm has been applied to a wide range of different images successfully. The experimental results are presented below to demonstrate the validity of the algorithm. The proposed distortion-free data embedding technique is able to embed about 15k-94k bits into a grayscale image of  $512 \times 512 \times 8$  imperceptibly, that is much more than what the existing techniques can do. Also the lossless recovery of original image is achieved. The invertible data hiding has wide applications in practice such as in the medical field and law enforcement.

Pratibha Sharma et. al [2] has discussed a digital image watermarking based on 3 level discrete wavelet transform (DWT) and compared with 1 & 2 levels DWT. In this technique a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. During embedding, watermark image is dispersed within the original image depending upon the scaling factor of alpha blending technique. Extraction of the watermark image is done by using same scaling factor as for embedding. Performance of method for

different value of scaling factor is analysed & compared with 1 & 2 levels DWT method by using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE). Experiment results show that the quality of the watermarked image is dependent only on the scaling factors and the recovered watermark is independent of scaling factor. Results show that the recovered images and the watermark are better for 3 level discrete wavelet transform than 1 & 2 level discrete wavelet transform.

Ali al Haj et. al [3] has proposed an imperceptible and a robust combined DWT-DCT digital image watermarking algorithm. The rapid increase of digitized media in today's world has enforced the development of copyright enforcement technologies to protect copyright ownership of multimedia objects. One of the techniques to do this is digital watermarking that has been developed to protect digital images from illegal manipulations. In particular, digital image watermarking algorithms which are based on the discrete wavelet transform have been widely recognized to be more prevalent than others. This is due to the wavelets' excellent spatial localization, frequency spread, and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. The proposed algorithm watermarks a given digital image using a combination of the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). Watermarking is done by altering the wavelets coefficients of carefully selected sub bands followed by the application of the DCT transform on the selected sub bands. Performance evaluation results show that combining the two transforms improved the performance of the watermarking algorithms that are based solely on the DWT transform. Ibrahim Nasir et. al [4] has discussed a new robust watermarking scheme for color images based on block probability in spatial domain. A binary watermark image is permuted using sequence numbers generated by a secret key and gray code and then embedded four times in different positions by a secret key. Each bit of the binary encoded watermark is embedded by modifying the intensities of a non-overlapping block of  $8 \times 8$  of the blue component of the host image. Extraction of the watermark is by comparing the intensities of a block of  $8 \times 8$  of the watermark and the original images and calculating the probability of detecting '0' or '1'. Experimental results show that the proposed scheme is robust and secure against a wide range of image processing schemes.

K.A. Navas et. al [5] has discussed a watermarking technique that satisfies the requirements of medical images like imperceptibility, high capacity and high robustness. Past works on data

hiding, watermarking and steganography are not reliable in all aspects. Electronic Patient Report (EPR) data hiding for telemedicine demand it blind and reversible. This paper discusses a blind reversible data hiding based on Integer wavelet transform. In blind reversible data hiding it is desired to retrieve the embedded patient data without original image and embedded media can be reversed to the original cover media without any distortion after the hidden data are recovered. EPR is embedded into Region of Background (ROB) excluding ROI. Data is hidden in ROB to avoid erroneous diagnosis. Integer wavelet transform allows to construct lossless wavelet transform which is important for reversible data hiding, further integer to integer transformation results in better computational complexity and lesser transmission time. Number of floating point operations is reduced hence more efficient. Data is embedded into the first level high frequency sub bands of image namely HL, LH. Experimental results show a large value of PSNR further the proposed method also has large capacity which is important for EPR data hiding.


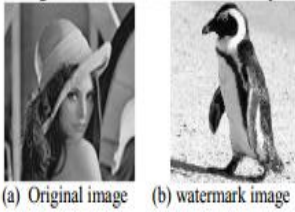


Guorong Xuan et.al [6] has discussed a reversible data hiding method based on wavelet spread spectrum and histogram modification. Data is embedded in the coefficients of Integer Wavelet Transform in high frequency sub bands because wavelet transform coefficients are highly decorrelated and are consistent with the feature of the HVS (Human Visual System). Slight modification of wavelet transform coefficients in high frequency sub bands is hard to be perceived by human eyes. Integer Wavelet transformation maps integer to integer and can reconstruct the original media without any distortion. Data hiding efficiency is enhanced by embedding the pseudo bits also. Histogram modification is used to prevent overflow and underflow. The presented method has superior performance in terms of high data embedding capacity and high visual quality of marked images.

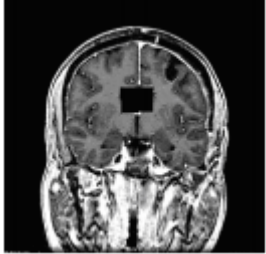

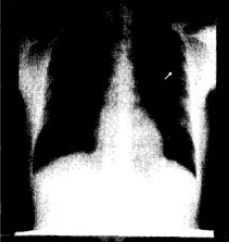
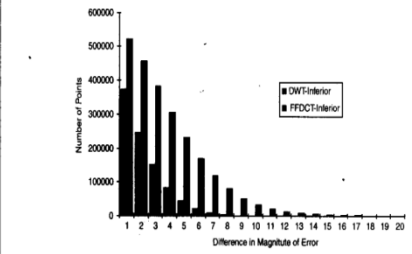

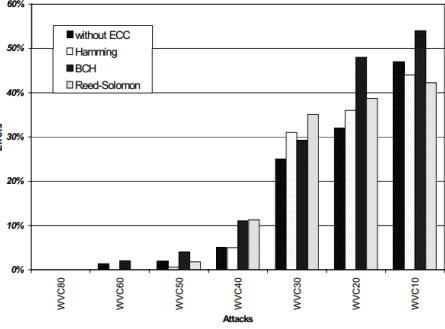
Pongsorn Saipetch et.al [7] has developed a compression algorithm based on discrete wavelet transforms (DWTs) and arithmetic coding (AC) that satisfies the requirements of Radiological archives. These images need to be compressed at a moderate compression ratio between 10: 1 to 20: 1 while retaining good diagnostic quality. Compression is achieved by transforming the picture into wavelet coefficients and then encoding the coefficients using arithmetic coding with order-1 model for execution speed. The wavelet transform is implemented using a linear phase biorthogonal transform, which does not need phase compensation in pyramidal implementation. Arithmetic coding is chosen over Huffman and LZW for encoding the coefficients because of its optimal performance without blocking of input data and its clean separation between modeling

the data and the encoding of information according to the model. Since radiological images usually contain artificial edges (labels, lettering, and cropping), FFDCT introduces ripple artifact due to truncation of high frequency coefficients. JPEG introduces blocking artifact due to independent error across the block boundaries. Diagnostic ability is degraded by both FFDCT ripples and JPEG block artifacts. This new method is superior to the previously developed full frame discrete cosine transform (FFDCT) method, as well as the industrial standard developed by the joint photographic expert group (JPEG). Since DWT is localized in both spatial and scale domains, the error due to quantization of coefficients does not propagate throughout the reconstructed picture as in FFDCT. Because it is a global transformation, it does not suffer the limitation of block transform methods such as JPEG. The severity of the error as measured by the normalized mean square error (NMSE) and maximum difference technique increases very slowly with compression ratio. Normalized nearest neighbor difference (NNND), which is a measure of blockiness, stays approximately constant, while JPEG NNND increases rapidly with compression ratio. Furthermore, DWT has an efficient finite response filter FIR implementation that can be put in parallel hardware. DWT also offers total flexibility in the image format; the size of the image does not have to be a power of two as in the case of FFDCT.

Nataša Terzija et. Al [8] has the influence of different error correction codes on the robustness of image watermarks is investigated. To encode the watermark three different error correction codes are considered: the Hamming, the BCH and the Reed-Solomon code. Following the idea of the JPEG2000 standard the encoded watermark is embedded by a method based on Discrete Wavelet Transform (DWT). Availability of the original image is presumed for extraction. The sensitivity against attacks on the watermarked image is investigated. The types of attacks applied are: the removal, denoising and compression attack. It is shown that the Hamming and the Reed-Solomon code yield better results than the BCH code. Due to the higher correction capability the Reed-Solomon code behaves better than the Hamming code.

**Table 2.1: Details of Literature review**

S. no	Author Name	Technique	Image Details	Results																																							
1	Guorong Xuan, Jidong Chen, Jiang Zhu	IWT and Arithmetic coding	 <p>Pepper image</p>	<table border="1"> <tr> <td>PSNR of marked image (dB)</td> <td>Pay-load (bits)</td> </tr> <tr> <td>29.11</td> <td>69,285</td> </tr> </table>	PSNR of marked image (dB)	Pay-load (bits)	29.11	69,285																																			
PSNR of marked image (dB)	Pay-load (bits)																																										
29.11	69,285																																										
2	Pratibha Sharma	3 level Discrete Wavelet Transform	 <p>(a) Original image (b) watermark image</p>	<table border="1"> <thead> <tr> <th></th> <th>q</th> <th>PSNR</th> <th>MSE</th> </tr> </thead> <tbody> <tr> <td>0.2</td> <td>0.009</td> <td>7.92</td> <td>10506.29</td> </tr> <tr> <td>0.5</td> <td>0.009</td> <td>12.07</td> <td>4032.757</td> </tr> <tr> <td>0.75</td> <td>0.009</td> <td>18.30</td> <td>961.776</td> </tr> <tr> <td>0.85</td> <td>0.009</td> <td>23.01</td> <td>324.854</td> </tr> <tr> <td>0.99</td> <td>0.009</td> <td>48.23</td> <td>0.976</td> </tr> <tr> <td>1.25</td> <td>0.009</td> <td>17.50</td> <td>1157.003</td> </tr> </tbody> </table>		q	PSNR	MSE	0.2	0.009	7.92	10506.29	0.5	0.009	12.07	4032.757	0.75	0.009	18.30	961.776	0.85	0.009	23.01	324.854	0.99	0.009	48.23	0.976	1.25	0.009	17.50	1157.003											
	q	PSNR	MSE																																								
0.2	0.009	7.92	10506.29																																								
0.5	0.009	12.07	4032.757																																								
0.75	0.009	18.30	961.776																																								
0.85	0.009	23.01	324.854																																								
0.99	0.009	48.23	0.976																																								
1.25	0.009	17.50	1157.003																																								
3	Ali Al-Haj	Combined DWT-DCT	 <p>Lena Image</p>	<table border="1"> <thead> <tr> <th></th> <th>DWT-Only (HL2)</th> <th>DWT-DCT (HL2)</th> <th>DWT-Only (HH2)</th> <th>DWT-DCT (HH2)</th> </tr> </thead> <tbody> <tr> <td>PSNR</td> <td>80.1 90</td> <td>97.0 72</td> <td>77.0 98</td> <td>97.0 83</td> </tr> </tbody> </table>		DWT-Only (HL2)	DWT-DCT (HL2)	DWT-Only (HH2)	DWT-DCT (HH2)	PSNR	80.1 90	97.0 72	77.0 98	97.0 83																													
	DWT-Only (HL2)	DWT-DCT (HL2)	DWT-Only (HH2)	DWT-DCT (HH2)																																							
PSNR	80.1 90	97.0 72	77.0 98	97.0 83																																							
4	Ibrahim Nasir, Ying Weng,	A new spatial domain-watermarking scheme based on a block probability	 <p>a)Original Image b) Watermark Image</p>	<table border="1"> <thead> <tr> <th rowspan="2">Attack method</th> <th colspan="2">Somchok's method</th> <th colspan="2">Proposed method</th> </tr> <tr> <th>Lena</th> <th>Peppers</th> <th>Lena</th> <th>Peppers</th> </tr> </thead> <tbody> <tr> <td>PSNR dB</td> <td>32.21</td> <td>32.32</td> <td>38.92</td> <td>39.10</td> </tr> <tr> <td>Median filter 3*3</td> <td>0.99</td> <td>1.00</td> <td>1.00</td> <td>1.00</td> </tr> <tr> <td>JPEG 75%</td> <td>0.99</td> <td>0.99</td> <td>0.82</td> <td>0.72</td> </tr> <tr> <td>JPEG 50%</td> <td>0.99</td> <td>0.99</td> <td>0.55</td> <td>0.50</td> </tr> <tr> <td>Rotate</td> <td>0.84</td> <td>0.81</td> <td>1.00</td> <td>1.00</td> </tr> <tr> <td>Scaling</td> <td>0.94</td> <td>0.92</td> <td>1.00</td> <td>0.65</td> </tr> </tbody> </table>	Attack method	Somchok's method		Proposed method		Lena	Peppers	Lena	Peppers	PSNR dB	32.21	32.32	38.92	39.10	Median filter 3*3	0.99	1.00	1.00	1.00	JPEG 75%	0.99	0.99	0.82	0.72	JPEG 50%	0.99	0.99	0.55	0.50	Rotate	0.84	0.81	1.00	1.00	Scaling	0.94	0.92	1.00	0.65
Attack method	Somchok's method		Proposed method																																								
	Lena	Peppers	Lena	Peppers																																							
PSNR dB	32.21	32.32	38.92	39.10																																							
Median filter 3*3	0.99	1.00	1.00	1.00																																							
JPEG 75%	0.99	0.99	0.82	0.72																																							
JPEG 50%	0.99	0.99	0.55	0.50																																							
Rotate	0.84	0.81	1.00	1.00																																							
Scaling	0.94	0.92	1.00	0.65																																							

5	K.A Navas, S. Archana Thampy, and M. Sasikumar	IWT		<table border="1"> <tr> <td>PSNR (db)</td> <td>BER</td> </tr> <tr> <td>44</td> <td>0</td> </tr> </table>	PSNR (db)	BER	44	0										
PSNR (db)	BER																	
44	0																	
6	Guorong Xuan et.al	Spread spectrum scheme,IWT, Histogram modification	 <p style="text-align: center;">Barbara</p>	<p style="text-align: center;">Payload VS PSNR of marked "Barbara" image</p> <table border="1"> <tr> <td>Payload (bpp)</td> <td>0.1</td> <td>0.2</td> <td>0.3</td> <td>0.4</td> <td>0.5</td> <td>0.6</td> </tr> <tr> <td>PSNR (dB)</td> <td>48.67</td> <td>45.18</td> <td>41.78</td> <td>39.03</td> <td>36.10</td> <td>30.87</td> </tr> </table>	Payload (bpp)	0.1	0.2	0.3	0.4	0.5	0.6	PSNR (dB)	48.67	45.18	41.78	39.03	36.10	30.87
Payload (bpp)	0.1	0.2	0.3	0.4	0.5	0.6												
PSNR (dB)	48.67	45.18	41.78	39.03	36.10	30.87												
7	Pon skorn Saipetch, Bruce K.T. Ho, Marco Ma	DWT and arithmetic coding	 <p style="text-align: center;">A chest radiograph</p>	 <p style="text-align: center;">Distribution of the error magnitude comparison between DWT and FFDCT</p>														
8	Nataša Terzija, Markus Repges, Kerstin Luck	DWT and Error correction codes	 <p style="text-align: center;">University Image</p>	 <p style="text-align: center;">Impact of ECCs after wavelet compression</p>														

## **CHAPTER 3: PROPOSED METHOD FOR IMAGE WATERMARKING USING ARITHMETIC CODING**

### **3.0 Proposed Algorithm:**

#### **3.0.1 Embedding**

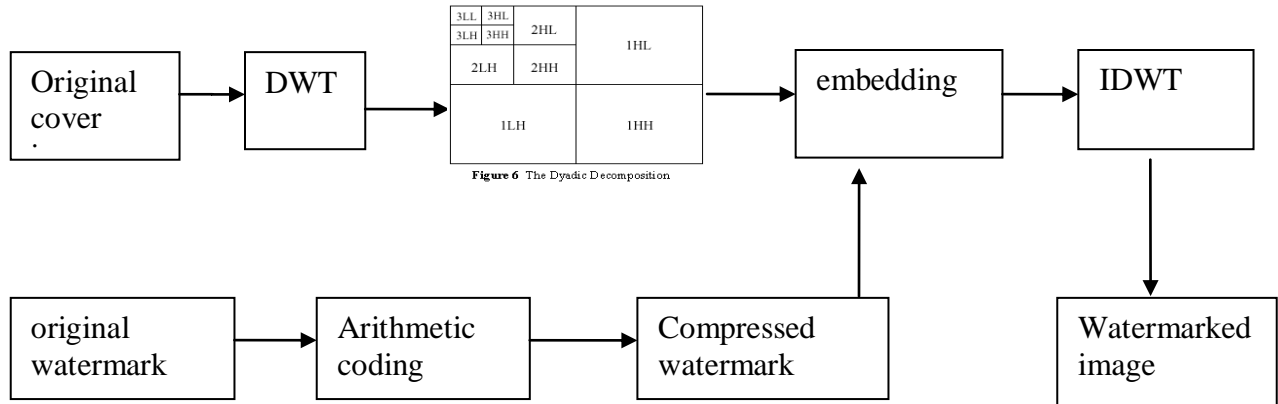
1. The cover image is first decomposed into several bands using the discrete wavelet transformation (DWT).
2. The arithmetic coding is used to losslessly compress the watermark because of its high coding efficiency.
3. This compressed watermark is then embedded in the low frequency subband (LL) of the image to get the watermarked image.
4. Various attacks like Gaussian noise, salt and pepper noise etc are applied on the watermark image to check the robustness of the watermarking system.

#### **3.0.2 Extraction**

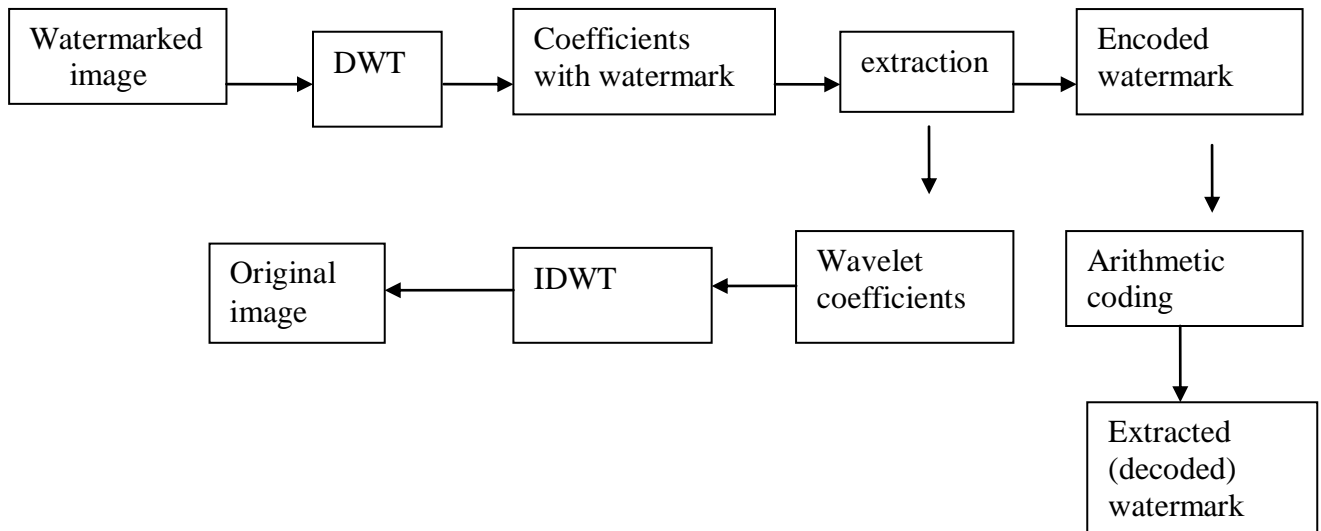
1. The watermark is extracted from the watermarked image which is in compressed form.
2. This encoded watermark is then decoded by applying arithmetic decoding to get the original watermark.
3. Performance parameters like PSNR (peak signal to noise ratio) and BER (bit error rate) are then computed and the results are recorded.

### 3.1 Block Diagrams

#### 1) Watermark embedding



#### 2) Watermark extraction







## CHAPTER 4: EXPERIMENTS AND RESULTS

### 4.0 RESULT

- Table 4.1 shows the value of PSNR and BER for a random text sequence of 469 bits. the watermark is losslessly extracted as there is no distortion and so the BER is also equal to zero. The value of PSNR is much above 40 which indicates our proposed algorithm is efficient.

**Table 4.1: The value of PSNR and BER for a given text sequence of 469 bits**

Original image	Watermark	Watermarked image	Extracted watermark	PSNR	BER
 <b>Lena image</b>	my name is prachi arora. Student of fourth year studying Btech CSE.  <b>Text sequence (469 bits)</b>	 <b>Watermarked Lena image</b>	my name is prachi arora. student of fourth year studying Btech CSE.  <b>Text sequence (469 bits)</b>	<b>49.03696</b>	<b>0</b>

- Table 4.2 shows the length of the original watermark and compressed watermark in bits. Arithmetic coding has a high coding efficiency and compresses data considerably so that large amount of data can be embedded inside the original cover image.







**Table 4.2 The length of the original watermark and compressed watermark**

Text Sequence	Original Watermark Length (bits)	Compressed Watermark length (bits)
my name is prachi arora. Student of fourth year studying Btech CSE.	<b>469</b>	<b>290</b>
my name is prachi arora	<b>168</b>	<b>92</b>

prachi arora	84	39
--------------	----	----

- Different attacks have been applied on the watermarked image like salt & pepper, Gaussian noise, median filter and speckle. The value of PSNR and BER is recorded and shown in Table 4.3

**Table 4.3 Different attacks have been applied on the image and the value of PSNR and BER is recorded**

Attack	Original Image	Watermarked image	Noise Factors	PSNR	BER
Salt & pepper			0.01	39.29238	176
			0.001	43.950	135
			0.0001	45.988	0
Gaussian noise			M=0.0005 V=0.001	35.608	179
			M=0 V=0.00001	46.73	171
			M=10 <sup>-9.6</sup> V=10 <sup>-9.6</sup>	48.848	0
Median filter			-	39.92	182

<b>Speckle noise</b>			V=0.04 N=0.02	<b>34.694</b>	<b>199</b>
			V= 0.0001 n=0.00001	<b>48.22</b>	<b>151</b>

- The value of gain factor used while embedding is changed and corresponding values of PSNR and BER are recorded. It is seen as the gain factor is reduced the value of PSNR increases. The value of BER is zero for all the cases as the embedded watermark is correctly extracted.

**Table 4.4 The value of PSNR and BER for different value of gains**

<b>Gain</b>	<b>PSNR</b>	<b>BER</b>
<b>0.1</b>	<b>39.036961</b>	<b>0</b>
<b>0.01</b>	<b>44.036961</b>	<b>0</b>
<b>0.001</b>	<b>49.036961</b>	<b>0</b>

- The DWT is first performed in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is used as the input. To perform DWT on 2 level we perform DWT on LL1 & for 3Level decomposition we applied DWT on LL2 & finally we get 4 subband of 3 level that are LL3, LH3, HH3, HL3. Watermarking is applied on the different sub levels and table 4.5 shows the value of PSNR and BER for it. It is seen that the value of PSNR decreases as the level of decomposition increases. But the watermark is more robust in the higher level of decomposition. Value of BER is zero.

**Table 4.5 the value of PSNR and BER for different level of decomposition**

<b>Levels</b>	<b>PSNR</b>	<b>BER</b>
<b>Level 1</b>	<b>51.995557</b>	<b>0</b>
<b>Level 2</b>	<b>50.318562</b>	<b>0</b>
<b>Level 3</b>	<b>49.036961</b>	<b>0</b>

#### **4.1 CONCLUSION AND FUTURE DIRECTION**

In the proposed work, the host cover image is transformed using discrete wavelet transform. the watermark which is a text sequence is losslessly compresses using Arithmetic coding and embedded in the transformed cover image. Compressing the watermark allows us to embed large amount of data into the host cover image. The performance of this algorithm is seen by calculating the value of PSNR and BER. The robustness of the algorithm is checked by applying different attacks and seeing the performance metrics for the same.

The future work of this project is to apply this algorithm on image, audio and video watermarks and see its performance on them.

## REFERENCES

- [1] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni and W. Su, "Distortionless data hiding based on integer wavelet transform," IEE Electronics Letters, December (2002) 1646-1648.
- [2] Pratibha Sharma, Shanti Swami, "Digital Image Watermarking Using 3 level Discrete Wavelet Transform," Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013).
- [3] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking," Journal of Computer Science 3 (9): 740-746, 2007 ISSN 1549-3636.
- [4] Ibrahim Nasir, Ying Weng, Jianmin Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain,"
- [5] K. A. Navas, S. Archana Thampy, and M. Sasikumar," EPR Hiding in Medical Images for Telemedicine," World Academy of Science, Engineering and Technology Vol:2 2008-02-20.
- [6] G. Xuan, C. Yang, Y. Zheng, Y. Q. Shi and Z. Ni, "Reversible data hiding based on wavelet spread spectrum," IEEE International workshop on multimedia signal processing (MMSP2004), Sept. 2004, Siena, Italy.
- [7] Pon skorn Saipetch, Bruce K.T. Ho, Ramesh Panwar, Marco Ma, and Jun Wei, "Applying Wavelet Transforms with Arithmetic Coding to Radiological Image Compression," IEEE ENGINEERING IN MEDICINE AND BIOLOGY, September/October 1995, 0739-5175/95/\$4.000 1995
- [8] Nataša Terzija, Markus Reppes, Kerstin Luck, Walter Geisselhardt, "Digital image watermarking using discrete wavelet transform: Performance comparison of error correcting code".

[9] Josep Domingo-Ferrer and Francesc Sebé, “Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images”, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC.02).

[10] Nikita Kashyap Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT) I.J.Modern Education and Computer Science, 2012, 3, 50-56 Published Online April 2012 in MECS.

[11] Subramanya A, “Image Compression Technique,” Potentials IEEE, Vol. 20, Issue 1, pp 19-23, Feb-March 2001.

[12] David Jeff Jackson & Sidney Joel Hannah, “ Comparative Analysis of image Compression Techniques,” System Theory 1993, Proceedings SSST 93, 25th Southeastern Symposium,pp 513-517, 7 –9 March 1993.

## APPENDIX

### Implementation Code

#### Embedding and Extraction

```
clc;
clear all;
close all;
% COVER IMAGE
img = imread('1.bmp');
img1 = im2double(rgb2gray(img));
img2 = imresize(img1,[512 512]);
figure(1);imshow(img2),title('Cover Image');
[LL,LH,HL,HH] = dwt2(img2,'haar','d');
[LL1,LH1,HL1,HH1] = dwt2(LL,'haar','d');
[LL2,LH2,HL2,HH2] = dwt2(LL1,'haar','d');

% WATERMARK
message=input('Enter the text message sequence: ','s');
mess1= dec2bin(message);

mess2=zeros(1,min(size(mess1))*max(size(mess1)));
jjj=1;
for ii=1:1:max(size(mess1))
for jj = 1:1:min(size(mess1))
    mess2(1,jjj) = mess1(ii,jj);
    jjj=jjj+1;
end
end
for i=1:1:min(size(mess1))*max(size(mess1))
if mess2(1,i)==48
```

```

        mess2(1,i)=0;
else
        mess2(1,i)=1;
end
end
%arithmetic coding
source=unique(message);
counts=zeros(1,length(source));
for i=1:length(source)
    counts(i)=length(strfind(message,source(i)));
end

seq=zeros(1,length(message));

for i=1:length(message)
    seq(i)=strfind(source,message(i));
end

code = arithenco(seq, counts)
code1=code;
code2=length(code1);
XX=length(code);
code3 = zeros(64,64);
x=0;
y = ((XX - mod(XX,64))/64) + 1;
z=1;
for i=1:1:64
for j= 1:1:64
if x+j >XX
break;
end

```



```

        code3(i,j) = code(1,x+j);
end
    x=64*z;
    z=z+1;
if z>y
break;
end
end

seq2=min(size(mess1))*max(size(mess1));
str = sprintf('Original watermark Bits Length = %d ----- Compressed watermark Bits Length =
%d',seq2,code2)

% WATERMARKED IMAGE

wimg = LL2 + 0.001*code3;
wimgl3 = idwt2(wimg,LH2,HL2,HH2,'haar');
wimgl2 = idwt2(wimgl3,LH1,HL1,HH1,'haar');
wimgl1 = idwt2(wimgl2,LH,HL,HH,'haar');

figure(2);

imshow(wimgl1,'DisplayRange',[0,1]),title('Watermarked Image');% L-1');

%% Noise attacks
% Salt & Pepper Noise
salt_img=imnoise(wimgl1,'salt & Pepper',0.5);
figure(3);
imshow(salt_img);title('Salt & Pepper Noise');
title('salt and pepper');
[PSNR_OUT] = psnr(img2,salt_img);

```

```

str = sprintf('PSNR salt & pepper noise = %f,PSNR_OUT);
disp(str);
% Gaussian Noise
M =0.0005;
V=0.001;

% imshow(wimg);title('Original Image');
Gaus_img = imnoise(wimgl1,'gaussian',M,V);
[PSNR_OUT] = psnr(img2,Gaus_img);
str = sprintf('PSNR gaussian noise= %f,PSNR_OUT);
disp(str);

figure(4);
imshow(Gaus_img,'DisplayRange',[]),title('Gaussian Noise');
filt_img = medfilt2(Gaus_img);
figure(5);
imshow(filt_img);title('Median Filtering');
title('Filtered Image');
[PSNR_OUT] = psnr(img2,filt_img);
str = sprintf('PSNR median filter = %f,PSNR_OUT);
disp(str);

%Speckle Noise

V= 0.04;
n=0.02;
spec_img= imnoise(wimgl1,'Speckle',V);
spec_img=wimgl1+n*wimgl1;
figure(6);
imshow(spec_img);title('speckle noise');
[PSNR_OUT] = psnr(img2,spec_img);

```

```

str = sprintf('PSNR speckle = %f',PSNR_OUT);
disp(str);

% cropping
crop_img=imcrop(wimg1);
figure(7);
imshow(crop_img);title('cropping');

%extraction
[wLL,wLH,wHL,wHH] = dwt2(wimg1,'haar','d');
[wLL1,wLH1,wHL1,wHH1] = dwt2(wLL,'haar','d');
[wLL2,wLH2,wHL2,wHH2] = dwt2(wLL1,'haar','d');

ewimg = wLL2 - LL2;

for i=1:1:64
for j=1:1:64
if ewimg(i,j)<0.00005
    ewimg1(i,j) = 0;
else
    ewimg1(i,j) = 1;
end
end
end

ewimg2 = zeros(1,length(code1));
x=0;
z=1;
for i=1:1:64
for j = 1:1:64
if x+j > XX

```

```

break;
end
    ewimg2(1,x+j)=ewimg1(i,j);
end
    x = 64*z;
    z = z+1;
if z>y
break;
end
end

dseq=arithdeco(ewimg2,counts,length(seq));
dec_mess=zeros(1,length(dseq));
for i=1:length(dseq)
    a=dseq(i);
    dec_mess(i)=source(a);
end
char(dec_mess)

dec_mess1=dec2bin(dec_mess);
dec_mess2=zeros(1,min(size(dec_mess1))*max(size(dec_mess1)));
jjj=1;
for ii=1:1:max(size(dec_mess1))
for jj = 1:1:min(size(dec_mess1))
    dec_mess2(1,jjj) = dec_mess1(ii,jj);
    jjj=jjj+1;
end
end
for i=1:1:min(size(dec_mess1))*max(size(dec_mess1))
if dec_mess2(1,i)==48
    dec_mess2(1,i)=0;

```

```

else
    dec_mess2(1,i)=1;
end
end
%BER
count=0;
for i=1:1:min(size(mess1))*max(size(mess1))

if mess2(1,i)~=dec_mess2(1,i);
    count = count + 1;
end

end
ber=count

```

### **PSNR**

```

function [PeakSNR]=psnr(img2,wimg1)
x = 0;
for i=1:1:512
    for j=1:1:512
        x = real(x + (wimg1(i,j)-img2(i,j))/(512*512));
    end
end
PeakSNR = 10 * log10(255/sqrt(x));

```