

WAVELET BASED IMAGE WATERMARKING USING ERROR CORRECTION CODES

Enrol.no:101282

Name: Neetika Luthra

Supervisor: Mr.Amit Kumar Singh



May 2014

Submitted in partial fulfillment of the Degree of

Bachelor of Technology

DEPARTMENT OF COMPUTER SCIENCE

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,

WAKNAGHAT

TABLE OF CONTENTS

Chapter No.	S.No.	Topic	Page No.
		Certificate	II
		Acknowledgement	III
		Abstract	IV
		List of figures	V
		List of tables	VI
Chapter 1		Digital Image Watermarking	
	1.0	Data Hiding: Introduction	1
	1.0.1	History of data hiding	2
	1.0.2	Need of Data Hiding	3
	1.0.3	Information Hiding Techniques	3-5
	1.1	Watermarking	5
	1.2	Principles of watermarking	6
	1.3	Characteristics of digital watermarking	7
	1.4	Applications of Watermarking	8
	1.5	Classification of Watermarking	9
	1.6	Watermark attacks	11
	1.7	Techniques of watermarking	14
	1.8	Performance metrics	20
Chapter 2		Literature Review	
	2.0	Literature Survey	23-29
Chapter 3		Proposed Method for image watermarking using ECC	
	3.0	Error Correcting Codes	30
	3.1	Proposed Method	34
	3.1.1	Embedding process	34
	3.1.2	Extraction process	36
Chapter 4		Experiments and Results	
	4.0	Result	37-44
		Conclusion and Future Direction	45
		Appendix	45-50
		References	51-54

CERTIFICATE

This is to certify that the work titled “**WAVELET BASED IMAGE WATERMARKING USING ERROR CORRECTION CODES**” submitted by “**NEETIKA LUTHRA**” in partial fulfillment for the award of degree of B.Tech. in Computer Science of Jaypee university of Information Technology, Wagnaghat 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:

Designation:

Date:

ACKNOWLEDGMENT

I take this opportunity to express my profound gratitude and deep regards to my guide **Mr. Amit Kumar Singh** for his exemplary guidance, monitoring and constant encouragement throughout the course of the project. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

I also take this opportunity to express a deep sense of gratitude to my Institution, college faculty and staff members for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

I also extend my thanks to the almighty, family and well-wishers.

Signature of student:

Name of student:

Date:

ABSTRACT

Information Technology has eased the duplication, manipulation and distribution of digital data in recent times which has resulted in the demand for safe ownership of digital images. A very crucial concern for the content owners and distributors is copyright protection and content authentication. The solution to these problems is digital watermarking, which is a technique for inserting information into an image and later extracted or detected for variety of purposes including identification and authentication. Watermark must have two most important properties: transparency and robustness. Transparency refers to the perceptual quality of the watermarked data. The watermark should be invisible over all types. Robustness is a most important property of watermark. It means that the watermark is still presented in the image and can be detected after distortion. Ideally, the amount of image distortion necessary to degrade the desired image quality should destruct and remove the watermark in the traditional watermarking without error correction code (ECC). So it is need to enhance the robustness of the embedded watermark by introducing the ECC, which can control the mistake and improve the reliability of data transmission in digital communication. With ECC appending some redundancy bits in the original embedded watermark, the error part of the extracted watermark can be corrected. In the proposed work, the embedding watermarks method based on the discrete wavelet transforms (DWT). Also, error correcting code (ECC) is applied to the ASCII representation of the text and the encoded text watermark is embedded. The performance of the proposed algorithm is evaluated in terms of imperceptibility and robustness against various attacks. The PSNR is used to measure the quality of the watermarked image. However, robustness of the extracted watermark is measured by BER. The proposed algorithm is robust against number of signal processing attacks without much degradation of the image quality.

Signature of Student:

Name:

Date:

Signature of Supervisor

Name:

Date:

List of Figures

Figure No.	Figure Name	Page No.
1.1	Classification of Information Hiding	4
1.2	Types of Steganography	6
1.3	Watermarking Block diagram	7
1.4	Watermark Attacks	12
1.5	Types of attacks	12
1.6	Watermarking techniques	14
1.7	Block Diagram of watermarking using DCT	19
1.8	DWT decomposition with three levels	20
3.1	Categories of Block Coding techniques	30
3.2	Embedding process of DWT with hamming	36
3.3	Extraction process of DWT with hamming	37
4.1	Graph of gain factor vs PSNR	38
4.2	Graph of gain factor vs BER	38

List of Tables

Table No.	Table Name	Page No.
1.1	Difference between Cryptography, Steganography and watermarking	4-5
2.1	Details of literature review	27
3.1	Extra bits for error correction/detection	30
4.1	Comparison between performance of watermark with hamming and without hamming	36
4.2	Comparison against different levels of DWT	37
4.3	Comparison of BER values on different DWT levels by changing the number of bits	38
4.4	Values of BER against different attacks	39

CHAPTER 1: DIGITAL IMAGE WATERMARKING

1.0 DATA HIDING: INTRODUCTION

Data hiding is a technique to embed data into digital media for the purpose of identification, authentication, and copyright. It is the process of hiding information in the image, audio signal or any video. Several constraints affect the process: the quantity of data to be hidden, the need for invariance of all these data under the conditions where a “host” signal is subject to distortions, and the degree to which the data must be immune to interception, modification, or removal by any other third party [1]. I have explored both traditional and novel techniques for addressing the data-hiding process and evaluate these techniques in light of three applications: copyright protection, authentication check, and robustness against attacks. In general term, information hiding is the principle of segregation of the design decisions in the computer program that are most likely to change, thus protecting the other parts of the program from extensive modification if the design decision has changed and increasing the security[2]. The protection involves providing the stable interface which protects the remainder of the program from the implementation. In other words, information hiding is the ability to prevent certain aspects of a class or software component from being accessible to the clients, and keep the information confidential [3].

Data hiding is a software development technique specifically used in object-oriented programming (OOP) to hide internal object information. It is the art of hiding a message into a host signal without any perceptual distortion of it. It is a form of subliminal signal [3]. Data hiding ensures exclusive data access to class members and protects object integrity by preventing unintended or intended alterations. Data hiding also reduces system complexity for increased robustness by limiting interdependencies between software components. Data hiding is also known as data encapsulation or information hiding [4]. Data hiding was introduced as part of the OOP methodology, in which a program is segregated into objects with specific data, functions and information. This technique enhances a programmer’s ability to create classes with unique data sets and functions, avoiding unnecessary penetration from other program classes [5]. Because software architecture techniques rarely differ, there is few

data hiding that contradicts. Data hiding only hides class data components, whereas data encapsulation hides class data parts and private parts.

1.0.1 HISTORY OF DATA HIDING

Information hiding serves as an effective criterion for dividing any piece of equipment, software or hardware, into modules of functionality [3]. For instance a car is a complex piece of equipment. In order to make the design, manufacturing, and maintenance of a car reasonable, the complex piece of equipment is divided into modules with particular interfaces hiding design decisions. By designing a car in this fashion, a car manufacturer can also offer various options while still having a vehicle which is economical to manufacture. For instance, a car manufacturer may have a luxury version of the car as well as a standard version. The luxury version comes with a more powerful engine than the standard version. The engineers designing the two different car engines, one for the luxury version and one for the standard version, provide the same interface for both engines. Both engines fit into the engine bay of the car which is the same between both versions. Both engines fit the same transmission, the same engine mounts, and the same controls. The differences in the engines are that the more powerful luxury version has a larger displacement with a fuel injection system that is programmed to provide the fuel air mixture that the larger displacement engine requires [4].

In addition to the more powerful engine, the luxury version may also offer other options such as a better radio with CD player, more comfortable seats, a better suspension system with wider tires, and different paint colors. With all of these changes, most of the car is the same between the standard version and the luxury version. The radio with CD player is a module which replaces the standard radio, also a module, in the luxury model. The more comfortable seats are installed into the same seat mounts as the standard types of seats. Whether the seats are leather or plastic, or offer lumbar support or not, doesn't matter. The engineers design the car by dividing the task up into pieces of work which are assigned to teams. Each team then designs their component to a particular standard or interface which allows the sub-team flexibility in the design of the component while at the same time ensuring that all of the components will fit together [3].

Motor vehicle manufacturers frequently use the same core structure for several different models, in part as a cost-control measure. Such a "platform" also provides an example of information hiding, since the floor pan can be built without knowing whether it is to be used in a sedan or a hatchback. As can be seen by this example, information hiding provides flexibility. This flexibility allows a programmer to modify functionality of a computer program during normal evolution as the computer program is changed to better fit the needs of users. When a computer program is well designed decomposing the source code solution into modules using the principle of information hiding, evolutionary changes are much easier because the changes typically are local rather than global changes.

Cars provide another example of this in how they interface with drivers. They present a standard interface (pedals, wheel, shifter, signals, gauges, etc.) on which people are trained and licensed. Thus, people only have to learn to drive a car; they don't need to learn a completely different way of driving every time they drive a new model of car.

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. Therefore, the data should stay hidden in a host signal, even if that signal is subjected to manipulation as degrading as filtering, resampling, cropping, or lossy data compression[2]. 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. Thus, the techniques used for data hiding vary depending on the quantity of data being hidden and the required invariance of those data to manipulation. Since no one method is capable of achieving all these goals, a class of processes is needed to span the range of possible applications [3].

1.0.3 INFORMATION HIDING TECHNIQUES

Information hiding can be mainly divided into three processes - cryptography, steganography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. As many advances were made in the field of communication it became rather simple to decrypt a cipher text [7]. 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 [8]. Thus even the existence of secret information is not known to the attacker. 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 [3]. Figure 1.1 shows the classification of information hiding.

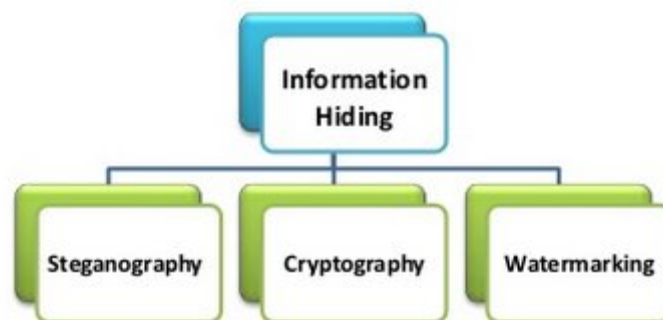


Fig1.1: Classification of Information Hiding [4]

Table 1.1: Difference between Cryptography, Steganography and Watermarking

Property – Technique	Cryptography	Steganography	Digital Watermarking
Carrier , Secret Data , Key And Output	Information is encrypted in text/image file	Payload is embedded in digital media with an optional key	Watermark is embedded in multimedia files
Cover Selection	N/A	Any cover can be chosen	Restriction on the cover selection
Objective	Robustness	Capacity	Robustness
Detection & Retrieval	Full retrieval of data without need of cover	Full retrieval of data without need of cover	Data is retrieved by cross correlation and cover may or not be necessary for the same

Cover-Visibility Relation	Due to encryption it is known that data is hidden but deciphering is Difficult	Information is not generally related to the cover and is never perceptible to human eye	Watermarks may or may not be visible to the human eye and become an attribute of the image.
Attacks	Cryptanalysis relates with deciphering the data encrypted	Steganalysis detects the presence of information	Image processing attacks aim at image distortion with attacks on watermark

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 [9]. 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. As many advances are made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods are designed to offer better security than what cryptography can 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. 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 1.2 below explains how watermarking is derived from steganography [10].

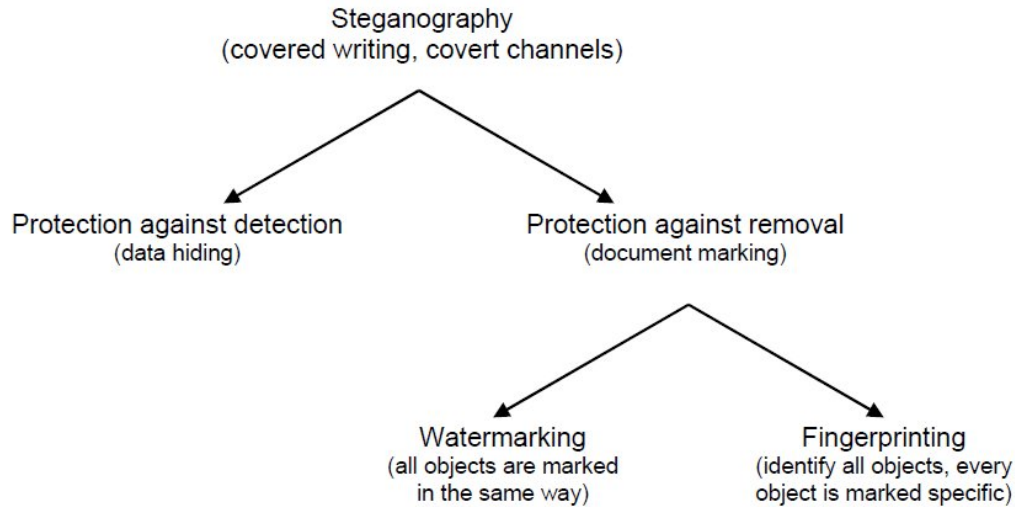


Fig 1.2: Types of Steganography [10]

1.2 PRINCIPLE OF WATERMARKING

A watermarking system is usually divided into three distinct steps, 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, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks [11]. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then 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 takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. Figure 1.3 below shows the basic block diagram of watermarking process. [10]

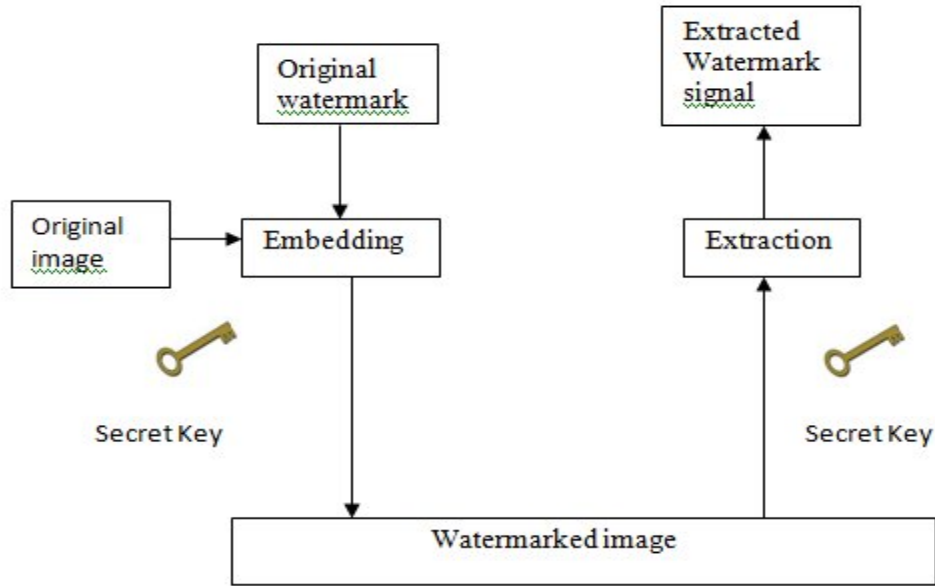


Fig 1.3: Watermarking block diagram [10]

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.

1.3 CHARACTERISTICS OF DIGITAL WATERMARKS

There are various important characteristics that watermarks exhibit [10]:

1.3.1 Transparency: The embedded watermark should not degrade the original image. If visible distortions are introduced in the image, it creates suspicion and makes life ease for the attacker .It also degrades the commercial value of the image.

1.3.2 Robustness: 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. Music, images and videos may undergo various types of distortions like lossy compression, colors might be altered, change in frequencies. Thus, a watermark must be robust to transformations that include distortions and attacks like rotation, compression, noise, cropping, etc. So, the embedded watermark should be such that

it is invariant to various such attacks. Robustness basically includes two issues; whether the watermark is still present after the distortion and second whether the watermark is detectable or not.

1.3.3 Capacity: This quantity describes the maximum amount of data that can be embedded into the image to ensure proper retrieval of the water during extraction.

1.3.4 Fidelity: The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. Earlier imperceptibility word had been used instead of fidelity.

1.3.5 Tamper resistance: Watermark is required to be resistant to signal that is solely intended to remove them, in addition to being robust against the signal distortions.

1.3.6 Security: The ability to resist hostile attacks that includes unauthorized removal, unauthorized embedding, and unauthorized detection.

1.4 APPLICATIONS OF DIGITAL WATERMARKS

Watermarking compliments encryption. A digital watermark is a piece of information that is hidden directly in media content, in such a way that it is imperceptible to a human observer, but easily detected by a computer. The principal advantage of this is that the content is inseparable from the watermark. This makes watermarks suitable for several applications, including: [4]

1.4.1 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. Watermarking an image will prevent redistribution of copyrighted images.

1.4.2 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.

1.4.3 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. An automated systems monitor's television, radio broadcasts, computer networks and any other distribution channels to keep

track of when and where the content appears. This helps in protection of illegal distribution of our content.

1.4.4 Content Labeling: Watermarks can be used to give more information about the cover object. This process is named content labeling. [10]

1.4.5 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. [10]

1.4.6 Digital Fingerprinting: This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner. This also assists in tracing the source of illegal copies. [10]

1.4.7 Signatures: The watermark identifies the authenticated owner of the content or image. So to secure the content, ownership, signatures are embed on the content. To use that content by anyone else, they have to take legal permission to copy or use their content [10].

1.4.8 Secret communication: The embedded signal is used to transmit secret information from one person to other without any third person knowing about this data transfer. There are many public-domain and shareware programs that use watermarking for the secret communications [10].

1.4.9 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 [12].

1.5. CLASSIFICATION OF WATERMARKING

The watermark can be classified on the basis of audio, video, image, and text.

1.5.1 Audio Watermark

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 [13].

1.5.2 Video Watermark

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 [14].

1.5.3 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.

1.5.4 Text watermarking:

Digital watermarking provides authentication and copyright protection for multimedia contents over the internet. In addition to image, audio, and video, now a day's text is 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 [15].

1.6 WATERMARK ATTACKS

Digital watermarking is not completely secure. In most watermarking applications, the marked data is likely to be processed in some way before it reaches the watermark receiver. An embedded watermark may unintentionally or inadvertently be impaired by such processing. Other types of processing may be applied with the explicit goal of hindering watermark reception. In watermarking terminology, an "attack" is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. The figure 1.4 shows the basic diagram of attacks on signals [11].

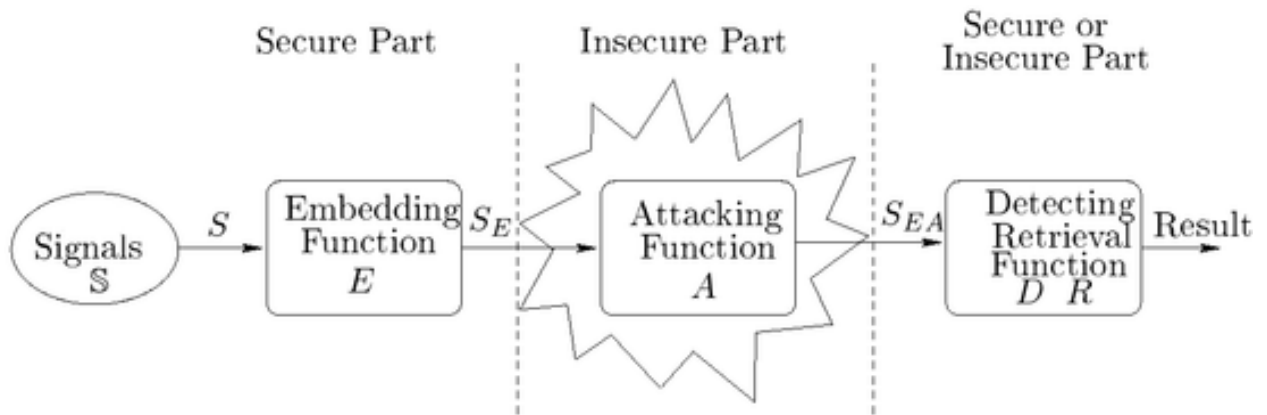


Figure 1.4: Watermark Attacks [11]

Broadly attacks can be classified as –

- Intentional Attacks
- Non-Intentional Attacks

The processed watermarked data is then called “attacked data”. 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. For multimedia, the usefulness of the attacked data can be gauged by considering its perceptual quality or distortion. Hence, robustness can be evaluated by simultaneously considering watermark impairment and the distortion of the attacked data. 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. Attacks can be classified as:

- Removal Attacks
- Geometric Attacks
- Cryptographic Attacks
- Protocol Attacks

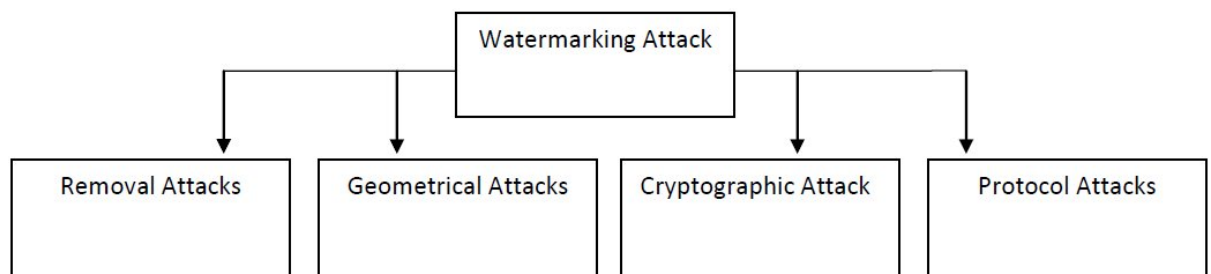


Fig1.5: Types of attacks [12]

1.6.1 REMOVAL ATTACKS

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. Collusion attacks are applicable when many copies of a given data set, each signed with a key or different watermark, can be obtained by an attacker or a group of attackers. In such a case, a successful attack can be achieved by averaging all copies or taking only small parts from each different copy [12]

1.6.2 GEOMETRIC ATTACKS

In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark with the embedded information. However, most recent watermarking methods survive these attacks due to the use of special synchronization techniques. The pixels are locally shifted, scaled, and rotated without significant visual distortion [12]

1.6.3 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. One such technique is brute-force search for the embedded secret information [17]

1.6.4 PROTOCOL ATTACKS

Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks. The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create ambiguity with respect to the true ownership of the data. It has been shown that for copyright protection applications, watermarks need to be noninvertible i.e. it should not be possible to extract a watermark from a non- watermarked data [12]. Another protocol attack is the copy attack. In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target

data. The estimated watermark is adapted to the local features of the target data to satisfy its imperceptibility. The copy attack is applicable when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor knowledge of the watermarking key. Again, signal-dependent watermarks might be resistant to the copy attack [17]

1.6.5 ESTIMATION- BASED ATTACKS

These types of attacks include the knowledge of watermarking technology and exploit statistics of the original data and watermark signal. Within the scope of these attacks, we present the concept of estimation-based attacks. This concept is based on the assumption that the original data or the watermark can be estimated - at least partially - from the watermarked data using some prior knowledge of the signals' statistics. The estimation does not require any knowledge of the key used for watermark embedding [17]

1.7 TECHNIQUES OR SCHEMES OF WATERMARKING

The figure 1.6 shows there are two types of techniques-Spatial Domain techniques and Frequency Domain techniques, and further subdivided into different techniques.



Fig 1.6: Watermarking techniques [11]

1.7.1 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 [18].

1.7.1.1 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 [18].

1.7.1.2 Predictive Coding Schemes

Predictive coding scheme was proposed by Matsui and Tanaka in [19] for gray scale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust when compared to LSB coding.

1.7.1.3 Correlation-Based Techniques

In this method a pseudo random noise (PN) with a pattern $W(x, y)$ is added to an image, according to the equation

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

$I_w(x,y)$ = Watermarked image.

$I(x,y)$ =Original image

k =gain factor

Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image. At the decoder the correlation between the random noise and the image is found out and if the value exceeds a certain threshold value the watermark is detected else it is not.

1.7.1.4 Patchwork Techniques

In patchwork watermarking, the image is divided into two subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k , the other subset will be decreased by the same amount. If $a[i]$ is the value of the sample at I in subset 'A' which is increased and $b[i]$ is the value of the sample in the subset 'B' whose value is decreased, then the difference between the two subsets would intuitively result in

$$\begin{aligned} \sum(a[i]-b[i]) &= 2N \quad \text{for watermarked images} \\ 1 \leq i \leq N &= 0 \quad \text{otherwise} \end{aligned}$$

1.7.2 FREQUENCY DOMAIN TECHNIQUES

The frequency domains techniques refer to the analysis of mathematical functions with respect to frequency rather than time. The transform domain methods embed the data by modulating the transform domain coefficients.

1.7.2.1 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 [20].

1.7.2.1.1 DCT –I

In JPEG compression the input data are two-dimensional, presented in 8×8 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:

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

$$\text{Where } u=0,1,\dots,N-1$$

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

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

1.7.2.1.2 DCT –II

The formula used for two-dimensional DCT:

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

$$\text{Where } u=0,1,\dots,N-1; v=0,1,\dots,M-1$$

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

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

Applying these formulas directly requires much computational resources therefore an implementation in hardware can be very efficient. The figure below, shows example of 8×8 block before DCT.

162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161

162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
163	161	164	164	158	155	161	159
160	160	160	163	158	160	162	159
156	159	155	157	158	159	156	157

After Discrete Cosine Transform the block has following values:

162.4	160.3	157.5	155.3	158.0	157.4	168.6	170.1
165.2	165.2	164.9	162.9	162.2	155.0	158.8	155.5
160.6	163.3	166.8	167.5	166.8	156.8	156.9	151.0
154.4	156.9	160.8	163.3	166.0	160.7	165.3	162.1
160.8	159.6	158.2	156.9	159.6	158.1	168.0	168.5
173.9	170.0	158.1	150.1	154.4	154.1	157.6	161.3
165.4	164.1	164.9	157.7	158.0	159.0	155.7	152.7
149.8	153.3	154.5	160.9	163.6	163.4	157.6	156.5

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 trade-off has to be made. The following figure shows the basic procedure of embedding

1.7.2.1.3 Basic Steps

- a. The image is segmented into non-overlapping blocks of 8x8.
- b. Forward DCT is applied to each of the block.
- c. Selection criteria are then applied.
- d. This is followed by applying coefficient selection criteria.
- e. Embed watermark by modifying the selected coefficients.
- f. Inverse DCT is applied to obtain the final watermarked image.

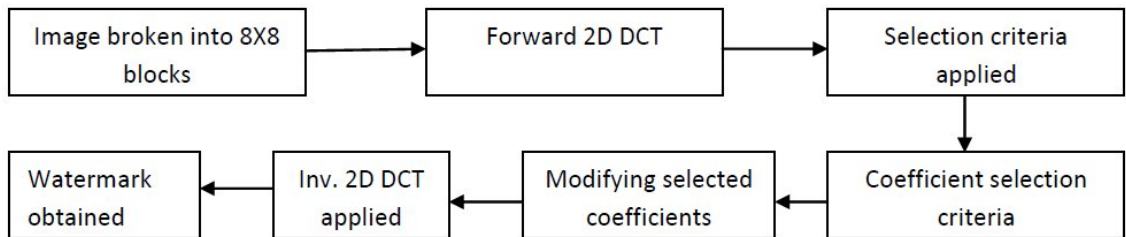


Fig 1.7: Block diagram of watermarking using DCT

1.7.3 DISCRETE WAVELET TRANSFORM

Wavelet transform is a multi-scale signal analysis method, which overcomes the weakness of fixed resolution in Fourier transform (DFT). DWT is a hierarchical sub-band system. Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error. Since the bandwidth of the resulting coefficient sets is smaller than that of the original image, the coefficient sets can be down sampled without loss of information. Reconstruction of the original signal is accomplished by up sampling, filtering and summing the individual sub bands. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution coefficient sets, a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The sub-band LL represents the coarse-scale DWT coefficients while the coefficient sets LH, HL and HH represent the fine-scale of DWT coefficients. To obtain the next scale of wavelet coefficients, the sub-bands are further processed until some final scale N is reached. [20]

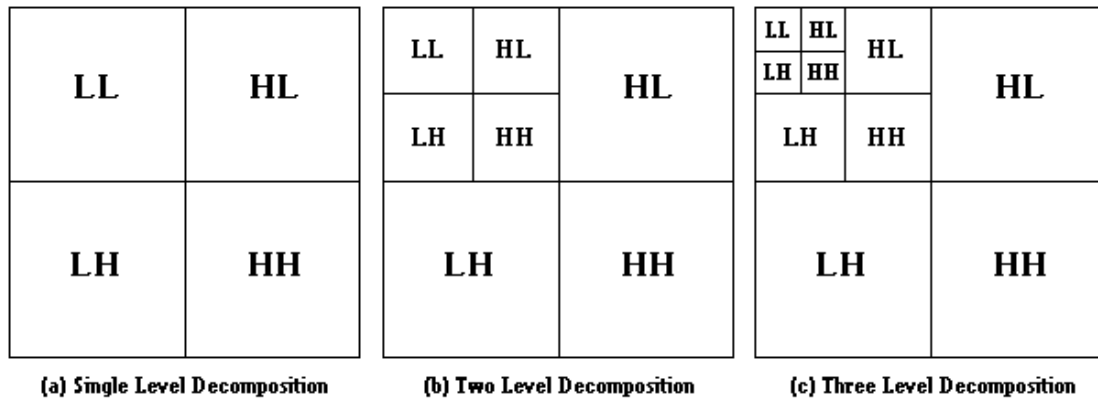


Figure 1.8: DWT Decomposition [20]

Due to its excellent spatial-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified. In general most of the image energy is concentrated at the lower frequency coefficient sets LL and therefore embedding watermarks in these coefficient sets may degrade the image significantly. Embedding in the low frequency coefficient sets, however, could increase robustness significantly. On the other hand, the high frequency coefficient sets HH include the edges and textures of the image and the human eye is not generally sensitive to changes in such coefficient sets. This allows the watermark to be embedded without being perceived by the human eye. The agreement adopted by many DWT-based watermarking methods, is to embed the watermark in the middle frequency coefficient sets HL and LH is better in perspective of imperceptibility and robustness. [20]

1.8. 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.

1.8.1 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

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

L is the peak signal value of the cover image

1.8.2 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

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

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

1.8.3 NCC (NORMALISED CROSS CORRELATION)

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

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

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

1.8.4 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].

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

CHAPTER 2: LITERATURE REVIEW

2.0 LITERATURE SURVEY

A wide number of researchers and scholars have worked in the literature on digital image watermarking that employs techniques like Singular Value Decomposition, Discrete Cosine Transform, Discrete Wavelet Transform and a combination of spatial domain and transform domain techniques. A survey of some of the motivating researches is briefly described below.

Miller et al. [10] has discussed applications of digital watermarking like signature, broadcasting, finger printing, authentication, fraud detection etc. and its various properties like fidelity, robustness, fragility, tamper-resistance, key restrictions, etc. It has also explained the examples of watermarking method and has proposed different methods [10]. The watermarking techniques are divided into two broad classes: spatial and transform domain techniques. In spatial domain techniques the data is embedded directly by changing the pixel values or code values. Although computationally simple these are less robust against attacks as compared to transform domain techniques. In transform domain, the image is transformed using some or the other method and then the watermarks are irregularly distributed over the whole image, making it robust against attacks. Some of the transform domain techniques are: SVD, DCT and DWT. Manjit et al. [22] proposed a technique based on Singular Value Decomposition (SVD) to embed a watermark. This algorithm requires less memory size and gives more accurate result. In the watermark embedding process, the SVD is applied on original image and then largest coefficient is extracted and quantized. The extracting procedure is same as embedding one except that the original image is replaced by watermark image. Kaushik et al. [23] proposed an algorithm based on DFT. In the embedding process, the original image is subdivided into blocks and then pseudo random sequence is produced. In this n is considered as a discrete time domain variable and k as a discrete frequency domain variable and then watermark is embedded in amplitude function $F(k)$, i.e. Fourier transform. To extract the watermark, image segmentation has been used which also

improved the security of watermark. Radhika et al. [24] has compared the techniques DWT and DCT to compare the robustness of both algorithms and the different places where they can be used. Dinghui et al. [25] worked to enhance the security and strength of the image by the amalgamation of the Arnold and Discrete wavelet transforms for Digital image watermarking.

Mohanty et al. [19] proposed an efficient techniques for visible and invisible watermarking using DCT. Visible watermarking is useful for enhanced copyright protection. The owner might want an ownership mark, that is visually apparent, and hence confirm ownership. The watermark embedding process computes DCT of the entire image it is one block, then the perceptually significant regions of the image are found out. The watermark is then computed and inserted into the DCT of the original image. The extraction process involves computing the difference in the DCT of the watermarked image and the original image. In invisible watermarking, although serves the purpose of ownership, the watermark is not visible but if detected in a cover image authenticates the owner. Singh et al. [21] has been performed watermark embedding and extraction using DWT. Haar transform is used to extract the watermark. This algorithm provides good resolution of images and has linear complexity. The cover image is decomposed in to n level (where $n=4$) wavelet transform. The watermarks are then embedded in the blocks of medium frequency band i.e. HL or LH sub band. Finally, the inverse Haar wavelet transform is performed to form a watermarked image. For the extraction of the watermark, the reverse steps are performed. Considering different techniques in spatial domain, Singh, et al. [26] proposed an algorithm using the least substitution bit method to embed the watermark. This method although simple but is vulnerable to cropping, noise and scaling . The watermark image is inserted into the least significant bit of cover image using simple substitution method. Also for the extraction algorithm the original image is required to match with the watermarked image and extract the watermark. Increased efforts are being made to use techniques that combine spatial and frequency domain techniques so that the advantages of the spatial and frequency domain techniques can be exploited to the maximum possible [19]. Mohan et al. [27] proposed an algorithm that is a combination of embedding in transform domains and extraction using Hadamard transform. The main concept utilized by the authors is that

embedding is based on the areas of image with the highest variations. Dabas et al. [28] proposed a method of watermarking techniques and performed simulations on a set of 4 images using Matlab and compared the results obtained as per LSB, DCT, AND DWT watermarking techniques and concluded with giving the advantages and disadvantages of these three techniques. Lu et al. [29] has utilized the texture active regions for embedding the watermark based on both spatial and frequency domain techniques. This technique has efficiently fulfilled the need of blind watermark extraction. Thapa et al. [22] has proposed an algorithm for digital image watermarking technique based on singular value decomposition; both of the L and U components are explored for watermarking algorithm. This technique refers to the watermark embedding procedure and watermark extracting procedure. Averkiou et al. [30] has present some of the most important applications of digital watermarking, explain some key properties that are desirable in a watermarking system, and give an overview of the most common models of watermarking. Chouarfia et al. [31] has studied some watermarking methods and the comparison result of their combination, the first one is based on the CDMA (Code Division Multiple Access) in frequency domain DWT(Discrete Wavelet Transform) noted CDMA-DWT ,CDMA in DCT(Discrete Cosine Transform) noted CDMA-DCT and CDMA in spatial domain noted CDMASD and its aim is to verify the image authenticity whereas the second one is the reversible watermarking (the least significant bits LSB and cryptography tools) noted RW and the reversible contrast mapping RCM its objective is to check the integrity of the image and to keep the confidentiality of the patient data. Shih et al. [32] proposed a combinational technique to split the watermark-image into two parts, respectively, for spatial and frequency domain. When different sized watermarks are embedded into a grayscale image, more watermark data can be inserted into the host image, so that the capacity is increased. The splitting of the watermark into two parts makes the degree of protection double. The splitting strategy can be designed even more complicated to be unable to compose. Mostly the important part of the image is not enormous. So, we can extract the important part of the image and divide it into two parts and embed in different domains, depending on the application. The center part of the image contains the most important data. The central window is therefore extracted for this purpose. Ahire et al. [33] have worked on a more robust

algorithm which combines DCT- DWT. The host image is decomposed upto 3 levels using DWT. Then, Discrete Cosine Transform of selected sub bands are computed. The watermark data is further embedded in the middle frequency coefficients of these bands to further improve resistance. Umaamaheshvari et al. [34] have presented a novel work on the application of hybrid transform. The DCT of the image is computed, followed by the DWT of the image. The watermark is then inserted into the selected bands of this hybrid transformed image using Least Substitution Bit. This scheme has been proved to be effective for image authenticity and integrity.

Abdul et al. [36] has proposed a more robust technique to embed a watermark based on wavelet transform with error correction codes. He also compares the efficiency of error correcting codes against different attacks like salt and pepper noise attack, Gaussian noise, cropping, rotation, jpeg compression, etc. He had chosen 8*8 signature size to embed in an image. The proposed algorithm used middle frequencies for the insertion of the mark as both invisibility and robustness against low pass filter attacks is required. He confirmed that by using error correction codes like hamming code, BCH code, Rees-Solomon code, or concatenation of two codes improved the robustness and the quality of watermarked image.

Mein et al. [35] has proposed a technique of DWT and error correction codes for embedding a watermark. According to her although spatial domain watermark is simple and easy to execute but at various attacks and noise it is less robust than frequency domain watermark embedding. Because of its multi resolution and spatial localization characteristics DWT is better than other techniques. She had implemented the DWT using Haar filter on both the images and then applied Block based error correcting code with convolution codes on input image and then embeds the watermark into input image.

Colin et al. [39] has discussed the role of DICOM and the need of watermarking in the medical. Teleradiology allows medical images to be transmitted over electronic networks for clinical interpretation and for improved healthcare access, delivery, and standards. Although such remote transmission of the images is raising various new and complex legal and ethical issues, including image retention and fraud, privacy, malpractice liability, etc., considerations of the security measures used in teleradiology remain unchanged. Addressing this problem naturally warrants investigations on the security

measures for their relative functional limitations and for the scope of considering them further. Watermark medical is the first and only automated end-to-end service for the diagnosis and treatment. Recently, telemedicine applications in teleconsulting, teliagnosis, and remote medical education play a vital role in the evolution of the healthcare domain. The transmission, storage and sharing of electronic medical data via the networks have many purposes such as diagnosis, finding new drugs and scientific research. Hospitals and medical centers have huge databases including medical images, text and patient records. The exchange of these databases through the networks requires content management to index medical record information and a high degree of security and authenticity to preserve the privacy of the patients' information. To achieve these objectives, different techniques of digital watermarking have been employed. The Digital Imaging and Communications in Medicine (DICOM) standard is the standard to exchange medical data. The DICOM medical image files are attached with header containing patient information which may be lost attacked or disordered with other header file. However, the watermarking of medical images using patient information overcomes these problems. However, there is a challenge that interleaving data in a medical image must not affect the image quality as this may result in wrong diagnosis.

Mostafa et al. [1] has presented a technique to how to increase the security, robustness, authenticity and management of medical images and information through storage and distribution. This paper presents a technique for embedding the EPR information in the medical image to save storage space and transmission overheads and to guarantee security of the shared data. In this paper a new method for protecting the patient information in which the information is embedded as a watermark in the discrete wavelet packet transform (DWPT) of the medical image using the hospital logo as a reference image. The patient information is coded by an error correcting code (ECC), BCH code, to enhance the robustness of the proposed method. The scheme is blind so that the EPR can be extracted from the medical image without the need of the original image. Therefore, this proposed technique is useful in telemedicine applications. Performance of the proposed method was tested using the modalities of medical images.

Table 2.1: Details of Literature review

S.no	Author name/Year	Technique	Image Details	Result
1	Amit Kumar Singh/ 2012	Discrete Wavlet Transform	--	PSNR=36.12 at k=2 PSNR=31.34 at k=2.5
2	Amit Kumar Singh/ 2012	Least Substitution Bit	8 bit, Lena image	At bit position 1: PSNR=51.14,MSE=0.5 At bit position 2: PSNR=45.12,MSE=2
3	Yinghua LU/ 2005	Joint Spatial:LSB transform:DWT	256*256 Lena image	NC-1 PSNR=42.517
4	Saraju P. Mohanty	Discrete Cosine Transform	Lena image	Visible watermark image implemented
5	Manjit Thapa/ 2011	Singular Value Decomposition	Lena image 256*256	PSNR=45.59
6	Radhika V.Totla/ 2013	DWT,DCT	Splash image	PSNR=91.5 in DWT PSNR=49.02 in DCT
7	Awanish Kr Kaushik/2012	DFT and image segmentation	512*512*8 bit image	PSNR=38.5914 NC=0.9976
8	Matt L.Miller/ 1999	--	--	--
9	Pooja Dabas/ 2013	LSB,DCT,DWT	256*256 pixels	--
10	B.Chandra Mohan	Hybrid Algorithm	Lena image 256*256	PSNR=51.622 NC=1
11	Zhang Dinghui/ 2007	DWT	512*512*8 image 64*64*8 watermark	--
12	Manjit Thapa	SVD	256*256	-PSNR=40.16
13	Mansi Hasija	Spatial Domain	--	--
14	Melinos Averkiou	Blind embedding	112*92	--

15	S.Bekkouche	DWT,DCT,SD	128*128	PSNR=54.21 in DWT PSNR=58.08 in DCT PSNR=40.48 in SD
16	Hongtao Ge	DWT,ECC	Lena image 512*512 Input text "Hello World"	PSNR=28.4
17	A.Umaamaheshvari/ 2013	DWT,ECC	CT image, MRI images	PSNR=66.03 in CT image PSNR=37.85 in MRI image
18	Chirag Sharma	DWT, Attacks	--	PSNR=21.49 ,BER=0.04 in Salt & pepper attack PSNR=20.81,BER=0.04 in Gaussian attack PSNR=15.76,BER=0.06 in cropping
19	Ching-Tang Hsieh/2001	DWT,BCH,JPEG compression attack	Lena image	PSNR=40.3

CHAPTER 3: Proposed Method for Image Watermarking using Error correcting code

3.0 ERROR CORRECTION CODES

Error correction codes are a coding system that incorporates extra parity bits in order to detect errors. These techniques enable reliable delivery of digital data over unreliable communication channels. Many communication channels are subject to channel noise, and thus errors may be introduced during transmission from the source to a receiver. Error detection techniques allow detecting such errors, while error correction enables reconstruction of original data. The general idea for achieving error detection and correction is to add some redundancy (i.e. some extra bits) to a message, which receivers can use to check consistency of the delivered message, and to recover data determined to be corrupted. The transmitter sends the original data, and attaches a fixed number of check bits, which are derived from the data bits by some algorithm. Then the receiver can simply apply the same algorithm to the received data bits and compare its output with the received check bits. If the values do not match, an error has occurred at some point during the transmission [36]. The figure 3.1 depicts the categories of block coding techniques.

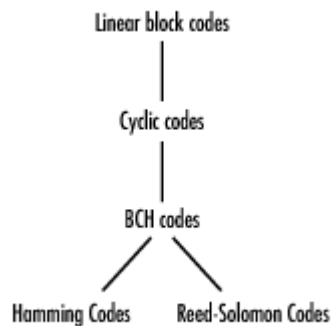


Fig 3.1: Categories of block coding techniques [36]

3.0.1 HAMMING CODE

Hamming codes are a family of linear error-correcting codes. Hamming codes can detect up to 2 bit errors or correct one bit errors. Data to be transmitted consists of a certain

number of information bits u and number of check bits p such that if a block is received that has at most one bit in error, then p identifies the bit that is in error. Specifically, in hamming's code p is interpreted as an integer which is 0 if no error occurred, and otherwise is the 1-originated index of the bit that is in error. Let k be the number of information bits and m be the number of check bits used. Because the m check bits must check themselves as well as information bits, the value of p , interpreted as an integer must range from 0 to $m+k$, which is $m+k+1$ distinct values. Because m bits can distinguish 2^m cases, we must have [40]

$$2^m > m+k+1$$

This is known as hamming rule.

No. of information bits, k	M
1	2
2 - 4	3
5 - 11	4
12-26	5
27-57	6
58-120	7
121-247	8
248-502	9

Table 3.1: Extra bits for error Correction/Detection

General Algorithm:

1. Number of bits starting from 1: bit 1, 2, 3, 4, 5, etc.
2. Write the bit numbers in binary: 1, 10, 11, 101, etc.
3. All bits position that are power of 2 are parity bits: 1, 2, 4, 8, etc.
4. All other bits position, with two or more 1 bit in the binary from form of their position, is data bits.
5. Each data bit is included in a unique set of 2 or more parity bits, as determined by the binary form of its bit position.
 - Parity bit 1 cover all bits position which have the least significant bit set: bit 1, 3, 5, 7, 9, etc.
 - Parity bit 2 cover all bits position which have the second least significant bit set: bit 2, 3, 6, 7, 10, 11, etc.

- Parity bit 4 cover all bits position which have the third least significant bit set: bits 4-7, 12-15, 20-23, etc.
- Parity bit 8 cover all bits position which have the fourth significant bit set: bits 8-15, 24-31, 40-47, etc.
- In general each parity bit covers all the bits where the bitwise AND of the parity position and the bit position is non zero.

Bit position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Encoded data bits	p1	p2	d1	p4	d2	d3	d4	p8	d5	d6	d7	d8	d9	d10	d11	p16	d12	d13	d14	d15	
Parity bit coverage	p1	X		X		X		X		X		X		X		X		X		X	
	p2		X	X			X	X			X	X			X	X			X	X	...
	p4				X	X	X	X				X	X	X	X						X
	p8								X	X	X	X	X	X	X						
	p16															X	X	X	X	X	

The key thing about Hamming Codes that can be seen from visual inspection is that any given bit is included in a unique set of parity bits. To check for errors, check all of the parity bits. The pattern of errors, called the error syndrome, identifies the bit in error. If all parity bits are correct, there is no error. Otherwise, the sum of the positions of the erroneous parity bits identifies the erroneous bit. [41]

3.0.2 BCH (Bose Chaudhuri Hocquenghem) Code

BCH form a cyclic error correcting codes that are constructed using finite fields. One of the key features of BCH codes is that during code design, there is a precise control over

the number of symbol errors correctable by the code. In particular, it is possible to design binary BCH codes that can correct multiple bit errors. Another advantage of BCH codes is the ease with which they can be decoded, namely, via an algebraic method known as syndrome decoding. This simplifies the design of the decoder for these codes, using small low-power electronic hardware. They are also very flexible, allowing control over block length and acceptable error thresholds. BCH codes are used in applications such as satellite communications, compact disc players, DVDs, disk drives, solid-state drives and two-dimensional bar codes.

For positive pair of integer's m and t , a (n, k) BCH code has parameters:

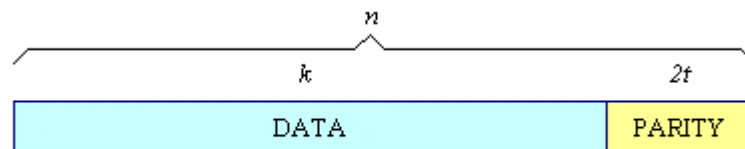
- Block length: $n = 2^m - 1$
- Number of check bits: $n - k \leq mt$
- Minimum distance: $d_{\min} \geq 2t + 1$

3.0.3 Reed- Solomon Code

Reed-Solomon codes are non binary cyclic codes with symbols made up of m -bit sequences, where m is any positive integer having a value greater than 2. R-S (n, k) codes on m -bit symbols exist for all n and k for which

$$0 < k < n < 2^m + 1$$

where k is the number of data symbols being encoded, and n is the total number of code symbols in the encoded block [41].



For the most conventional R-S (n, k) code,

$$(n, k) = (2^m - 1, 2^m - 1 - 2t)$$

where t is the symbol-error correcting capability of the code, and $n - k = 2t$ is the number of parity symbols. An extended R-S code can be made up with $n = 2^m$ or $n = 2^m + 1$, but not any further [43].

3.1 Proposed Method

In this technique, DWT is used to decompose the cover image into sub bands, LL, LH, HL, HH and further sub divided into bands according to the level of DWT. In the watermark embedding process, watermark text is encoded by Hamming code (7, 4). Then the encoded watermark is embedded into higher coefficients of second level. Due to this, the robustness of image gets improved and we can check whether the extracted text is same as embedded text or not. Hamming (7, 4) contains 4 data bits and 3 parity bits. First we convert the text into binary bits and after this hamming (7, 4) is applied on it. Hamming code can correct up to one bit error. To recover the text from watermarked image, text is decoded and again converted into char. PSNR and BER is used to calculate the quality of the watermarked image and robustness of the extracted watermark respectively. Figure 3.2 and Figure 3.3 show the embedding and extraction process of the proposed method respectively.

3.1.1 Embedding process

Input: Original image, text

Output: Watermarked image

Steps:

- Read the input image of size 256*256
- Apply DWT on the cover image and decomposed up to second level.
- Read the text to be embedded and calculate its length.
- Convert the text into binary form.
- Apply hamming code on the text watermark
- Embed the encoded text into cover image using the equation,

$$f'(m,n) = f(m,n) + \alpha f(m,n)w(k)$$

where, $f(m,n)$ =DWT coefficients of cover image

α = strength of factor controlling the level of watermark $w(1).....w(L)$

- Apply IDWT to generate final watermarked image.
- Display watermarked image.
- Calculate MSE and then PSNR.

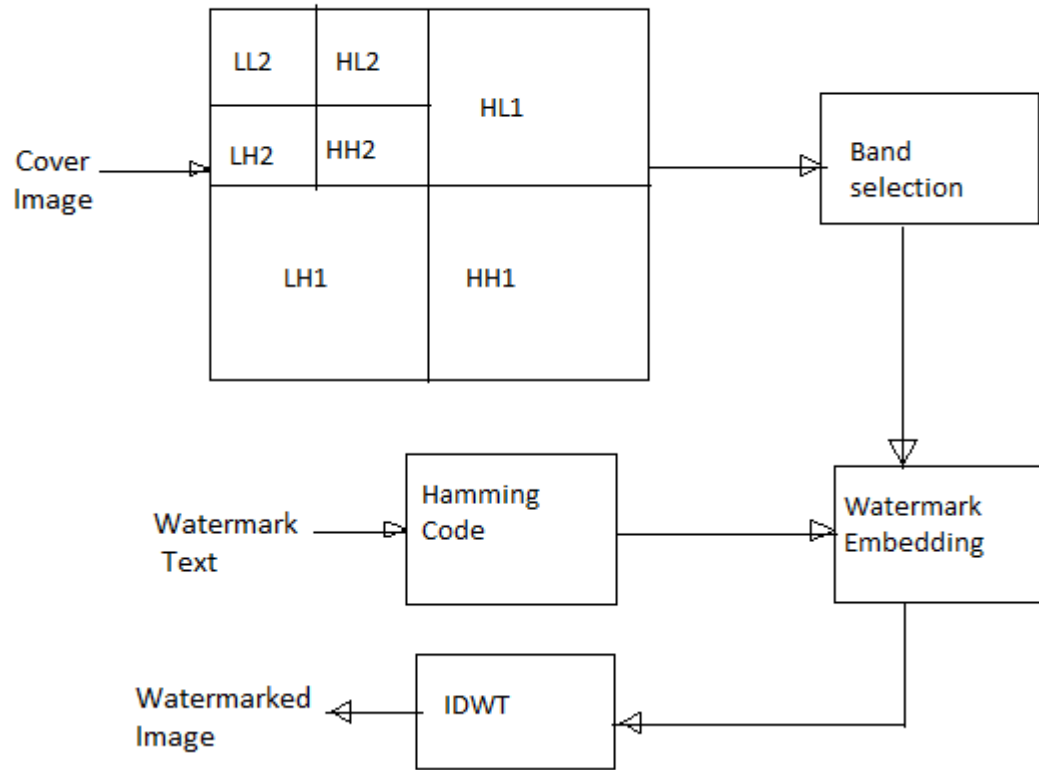


Fig 3.2: Embedding Process [31]

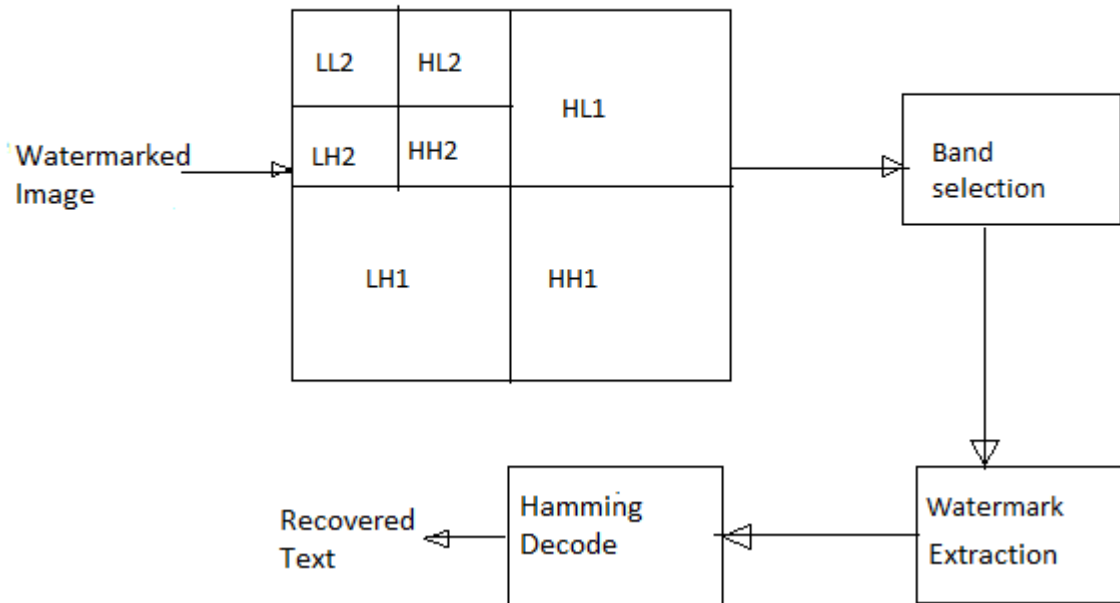


Fig 3.3: Extraction Process [31]

3.1.2 Extracting Process

Input: Watermarked image

Output: Recovered text

Steps:

- Read the watermarked image
- Apply IDWT on the image
- Extract the text from watermarked image, using

$$w_r(k) = (f_r'(m,n) - f(m,n)) / (\alpha f(m,n))$$
 where, $f_r'(m,n)$ = DWT coefficients of received image
 α = strength factor

Also it is better to take the extracted watermark $w_e(k) = \text{sgn}(w_r(k))$

- Decode the text and again covert the extracted bits into char
- Display the text.
- Calculate BER.

CHAPTER 4: EXPERIMENTS AND RESULTS

4.0 RESULT

- The table 4.1 shows the comparison between performance of watermark with hamming code and without hamming code. It shows that after applying hamming code the BER gets 0, thus increasing the quality of recovered text. There is less chances of error in recovering the watermark with hamming code. The PSNR value is little lower with hamming code compared to without hamming code because to apply hamming code more calculation are done and cover image is changed more compared with without hamming code. Thus the quality gets affected due to this.

Table 4.1: Comparison between performance of watermark with hamming and without hamming code at different gains against 140 bits.

Gain Factor	With Hamming		Without Hamming	
	PSNR	BER	PSNR	BER
0.01	78.65	45.71	79.90	47.12
0.05	64.67	37.85	65.92	47.12
0.09	59.57	25	60.81	47.12
0.1	58.65	22.85	59.90	48.21
0.5	44.67	0	45.92	48.21
0.9	39.57	0	40.81	48.21
1.0	38.65	0	39.90	48.21
1.5	35.13	0	36.38	48.21
2	32.63	0	33.88	48.21
4	26.61	0	27.86	48.21
9	19.57	0	20.81	48.21

- The table 4.2 shows the comparison between PSNR and BER values in different levels of DWT. The watermark embedded at DWT level 1 can be easily distorted and changed, so it's difficult to recover exact embedded text, thus BER value 0 is difficult to get. On the other hand PSNR value is good here because the cover image is not changed much here. At DWT level 4 the size where to embed watermark or text is very small so here also it's difficult to keep the quality of image and to recover the text properly.

Number of bits=140

Table 4.2: Comparison against different levels of DWT

Gain factor	Level 1 DWT		Level 2 DWT		Level 3 DWT		Level 4 DWT	
	PSNR	BER	PSNR	BER	PSNR	BER	PSNR	BER
0.09	62.24	45.72	59.57	25	56.50	32.14	55.80	36.42
0.1	61.34	46.42	58.65	22.85	55.59	30.71	54.89	36.42
0.5	42.25	12.14	44.67	0	41.61	0	40.91	27.85
1	41.34	7.85	38.65	0	35.59	0	34.89	25.71
2	35.32	1.4	32.63	0	29.57	0	28.87	21.42
4	29.30	0	26.61	0	23.55	0	22.84	20

- The table 4.3 shows the maximum number of bits that can be embedded in cover image after applying different levels of DWT. Its shows that we can embed high number of bits at DWT level 1 but to embed at DWT level 4, the number of bits must be very small.

Table 4.3: Comparison of BER values on different DWT levels by changing the no.of bits

Bits	Gain factor	Level 1 DWT	Level 2 DWT	Level 3 DWT	Level 4 DWT
		BER	BER	BER	BER
392	16	0	Very high	Very high	Very high
196	4	0	0	0	Very high

- The table 4.4 shows the value of BER against different attacks and thus the robustness of the watermark. The values taken for gain factor and the number of bits are written below.

Gain factor, K=1

Bits=140

Table 4.4: BER against different attacks

Attacks	BER
Gaussian Noise:	
M=0, V=0.1	32.14
M=0, V=0.01	12.85
M=0, V=0.001	0
Speckle Noise	
V=0.5	17.85
V=0.1	7.85
V=0.02	2.14
V=0.01	0
JPEG Compression	
Quality=5	48.57
Quality=35	3.57
Quality=50	0
Quality=75	0
Rotation	
Angle=90(degree)	58.57
Angle=180	60.71
Angle=360	0
Cropping[xmin,ymin,width,height]	
[2,2,1200,1900]	57.85
[3,3,1200,800]	60.01
[1,1,400,500]	0
[0,0,300,300]	0
Salt and Pepper Noise	
Density=0.5	42.14
Density=0.1	22.14
Density=0.01	0
Density=0.001	0

- The following figure shows the difference between the watermarked images on applying different level DWT on cover image with hamming code. It also shows the quality of watermarked image by PSNR values and the quality of recovered text by calculating BER value. It clearly shows that applying DWT of level 4 is not good because it doesn't recover actual embedded text. DWT level 1 is best

but here we can embed general information because it is easy to distort information at DWT level 1. The main information can be embed at DWT level 2 and the signature at DWT level 3. By increasing the level, security increased but the recovered text quality decreases.







Cover Image:

Input Text=neetikajuitwaknaghat

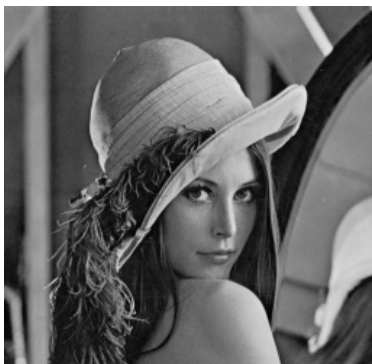
Gain factor, $K=2$

Output:

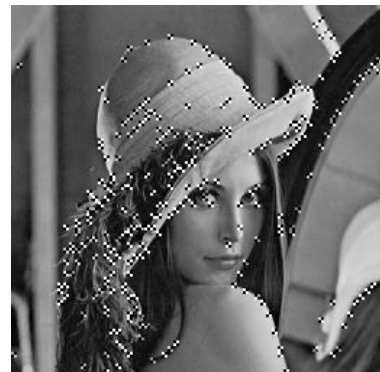
DWT Level	PSNR(db)	BER	Watermarked Image
4	28.87	20	
3	29.57	0	

2	32.63	0	
1	35.32	0	

- The following figures show the cover image, input text and corresponding to different gain factor values, different watermarked image. It shows the difference between qualities of watermarked image.



+ neetikajuitwaknaghat =



Cover image; K=17

input text

watermarked image, PSNR=18.65



+ neetikajuitwaknaghat =



Cover image; K=17

input text

watermarked image, PSNR=13.55



+ neetikajuitwaknaghat =



Cover image; K=7

input text

watermarked image, PSNR=21.7



+ neetikajuitwaknaghat =



Cover image; K=2

input text

watermarked image, PSNR=32.63



Cover Image; K=0.1

Input Text

Watermarked image, PSNR=58.65

- The figure 4.1 graph explains the relation between gain factor and PSNR. It explains that on increasing the value of gain factor, PSNR decreases and thus decreasing the quality of watermarked image and its imperceptibility.

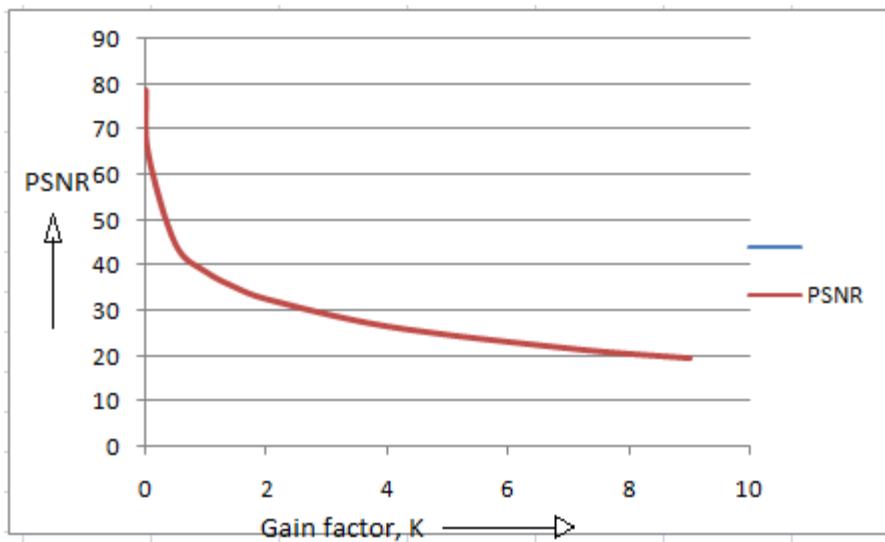


Fig 4.1: Graph of Gain factor vs PSNR

- The figure 4.2 graph shows the relation between gain factor and BER. Initial BER is high but on increasing the gain factor BER comes out to be zero, thus increasing the quality of recovered text.

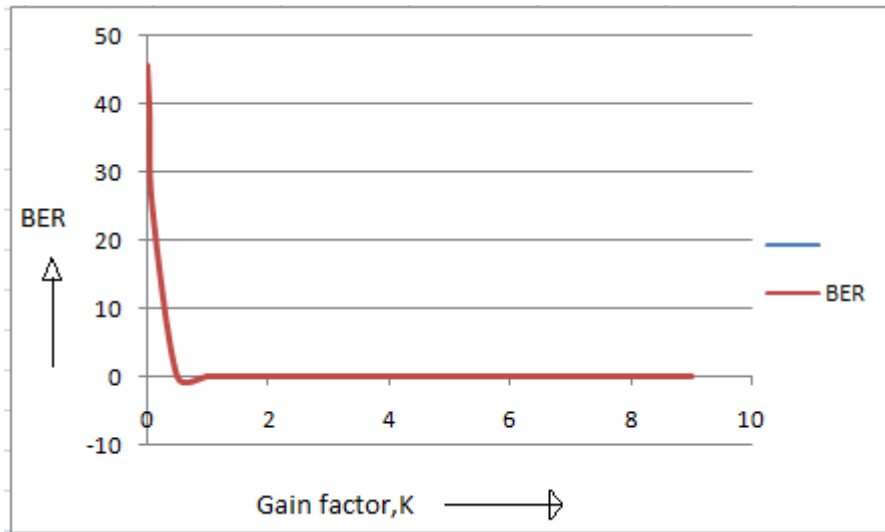


Fig 4.2: Graph of Gain factor vs BER

CONCLUSION AND FUTURE DIRECTION

In the proposed work, the embedding watermarks method based on the discrete wavelet transforms (DWT). Also, error correcting code (ECC) is applied to the ASCII representation of the text and the encoded text watermark is embedded. In order to make the data error correctable, additional bits in the form of ECC is required to be added in the original bits. However, if we want to further improve the error correction capabilities the length of error correction code may be suitably increase. We would like to further improve the performance in terms of image quality of watermarked image and robustness of the extracted watermark.

APPENDIX

IMPLEMENTATION

```
img= imread('as.bmp');
img=imresize(img,[256 256]);
cover_img=double(img);
[Mc Nc]=size(cover_img);% determine size of watermarked image
[ca1,ch1,cv1,cd1]=dwt2(img,'haar');
[ca2,ch2,cv2,cd2]=dwt2(ca1,'haar');

% Converting watermarking text to Binary bits
Wtxt = dec2bin('neetikajuitwaknaghat'); %text to be watermarked
Wtxtr= reshape(Wtxt',1,numel(Wtxt));
Wmsg=~isspace(regexprep(Wtxtr, '0', ' '));
IMS=size(Wmsg,2);

%%Hamming encoder algorithm and embedding
m = 3; n = 2^m-1; % Codeword length = 7
k = 4;          % Message length
vc=(IMS/7);    %Change the value here
Wb=double(reshape(Wmsg,4,(7/4)*vc).');
code = encode(Wb,n,k,'hamming/binary');
[R C]=size(code);
Vr=R;
for i=1:R
    for j=1:C
        if code(i,j)==0
            Wbt(i,j)=-1;
        else
            Wbt(i,j)=1;
        end
    end
end
```

```

        end
    end
end
Wbit=reshape(Wbt.',1,((7/4)*7*vc));
L=length(Wbit);
A=cd2;
[H]=img_embd(A,Wbit,L);
cd2=H;
Wmg=idwt2(ca2,ch2,cv2,cd2,'haar');
watermarked_image = idwt2(Wmg,ch1,cv1,cd1,'haar',[Mc,Nc]);

%% MSE and PSNR calculation
MSE1=mse(cover_img,watermarked_image,Mc,Nc);
MSE =10*(log10(MSE1))
PSNR= 10*(log10(255^2/MSE));
mse=mean(squeeze(sum(sum((double(cover_img)-
double(watermarked_image)).^2))/(Mc*Nc)));
PSNR=10*log10(255^2./mse);
msg=sprintf('\n\n-----\nWatermark by SVD PSNR=%fdB\n-----
-----\n\n', PSNR);
disp(msg);

%% Hamming Decoder Algorithm
Wr=(reshape(Wcr,7,Vr)).';
n=7;k=4;
code = decode(Wr,n,k,'hamming/binary');
Wt=reshape(code.',1,IMS);
display(Wt);

%% Watermarking bits converted back to char
for n=1:(IMS/7)

```

```

    Wbitr(n) = sum(Wt((7*(n-1)+1):7*n).*2.^[6:-1:0]);
end
Wmsgr=char(Wbitr)

%% Read the Image & its decomposition through DWT
function [H]=img_embd(A,Wbit,L)
%% Watermarking Algorithm implimentation
H=A;
for i=1:L
    kg=2;          %Watermark strength coefficient
    [value,location]=max(A(:));
    [R,C] = ind2sub(size(A ),find(A==value));%givies row & column of the value
    P=(ismember(A,[value]));
    G=P.*A;
    H=H+(kg*G*Wbit(i)) ;          %watermarked matrix
    V=~(ismember(A,[value]));
end
end

%% Attacks

% Salt & Pepper Noise
wm_image=imnoise(I,'salt & Pepper',0.0001);
imwrite(wm_image,'WMESVDHamming20.05SPN.bmp','bmp');
title('Salt and Pepper noise');
I=imread('leena.bmp');

%% Gaussian Noise
M =0.0005;
V=0.001;
imshow(I);title('Original Image');
M = imnoise(I,'gaussian',M,V);

```

```

imshow(M);title('Gaussian Noise');
K = medfilt2(M);
imshow(K);title('Median Filtering');
title('Filtered Image');

%%cropping attack
K=imcrop(I,[0,0,300,300]);
imshow(K);
title('Cropped Image');

%%jpeg compression
imwrite(I,'K.jpg','quality',35)
M=imread('K.jpg');
imshow(M);
title('JPEG compression');

%% After attacks calculating new coefficients

[ca1,ch1,cv1,cd1] = dwt2(I, 'haar');
[ca2,ch2,cv2,cd2] = dwt2(ca1, 'haar');
img_cvr=imread('as.bmp');
[LL1,HL1,LH1,DD1] = dwt2(img_cvr, 'haar');
[LL2,HL2,LH2,DD2] = dwt2(LL1, 'haar');
ke=4;      %watermark strength
q=(IMS/7); % Change the value of q for each letter
Wk=sign((cd2-DD2)./(ke*DD2));
Wb=zeros(1,(7*R)); % Change the value for each letter
L=length(Wb);
for i=1:L
    [value,location]=max(DD2(:));
    [R,C] = ind2sub(size(DD2),find(DD2==value));%gives row & column
    I=R(1);J=C(1);

```

```
Wbt(i)=Wb(i)+Wk(I,J);  
k=~(ismember(DD2,[value]));  
DD2=k.*DD2;  
end
```


REFERNCES

1. Salwa A.K. Mostafa, Naser-EL-Sheimy, A.S.Tolba, F.M.Abdelkader and Hisham M.Elhindy, "Wavelet-Packets based Blind Watermarking for Medical Image Management", the open biomedical engineering journal, 2010.
2. Prithish Bhautmage ,Amuthya Jeyakumar, Ashish Dahatonde, "Advanced Video Steganography Algorithm", International Journal of engineering research and application(IJERA), Vol.3, Issue 1, January 2013 .
3. Stefan Katzenbeisser and Faviën A.P.Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House on Demand, 2000.
4. Fabien A.P.Peticolas,Ross J.Anderson and Markus G.Kuhn, "Information Hiding-A Survey", Processing of the IEEE, special issue on protection of multimedia content, July 1999.
5. Vikas Pratap Singh, Shrikant lade, " Haar Wavelet Domain Analysis of Image Steganography", International Journal of Technical Research and Application, Vol.1, Issue 5, Nov-Dec2013 .
6. Prithish Bhautmage ,Amuthya Jeyakumar, Ashish Dahatonde, "Advanced Video Steganography Algorithm", International Journal of engineering research and application(IJERA), Vol.3, Issue 1, January 2013.
7. Dipti Kapoor Sarmah, Neha Bajpai, "Proposed System for data hiding using Cryptography and Stegnography", International Journal of Computer applications, 2010.
8. Pye Pye Aung, Tun Min Naing, "A Novel Secure Combination Technique of Steganography and Cryptography", International Journal of Information Technology, Modeling and Computing, Vol.2, February 2014.
9. Zhang Dinghui, Dong Haixia, "Researches on Digital Image Watermarking", The Eight International Conference of Electronic Measurement and Instruments, 2007.
10. Matt L. Miller,Ingemar J. Cox and Jean-Paul M.G. Linnartz Ton Kalker , "A review of watermarking principles and practices" , Published in "Digital Signal Processing in Multimedia Systems, Ed. K. K.Parhi and T. Nishitani, Marcell Dekker Inc., 461-485, 1999.

11. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, "Techniques and Applications of Digital Watermarking and Content Protection", Artech House, 2003.
12. M. Kutter and F. Petitcolas, "A fair benchmark for image watermarking systems," Electronic Imaging 199: Security and Watermarking of Multimedia Content, Vol. 3657 of SPIE Proceedings, San Jose, California USA, 25-27, January 1999.
13. G. Coatrieux, H. Main, B. Sankur, Y. Rolland, R. Collorec, "Relevance of watermarking in medical imaging", IEEE-embs Information Technology Applications in Biomedicine, Nov. 2000.
14. Darko Kirovski and Henrique S. Malvar, "Spread Spectrum Watermarking of audio signals", IEEE Transactions on Signal Processing, Vol. 51, April 2003.
15. B. Pfitzmann, "Information Hiding Terminology", Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May 30-June 1, Lecture notes in Computer Science, Vol. 1174, Ross Anderson (Ed.), pp. 347-350, 1996.
16. Chao Li Ou, "Text watermarking for text Document Copyright Protection", 2003.
17. S. Craver, N. Memon, B. Yeo, and M. Young, "On the invertibility of invisible watermarking techniques," Proc. Of the IEEE Int. Conf. On Image Processing 1997, Vol. 1, p. 540-543.
18. Frank Y. Shih, Scott Y. T. Wu, "Combinational image watermarking in the spatial and frequency domains", Computer Vision Laboratory, Department of Computer Science, New Jersey Institute of Technology, Newark, NJ 07102, USA, February 2002.
19. Saraju P. Mohanty, "Digital Watermarking: A Tutorial Review", Indian Institute of Science, Bangalore, 1999.
20. Vijaya K. Ahire, Vivek Kshirsagar, "Robust Watermarking Scheme Based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for Copyright Protection of Digital Images", International Journal of Computer Science and Network Security, VOL. 11 No. 8, August 2011.
21. Amit Kumar Singh, Mayank Dave and Anand Mohan, "A Novel Technique for Digital Image Watermarking in Frequency Domain", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012.

22. Manjit Thapa ,Dr. Sandeep Kumar Sood and A.P Meenakshi Sharma , "Digital Image Watermarking Technique Based on Different Attacks", International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011
23. Awanish Kr Kaushik, "A Novel Approach for Digital Watermarking of an Image Using DFT",International Journal of Electronics and Computer Science Engineering 35 ISSN-2277,1986 .
24. Radhika v. Totla, K.S.Bapat , "Comparative Analysis of Watermarking in Digital Images Using DCT & DWT",International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.
25. Zhang Dinghui ,Dong Haixia and Zhou Chao,"Researches on Digital Image Watermarking", The Eighth International Conference on Electronic Measurement and Instruments ICEMI,2007 .
26. Amit Kumar Singh, Nomit Sharma, Mayank Dave and Anand Mohan,"A Novel Technique for Digital Image Watermarking in Spatial Domain", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012.
27. B.Chandra Mohan , S. SrinivasKumar and B.N.Chatterjee, "Digital image watermarking in dual domains", Signal Process385-403 ,1998.
28. Pooja Dabas and Kavita Khanna, "Efficient Performance of Transform Domain Digital Image Watermarking Technique over Spatial Domain", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.
29. Yinghua Lu, Wei Wang, Jun Kong, Jialing Han and Gang Hou, "Joint Spatial and Frequency Domains Watermarking Algorithm Based on Wavelet Packets",S. Zhang and R. Jarvis (Eds.): AI 2005, LNAI 3809, pp. 934 – 937, 2005.© Springer-Verlag Berlin Heidelberg 2005.
30. Melinos Averkiou, "Digital Watermarking", University of Cambridge, 2011.
31. S.Bekkouche and A.Chouarfia, "A New Watermarking Approach– Combined RW/CDMA in Spatial and Frequency Domain", International Journal of Computer Science and Telecommunications, Volume 2, Issue 4, July 2011.
32. Frank Y. Shih , Scott Y. T. Wu , "Combinational image watermarking in the spatial and frequency domains", Computer Vision Laboratory, Department of

Computer Science, New Jersey Institute of Technology, Newark, NJ 07102, USA, February 2002.

33. Vijaya K. Ahire, Vivek Kshirsagar, "Robust Watermarking Scheme Based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for Copyright Protection of Digital Images", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.8, August 2011.
34. A. Umaamaheshvari, K. Thanushkodi, "High Performance and Effective Watermarking Scheme for Medical Images", European Journal of Scientific Research, 2012.
35. Wei-Min Yang, Zheng Jin "A Watermarking Algorithm Based on Wavelet and Cosine Transform for Color Images", First International Workshop on Education Technology and Computer Science, 2009.
36. Wadood Abdul, Philippe Carre, Philippe Gaborit, " Error Correcting Codes for robust color wavelet watermarking", EURASIP Journal on Information Security",2013.
37. A.Umaamaheshvari, "Robust Image Watermarking Based on Block Based Error Correction Code", International Conference on Current trends in engineering and technology, 2013.
38. G. Kontazakis, "Telemedicine: Current technological status,applications and future aspects", In: *Proc. Biomedical Imaging IV -Lecturers and Participants*, 4th IEEE-EMBS International Summer School on Biomedical Imaging, France, June 2000.
39. R. R. Colin, C. F. Uribe, and J. A. M. Villanueva, "Robust watermarking scheme applied to radiological medical images", IEICE Trans. Inf. Syst. vol. E91-D, no. 3.
40. Ming-harn Lee, Shu Te Univ, Kaohsiung, "A DC approach to robust watermarking with hamming code",IIHMSP, volume 2,2007.
41. Behrouz A.Forouzan, "Data Communication and Networking", Alan R. Apt, 2007.
42. Stephen B.Wicker, Vijay K.Bhargava, "An introduction on Reed Solomon Codes",International Journal for Industrial and applied Mathematics, 1960.

43. Martyn Riley and Iain Richardson, "An introduction to Reed-Solomon Codes: principles, architecture and implementation", Indian Journal of Science and Technology, Volume 2, March 2009.
44. Saied Amirgholipour Kasmani, Ahmadreza Naghsh-Nilchi "A New Robust Digital Image Watermarking Technique Based On Joint DWT DCT Transformation. Third 2008 International Conference on Convergence and Hybrid Information Technology IEEE computer society, 2008.
45. Nikita Kashyap and G.R.Sinha, "Image Watermarking Using 2-level DWT" ,Advances in Computational Research, ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 4, Issue 1, 2012.