MAJOR PROJECT REPORT

ON

# AN IMAGE WATERMARKING TECHNIQUE USING POWER SPECTRUM CONDITION

Submitted for the Partial Fulfillment of the Degree

MASTER OF TECHNOLOGY

IN

SIGNAL PROCESSING AND DIGITAL DESIGN

BY

PRINCE GARG
2K15/SPD/11

Under the Guidance of

Dr. JEEBANANDA PANDA

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY, DELHI-110042
(SESSION 2015-2017)

# CERTIFICATE

This is to certify that the thesis entitled "An Image Watermarking Technique Using Power Spectrum Condition" is being submitted by Prince Garg, 2K15/SPD/11 for partial fulfillment of the degree "Master of Technology" in "Signal Processing and Digital Design" from Delhi Technological University. This work carried out by Prince Garg under my guidance and supervision. The matter contained in this thesis has not been submitted elsewhere for award of any other degree.

Dr. Jeebananda Panda
Associate Professor
Deptt. of E&C Engg.
Delhi Technological University
Delhi-110042

# ACKNOWLEDGEMENT

I would like to express my heartily gratitude and thanks to my project guide Dr. Jeebananda Panda, Associate Professor in Department of Electronics and Communication Engineering, Delhi Technological University, for continuous inspiration, encouragement and guidance in every stage of preparation of this thesis work.

I am also extremely thankful to Dr. S. Indu, Head of the Department of Electronics and Communication Engineering, Delhi Technological University, for the support provided by her during the entire duration of degree course and especially in this thesis.

I would like to thank my batch mates for their support throughout the entire duration of the degree.

Prince Garg
2K15/SPD/11
Department of Electronics and Communication Engineering
Delhi Technological University

# ABSTRACT

In this project, the energy efficient watermarking scheme is explored. The energy efficient watermark has the power spectrum which is same as the power spectrum of the original signal, So, the watermark signal has high resemblance with original signal. In order to be energy efficient, the watermark must satisfy the power spectrum condition according to which the power spectrum of watermark signal is directly proportional to power spectrum of original signal. The watermarks which follow the criteria of power spectrum are more robust as compared to the watermarks which do not fulfill the criteria of power spectrum condition. The watermark which do not satisfy the power spectrum condition are vulnerable to Wiener attacks whereas the watermark which are PSC complaint are highly resist to wiener attacks and the watermark can be recovered with very high perceptibility.

# TABLE OF CONTENTS

# List of Figures

# List of Tables

# CHAPTER 1

# 1. INTRODUCTION

In the advance age of technology it becomes very easy to copy, store and distribute the digital data such as digital images, audio, video and texts over the internet. This easy availability of distribution compromises the intellectual property of the digital data. The production house of the digital data such as images, video, audio wants to protect their property against unauthorized use. In paper [1], Dr. György Molnár PhD., Dr. Zoltán Szűts PhD, describes the availability of data over the internet.

One way to protect the copyright data is digital watermarking. Digital watermarking is process in which we add an additional message in the host file (image, audio, video and text) without compromising the quality of the host file, through the embedded information we can authenticate and protect the digital data. The encrypted watermarks are used very often as they are difficult to remove. Digital watermarking is very useful in protecting the intellectual property of the digital content.

Digital watermark is highly robust in nature so it can survive various kinds of attacks which include filtering operation, geometric attacks such as rotation, cropping, scaling etc.

## 1.1 CRYPTOGRAPHY

Cryptography is an encryption technique in which we hide the information such that it can only be decrypted when correct key is used. This is method of secret communication in which only the sender and receiver can extract the secret information from the message. After the encryption, ciphers are generated which no one can understand. The major advantage of cryptography is it does not need complex computation for decryption it can be decrypted by human visual system. In the paper [2], the ciphers are generated with the scheme used gave no information from the visual inspection and the graying effect was reduced to zero due to the high contrast nature of ciphers. The people in this field are called cryptographers. There are majorly four aim of cryptography; they are integrity, confidentiality, authentication and non-repudiation. Cryptography provides secrecy in sending the message, in storage, in authentication, it gives credibility to the overall system.

## 1.2 STEGANOGRAPHY

Steganography is a hidden communication mode that means covered writing. In steganography, the message is hidden in another message and the resulting message looks like a normal message

whereas in cryptography, the hidden message is encrypted that no one can understand until he/she has the key. Steganography hides the information in plain sight, whereas in cryptography the encrypted information is a string of meaningless characters so it may raise questions of secret activity. When someone is using steganography then he/she must be cautious while reusing the pictures, sound or some other content. Steganography is very useful in preventing data alteration, providing access for distribution of digital content, storage of secret data.

**Fragile Invisible Steganography Algorithm "Manipulating LSBs"**

**Goal: To hide image-B in image-A**

- Replace one LSB of image-A with the corresponding one MSB of image-B
- Replace two LSBs of image-A with the corresponding two MSBs of image-B
- Compare the results of the two manipulations with the original image-A
- In general, replace 'k' LSBs of image-A with the corresponding 'k' MSBs of image-B, and observe the results.

## 1.3 DIGITAL WATERMARKING

Digital watermarking is a process of hiding an additional message in the host file, such as text, audio, video, image, after addition of such watermark in the digital content, it is possible to locate the source of the leak and then it is possible to put a dot in the piracy industry.

Digital watermarking is smart way of inserting digital information in digital media. It more or less works like a digital communication system in which the signal to be transmitted is align with the channel and then transfer it through the channel, after that it is received at the receiver.

While transmission the watermarked signal may suffer some distortion such as geometrical attacks which include rotation, cropping and filtering attacks. The distortion that watermarked signal experience could be intentional or unintentional attacks. Intentional attacks are those attacks which have a motive of modifying the watermark in the watermarked data so that they can abuse the digital content in whatever way they want without getting caught. The unintentional attacks include the distortion introduced by mainly the transmission channel for example, JPEG compression in which some of the bits in the watermarked data gets lost and watermarked becomes noisy and it affects the embedded information in the host file, analog to

digital and digital to analog conversion during transmission these are the operations which can introduce distortion in the watermarked data.

Digital watermarking is quite a useful method to protect the copyrights and authenticity of intellectual property. Spatial [19] and frequency [20] are two domain in which watermarking can be done.

The spatial domain watermarking technique has low computational cost and a fragile one, a fragile watermark gets damaged upon any attack on the watermarked signal, in this, the watermark is embedded by modifying the bits of the pixels, Whereas the robustness of frequency domain watermarking technique is very high and the watermark won't get damaged so easily upon the attack, the transformed digital content is modified and then inverse transformation is used to construct the watermarked media.

Watermarking in images is very popular field of research and study. In digital images, watermarking must meet some of the prime requirements for implementation, some of them are:

### 1.3.1 Imperceptibility:

Imperceptibility implies that there should be perceptual equivalence between the watermarked data and the unwatermarked original data. In some application the watermark needs to imperceptible as well. The embedded watermarks should not create any visible signs in the image, change the bitrate of video files and audible frequencies in the audio files. The watermark should be chosen in such a way that it does not compromise the fidelity of the host file.

### 1.3.2 Robustness:

Robustness is very important to watermarking system, it implies; In the watermarked data, the embedded watermark cannot be make undetectable without degrading the quality of the image or host file so that the attacker cannot abuse the data for his/her own personal gain. So that the embedded watermark should be able to survive various kinds of attacks such as JPEG compression, rotation, Gaussian noise, salt and pepper noise, scaling, cropping, filtering

operations. Some of the attacks are unintentional such as compression, filtering operation during transmission because while transmitting data over the channel one may need to apply A/D and D/A conversion.

The watermark must be robust with respect to the following concerns:

#### 1.3.2.1 Inseparability:

The attacker must not be able to separate the watermark from the watermarked data without degrading the quality of the host file.

#### 1.3.2.2 Common Signal Processing:

The watermarked should be robust enough to survive the common signal processing operations such as D/A and A/D conversion, low pass filter, high pass filter and median filter.

#### 1.3.2.3 Common Geometric Distortions:

The watermarked data should be robust enough to survive geometric attacks such as rotation, cropping, scaling and translation.

#### 1.3.2.4 Subterfuge Attacks (Collusion and Forgery):

A watermark should be robust to the repeated watermarking that implies forgery, and watermark should be able to survive the collusion that is group of same data watermarked with different watermark.

#### 1.3.2.5 Unambiguousness:

The identification of the owner should be unambiguous after the extraction of the watermark.

### 1.3.3 Capacity:

Capacity is the trait which gives the possibility of embedding large number of different watermarks. In [3], it is stated that the most significant components of the image carry enough perceptual capacity that watermark can be inserted without degrading perceptually. This fact implies that whenever an attacker tries to manipulate the watermark then the attacker also manipulates the most significant components of image so the attacker cannot abuse the intellectual property of the digital image.

### 1.3.4 Security:

The digital watermarking techniques are designed in such a way that only authorized users are able to detect/modify the watermark signal in the host file. We can make sure that only authorized have the access to watermarking through keys, only the user with the key is recognized as the authorized user.

### 1.3.5 Image fidelity:

When we perform the watermarking on image then it is inevitable that it degrades the quality of the image. To keep this degradation minimum, there is a tradeoff between the strength of embedded watermark and the quality of the host file; we make sure that no difference can be observed in the image fidelity.

### 1.3.6 Payload Size:

Payload size is very important property in watermarking model. Each watermarked carry some payload due to the embedded watermark in it. There are many watermarking that needs only one bit to be embedded and there are others which may require multiple bits embedded in it.

### 1.3.7 False Positive Rate:

This is also very important property in a watermarking system. This rate represents the number of digital data in which watermark is detected but in actual watermark was never embedded in those digital data. The watermarking systems should be designed in such way that false positive rate should be as low as possible.

## 1.4 APPLICATIONS OF DIGITAL WATERMARKING

Let us look upon some of the scenarios where watermarking is being already used as well as other potential applications. The list given here is by no means complete and intends to give a perspective of the broad range of possibilities that digital watermarking opens.

### 1.4.1 Image Watermarking:

There are various techniques that are developed for the watermarking of images. In image watermarking, the watermark is directly embedded into the original image data by modifying its color components such as RGB components in case of color image watermarking. In this way, we can take the advantages of perceptual and robustness properties of manipulations in signal.

Imperceptibility, survival against signal processing operations and capacity are prime requirements of image watermarking. Signal operations against which we intend that our watermark is strong enough to resist them are JPEG compression, filtering operations, scaling, cropping, rotation, and additive noise.

There is another property which plays major role in embedding the watermark signal that is capacity which signifies the amount of data that can be embedded in the image and at the receiver end can be detected with reliable output.

Most of the available watermarking schemes are additive in nature as we simply add the watermark signal in the host image or in its transformed version. The embedded watermark signal must be scaled in an appropriate manner so that the distortion can be reduced to minimum level. For determination of the scaling factor, perceptual models can be employed in the watermarking system. The watermark information, original image information, key to the extraction all are part of watermark itself. Common examples of watermark used to embed are PN sequences, a 2D signal (for example: image), or a digital signature or some personal message. There are many watermark techniques which insert only one bit of information for a whole lot of pixels and then they can recover the data at the receiver end. These techniques are called spread spectrum approach. In Image watermarking model, the watermark information is directly added to the pixel values of the image in spatial domain or in transform domain, the transforms which are popularly used for this work are discrete cosine transform, discrete Fourier transform, discrete wavelet transform.

There are watermarking schemes which uses random M sequences as watermark as they have good correlation properties so that watermark can be detected easily by taking into account that property. These techniques are cheap and we can also take 2D M sequence which can be added on a block by block basis and detection can be done in the same manner.

### 1.4.2 Video Watermarking:

The digital era has changed the distribution of multimedia at a very large scale. By exploiting the internetwork and advance software technologies one can easily create the copies of high quality digital videos in no time and can distribute it with the use of vast network available throughout the world. The applications of videos cover a very wide category some of them are: broad casting, conferencing and video on demand etc, these applications also create security issues,

videos can be tempered, forged and copyright issues [4]. So videos needed to be protected against their unauthorized usage, digital watermarking can provide protection against copyright issues and unauthorized use.

### 1.4.3 Audio Watermarking:

In audio watermarking, frequency and time masking properties of the human ear are employed in the watermark and make it inaudible to the human ear. One of the challenges in this process is the synchronization of the watermark and watermarked audio file.

### 1.4.4 Hardware/Software Watermarking

Watermarking model allows us to protect the copyright property of every kind of data. When same information can be expressed in two different ways than one bit of information can be guarded. It implies that compression does not leave space for watermarking.

In hardware context, different but equivalent Boolean expressions can be used to have different types of gates and that can be addressed by the hidden information bits.

### 1.4.5 Text Watermarking

Text watermarking is an approach which is used to protect the copyrights of text documents. As we watermark the text document that means, the text document is carrying the copyright information so that if someone tries to use it in unauthorized way he/she will get caught. In the computer era, it is very easy to generate the copies of confidential documents so watermarking the text documents is necessity. There are two types of watermark: visible and invisible. In invisible watermarking, some information is embedded into the text document and that information will get pass into the copies of the same text document easily.

### 1.4.6 Labeling

The watermarking information also contains labels that help in annotation of digital data such as image and video. With watermarking it becomes very hard to delete the label, this methodology is used in medical applications since it can prevent fatal errors.

### 1.4.7 Transaction Tracking

This is very application of watermarking. The embedded watermark in the host file can be used to record more than one transaction in the history of the copy of this work. For example: we can embed a different watermark in each copy of a movie so, in case the movie leaks then the source of the leak can be identified by the watermarking information.

### 1.4.8 Owner Identification

Digital watermarking can be used to identify the owner of a particular digital file such as image, audio and video. It becomes a very important task when the copyright infringement issues are involved so by inserting proper watermark in digital data copyright infringement issues can be solved very effectively.

### 1.4.9 Broadcast Monitoring

This is one of the crucial applications of digital watermark. There are many giant organizations who pay for the broadcasting of their product advertisement [18], they pay a lot of money for the air time, and they can make sure of the air time they bought by the use of digital watermarking, they can simply insert the watermark in their advertisement whether it is image, audio or video, they can monitor their advertisements on the TV from their monitoring station.

### 1.4.10 Authentication

With the increasing technology, the digital photographs can be easily modified in a very perfect way so that it becomes very difficult to detect that it's a forgery. There are many areas of study which needs to authenticate the data such as legal cases and medical applications [5]. The most optimum solution to this problem is digital watermarking. We can simply insert the watermark in the digital data whether it is image, video or audio and that watermark stays with the digital data as long as we want so forgery can be prevented by the use of digital watermarking. Digital watermark can also resist various attacks on the host file so that watermark remains intact, some common examples of attacks are: common signal processing operations such as rotation, scaling, cropping, and some filtering operations.

### 1.4.11 Covert Communication

It is one of the primary applications of watermarking; in this the secret messages are transferred from sender to receiver. In paper [11], Simmons stated the prisoners problem, in which two prisoners are held captive in the holding cell, they can pass the messages to each other through

warden, but warden punishes them if he finds out that they are planning to escape so that they have to hide the information in the messages in such a way, to warden the messages should appear normal with no escape activity.

## 1.5 DISTORTION AND ATTACKS

A watermarked data can altered through various kinds of attacks, the attacks could be on purpose or not but the watermarking system should be able to detect and extract the watermark. The distortions we consider are those in which the fidelity of the host is maintained otherwise the host file gets unusable. The distortions caused in the watermarked data degrade the performances of the watermarking systems.

Some of the common attacks and distortions we come across in watermarking are:

### 1.5.1 Additive Noise

Additive noise may be introduced in the watermarked data from analog to digital or digital to analog conversion while transmission. Or it may be introduced by the attacker to destroy the watermark and make unauthorized use of the digital data. It includes additive white Gaussian noise, salt n pepper noise.

### 1.5.2 Filtering

Filtering is the most common operation in digital signal processing, so whenever the watermarked data is processed then there is a high probability that it must have undergone some filtering operation, we have consider the low pass filter, high pass filter and median filter in this class and tested the performance of the system that the watermark from the watermarked data can be detected and extracted.

### 1.5.3 Cropping

This is a very usual attack on the digital images, suppose the attacker is interested in only some part of the watermarked data say, a portion of the image or some limited number of frames in the video sequence. So the watermark needs to be present where the attack takes place.

### 1.5.4 Compression

Compression is a very common operation in today era of internet. All the digital data which is distributed over the internet is in compressed form. So, the watermarking model should be able to detect and extract the watermark from the watermarked data.

### 1.5.5 Rotation and Scaling

These attacks come under the category of geometric attacks. They are often used by the attacker in order to disrupt the watermark information embedded in the digital data. The watermarking model should be able to resist against these attacks and the watermark can be detected and extracted after these attacks on the watermarked data.

### 1.5.6 Statistical Averaging

In this attack, an attacker tries to estimate the array of watermark so that he/she can subtract the estimated value from the watermarked data and left with original data to abuse. Because of this the watermark must depend upon the original data so that if attacker is able to remove the watermark than the host file gets damaged and it is of no use anymore.

## 1.6 PREVIOUS WORKS

In [6], Caronni added insignificant geometric patterns in the digital images on their brightness level. The idea of embedding a spatial watermark in a 2D signal is excellent but this scheme may be susceptible to attacks on the bit level. As the level of attack increases the watermark information in the digital image becomes weaker and after a while it is not possible to detect and extract the watermark from the host file.

In [7], Brassil define three ways for document images in which text is present. These are as follows: vertically shifting text lines, horizontally shifting words and altering text features such as the vertical endlines of individual characters. All the three methods are susceptible to attacks.

In [8], Tanaka, *et al*. proposes watermarking the facsimile data. This method increases or decreases the some runs of data in the run length code used to generate the coded fax image, this method is prone to A/D and D/A conversion.

In paper [9], A method is discussed for watermarking of images. In the discussed method, the watermarking information is inserted in the least significant bit of pixels. As the watermarking information is embedded in the least significant bit so it can be easily destroyed.

In paper [10], Rhoads, *et al*. discussed a method in which random quantities are added or subtracted from each pixel. The decision of addition or subtraction took on the basis of least significant bit value; if it is equal to the corresponding bit in the mask than it is added otherwise subtracted. This method does not take collusion attacks in account.

## 1.7 DIGITAL WATERMARKING SYSTEM

There are various ways in which one can model the watermark system. Essentially, a watermarking model consists of an embedding unit and a detector unit as shown in the figure below. The embedding unit inserts the watermark signal in the original image whereas the detector/extractor unit recover the presence of watermark signal. The watermark key here in the model of watermarking system is optional, it is mainly use for encryption purpose [17]. The watermark key is unique for every watermark. When the watermark key is taken into account than this key is only known to authorize users, and this makes sure that the watermark can only be recovered by the authorized parties. The communication channel introduces noise during transmission as we have to process the signal in order to transmit it so some common signal processing operations are implemented in this part for example, compression, A/D and D/A conversions. Because of the noises introduced during transmission and attacks on the watermarked data in order to abuse the copyrighted content, the watermarking model should be robust against theses noises and attacks.

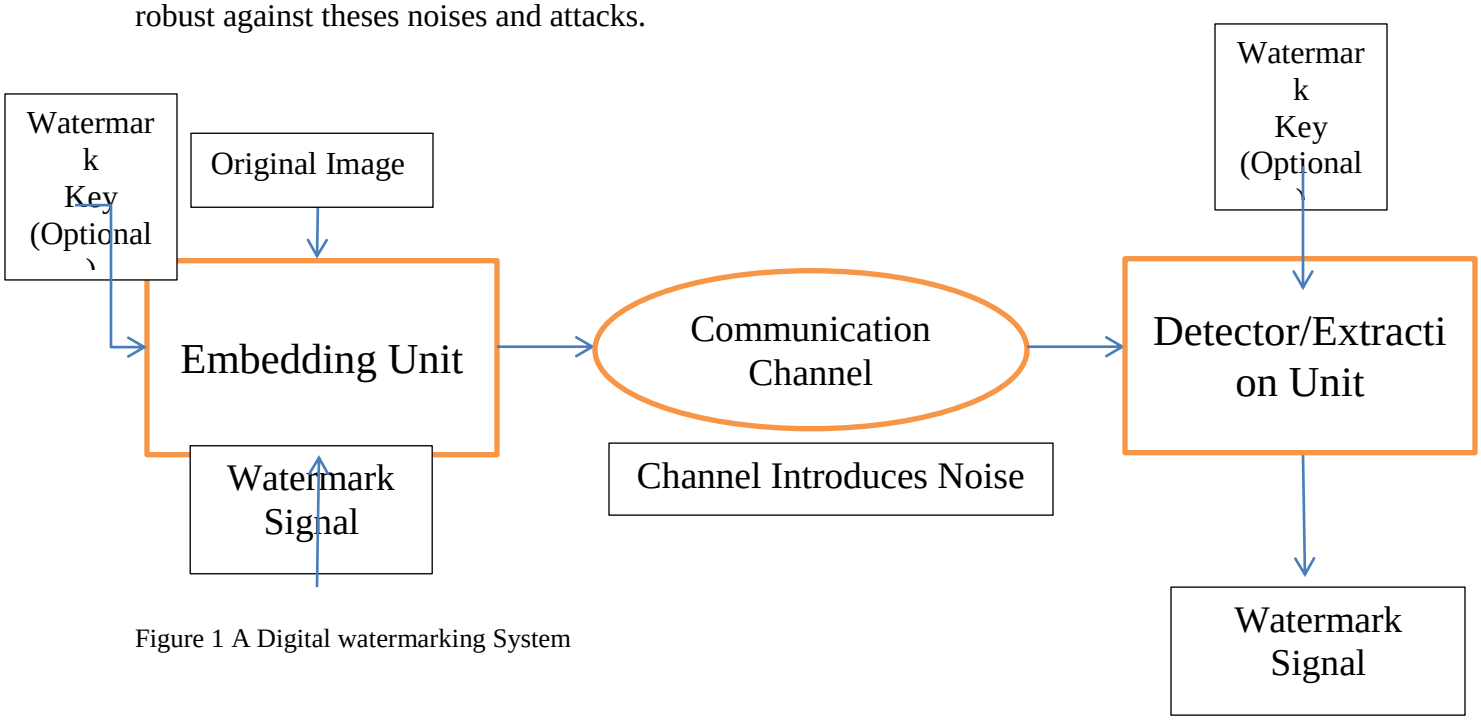



Figure 1 A Digital watermarking System

## 1.8 STRUCTURE OF WATERMARKING SYSTEM

There are two units in every watermarking system 1) Insertion unit 2) Detection/Extraction Unit. A block diagram of inserting a watermark in any digital data is shown below in figure 2. The block diagram represents a watermark insertion unit which takes user key, input image and

watermark as input and it gives watermarked image at the output. The user key mentioned here is optional; it is used when we want to add additional security to the watermarking model so that only authorize users can access and modify the watermark signal, no illegal activity can be performed on the digital data by the attacker. The attacker may employ certain attacks include, JPEG compression, low pass filter, high pass filter, median filter, rotation, scaling, cropping, wiener filter, Gaussian noise, salt n pepper noise. We can protect the watermark from these attacks by increasing the strength of the watermark to be embedded but there is tradeoff between the strength of the watermark in the host image and the perceptual quality of the original image. The watermarked image should not be distinguishable from the original image.

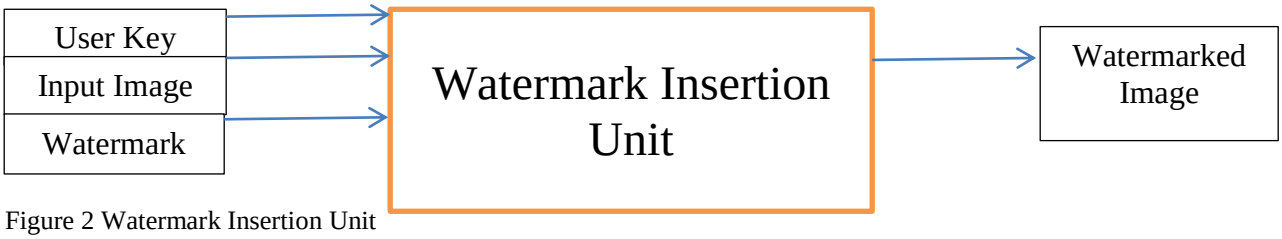



Figure 2 Watermark Insertion Unit

The diagram given below represents the watermark extraction unit. Extraction of the watermark can be performed in two steps, first is locating the position of the watermark that is where it is embedded in the image and, second is recovering that information.

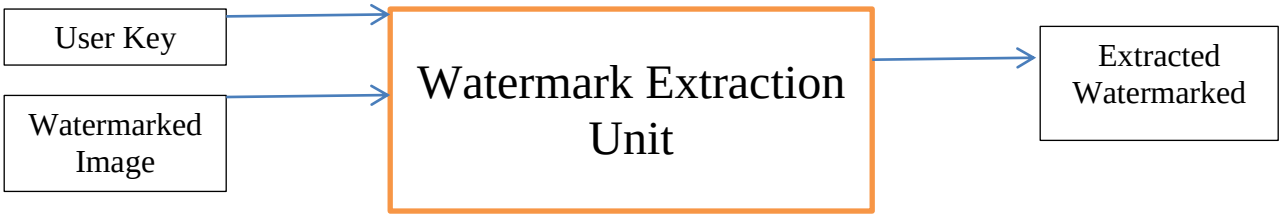



Figure 3 Watermark Extraction Unit

The diagram given below represents the watermark detection unit. The watermark detection unit first extracts the watermark and then the extracted watermark is compared with the original watermark. At the output, the answer is 'YES' if the watermark is present and 'NO' if the watermark is not there.

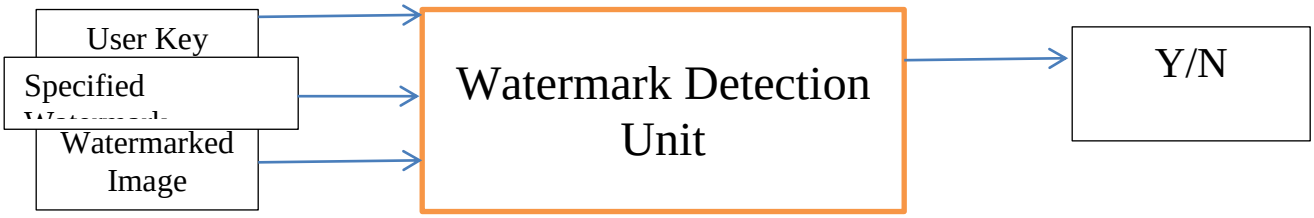



Figure 4 Watermark Detection Unit

# CHAPTER 2

## 2.1 WATERMARKING IN FREQUENCY DOMAIN

Before we explain the significance of frequency domain watermarking, one must know that the marked image pass through a series of operations before extraction or detection. These operations have different effects on the image [3].

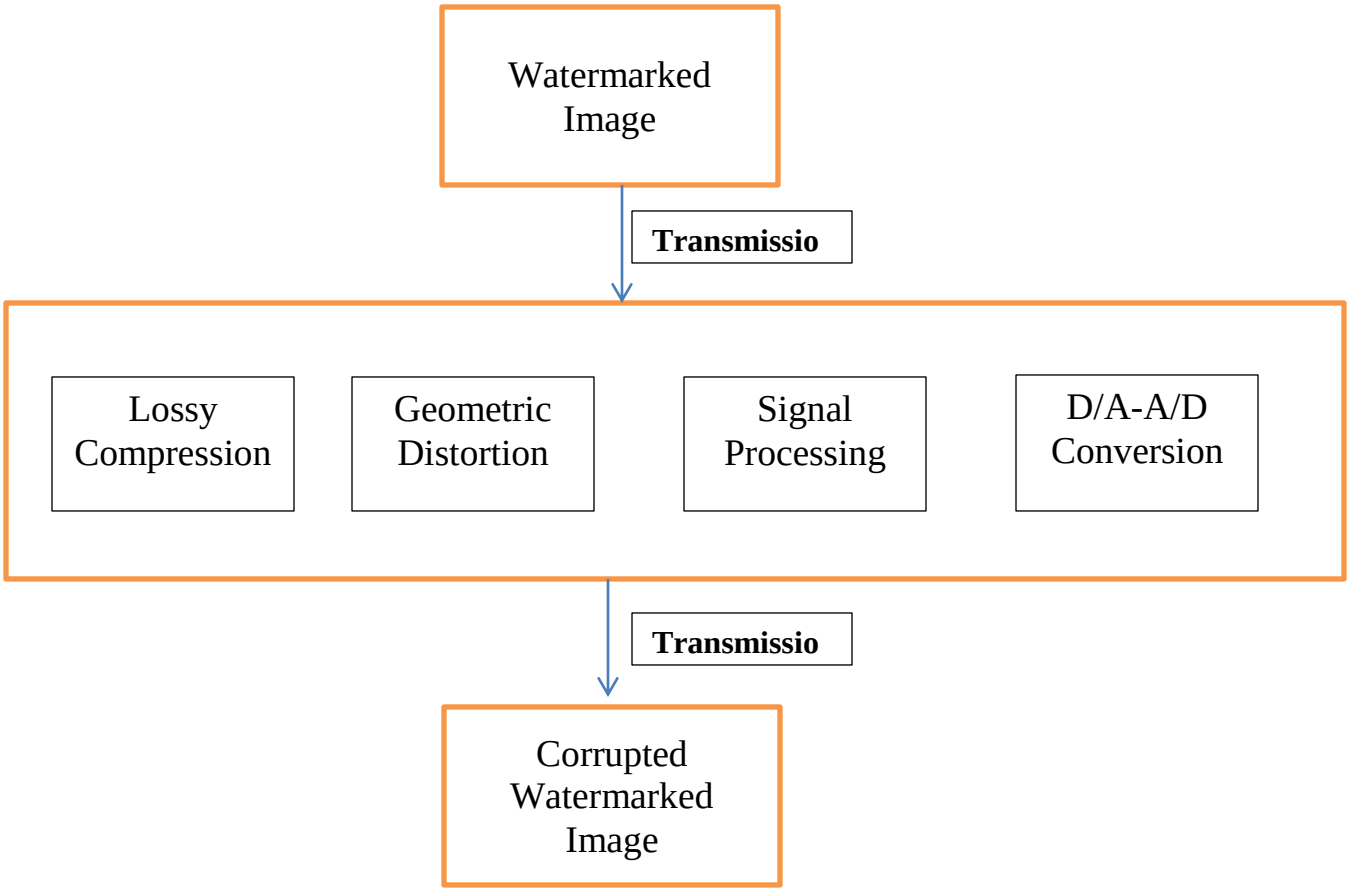



Figure 5 Processing Operations on a Watermarked Image

As shown in the figure above, the term 'Transmission' represents that he watermarked image is to be transmitted across a channel to the receiver end during transmission the channel applies standard encryption techniques. These techniques brought distortion in the watermarked data. In addition to that, the processes involved are lossy in nature hence degrade the quality of the watermarked data, so as we stated earlier the watermarking method should be strong enough to survive these distortions.

Lossy compression [16] operation results in the partial loss of data and degrades the quality of the original data. Most of the above mentioned operations occur in the frequency domain.

At the receiving end, the watermarked image go through a number of transformations depend upon what kind of application we have for the watermarked data. The transformation can be classified into two categories: geometric distortions and signal distortions, geometric distortion include operations such as rotation, scaling and cropping. In cropping, a portion of the watermarked image is removed so this leaves the image with permanent damage however in case of spatial domain watermarking the cropping operation would have damaged the image completely, but in frequency domain the watermark is spread over the whole image so cropping operation seems to have very less effect on the watermarked data [3].

The signal distortion operations include compression, D/A and A/D conversions, additive white Gaussian noise, salt n pepper noise, enhancing color of the image and there are many more. It is very difficult to study the effects of these operations on the image, for example, histogram equalization technique is a simple enhancement scheme of contrast, which can be undone by histogram warping techniques [12].

The watermark must be resistant to these distortions and watermark should be able to survive the attacks by the users who want to abuse the intellectual property of digital data.

## 2.2 WATERMARK INSERTION ALGORITHM

The watermarking scheme must be robust enough to resist different types of distortions whether intentional or unintentional.

In Algorithm, steps involved are:

1. First, we consider the original image and apply 2 level discrete wavelet transform and extract LL2 coefficients.
2. Apply singular value decomposition on the LL2 coefficient matrix of original image, and store the singular values in $S$.
3. Take the watermark to be inserted and apply the 2 level discrete wavelet transform and extract the LL2 coefficients.
4. Apply singular value decomposition on the LL2 coefficient matrix of watermark to be inserted, and store the singular values in $S_w$.
5. Now modify the singular values of original image as per the equation given below:

$$S_{new} = S + \alpha * S_w \quad (1)$$

Where, α represents the embedding strength.

6. After that, inverse discrete wavelet transform is applied to regenerate the original image with modified singular values or to generate watermarked image.

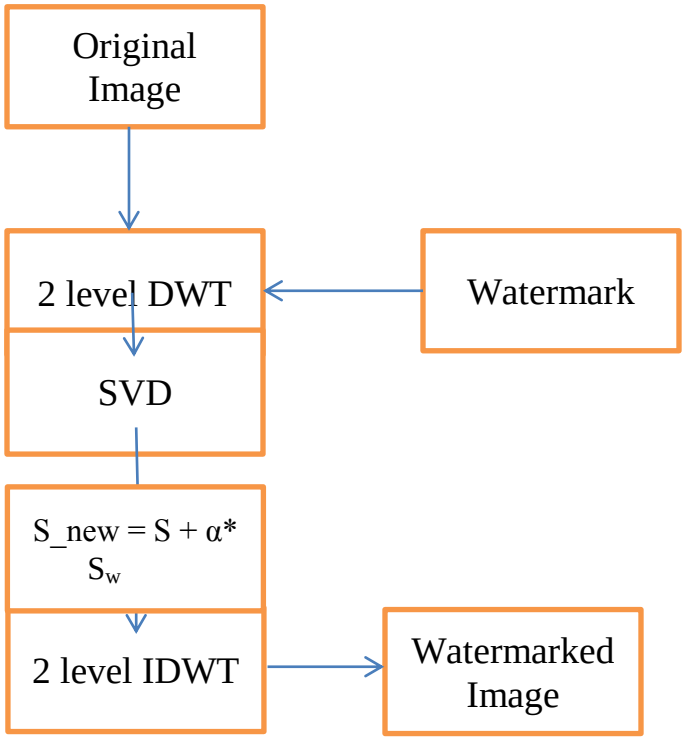



Figure 6 Watermark Insertion Algorithm

## 2.3 WATERMARK EXTRACTION ALGORITHM

This is non-blind extraction scheme, the steps involved are:

1. Take the watermarked image and apply 2 level discrete wavelet transform and extract LL2 coefficients of watermarked image.
2. Apply singular value decomposition on the LL2 coefficient matrix of the watermarked image and store singular values in $S_{wI}$.
3. Now recover the singular values of watermark by the following equation:

$$Swrec = (S_{wI} - S)/\alpha \quad (2)$$

4. Apply the inverse singular value decomposition to reconstruct the LL2 coefficient matrix of watermark.
5. Then, apply inverse discrete wavelet transform to regenerate the watermark.

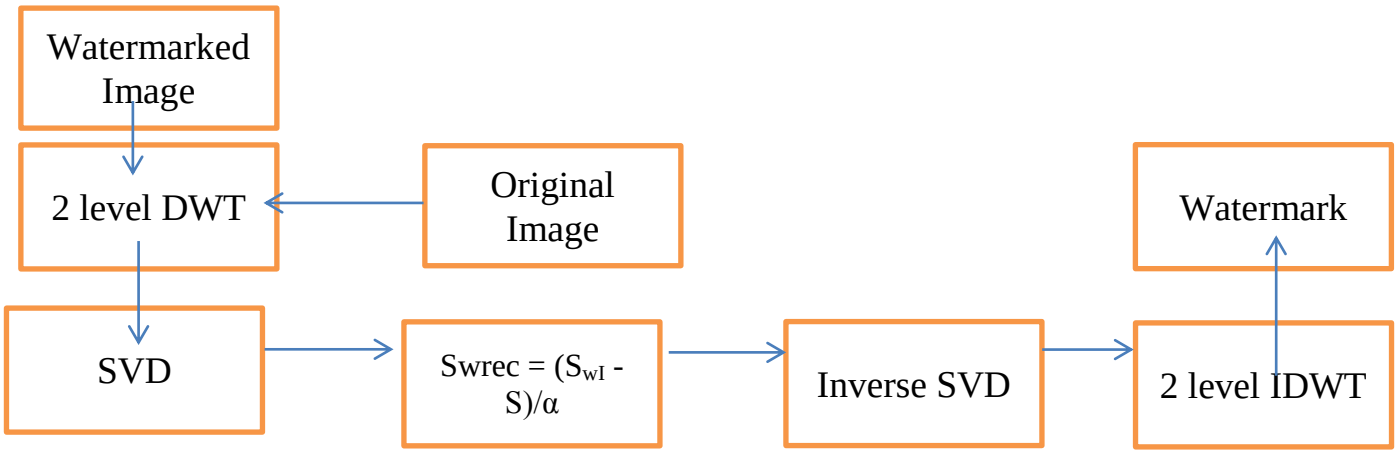



Figure 7 Watermark Extraction Algorithm

# CHAPTER 3

## 3. ENERGY EFFICIENT WATERMARKING

Energy efficient watermarking is one of the scheme in which the watermark is able to resist the MMSE estimation and gives a more robust watermark to various other attacks as well. Energy efficient watermark must satisfy the power spectrum condition (PSC) [13], as per that the power spectrum of watermark is directly proportional to power spectrum of original signal. It is shown in the results and analysis section that PSC compliant watermark are more robust to various attacks.

### 3.1 GENERATE PSC COMPLIANT WATERMARK

The PSC compliant watermark can be generated by the equation given below [13]:

$w[n1, n2] = Sqrt(\sigma^2_w / \sigma^2_x) IDWT\{sqrt(Per_{xx}[k1, k2]) * U[k1, k2]\}$ (3)

Where, $U[K1, k2]$ is 2-D DWT of the output $u(n1, n2)$ of a unit variance white Gaussian random number generator, and

$Per_{xx}[k1, k2] = |X[k1, k2]|^2/(N1*N2)$

Where, $X[K1, k2]$ is the 2D – DWT of $x[n1, n2]$,

$U[K1, k2]$ is the 2D – DWT of $u[n1, n2]$.

### 3.2 DISTORTION MEASURE

It is the measurement of distortion between attacked signal $\hat{x}$ and the original signal $x$ through sample mean squared error.

$$D(\hat{x}, x) = \frac{1}{N} \sum_{n \epsilon N} (\hat{x}[n] - x[n])^2$$

### 3.3 WIENER ATTACK

The goal of the attacker is to minimize $D(\hat{y}, x)$, the signal after Wiener attack [13] is:

$\hat{y}[n] = g[n] * y[n] + v[n]$

$\hat{y}[n] = g[n] * [x[n] + w[n]] + v[n]$ (4)

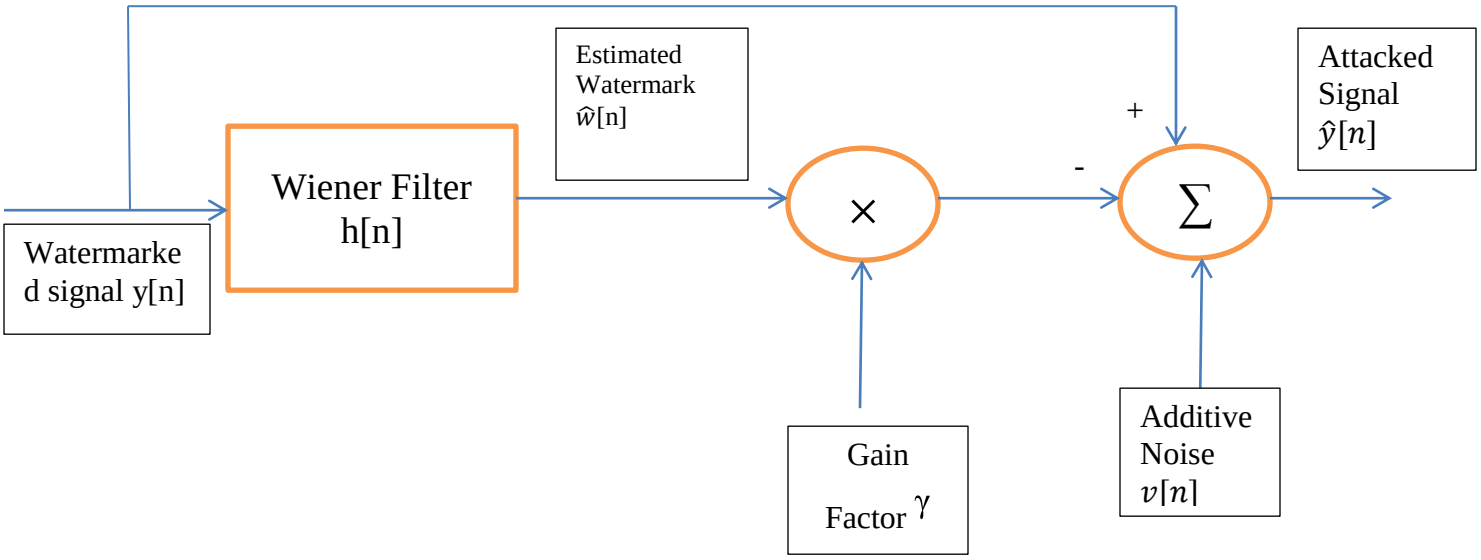



Figure 8 Block Diagram of Wiener Attack

Given, $\Phi_{xx}(\omega)$, $\Phi_{ww}(\omega)$ and $r_0$, $D(\hat{y}, x)$ is minimized under the constraint $r = r_0$, iff

$G(\omega) = 1 - \gamma * H(\omega)$ , $\Phi_{vv}(\omega) = 0$

Where, $\gamma$ is a real gain factor.

As per the block diagram shown in figure 8,

$$H(\omega) = \frac{\Phi_{ww}(\omega)}{\Phi_{xx}(\omega) + \Phi_{ww}(\omega)}$$

Equation (4) can be written as

$$\hat{y}[n] = (\delta[n] - \gamma h[n]) * y[n] + v[n] \quad (5)$$

## 3.4 ENERGY EFFICIENT WATERMARKING AND ROBUSTNESS CRITERIA

The normalized mean squared error that is $E/{\sigma_w}^2$, represents the fractional energy of watermark that can resist MMSE estimation. So, we can infer that the energy that can be estimated, it can be removed as well [13]. The watermark with the maximum value of $E/{\sigma_w}^2$ is energy efficient watermark.

## 3.5 POWER SPECTRUM CONDITION

In power spectrum condition, E is maximum [13], iff,

$$\Phi_{ww}(\omega) = \frac{{\sigma_w}^2}{{\sigma_x}^2}\Phi_{xx}(\omega) \quad (6)$$

The maximum MSE is

$$E_{PSC} = \frac{{\sigma_x}^2{\sigma_w}^2}{{\sigma_x}^2 + {\sigma_w}^2}$$

# CHAPTER 4

# 4. DISCRETE WAVELET TRANSFORM OVER FAST FOURIER TRANSFORM

Discrete wavelet transform is very popular in image and signal processing. DWT provides excellent localization in time and frequency domain as well. DWT is preferred over DCT because it is closer to human visual system and more robust to attacks in addition, it also offers inherent scalability and tolerable degradations.

There are different kinds of wavelet transform [14], for example Haar wavelet, Daubechies wavelet *etc*, Haar functions were introduced by Hungarian mathematician Alfred Haar in 1910.

Haar function can be defined as follows:

$$H(x) = \begin{cases} 1 \; when \; 0 \leq x \; \leq \frac{1}{2} \\ -1 \; when \; \frac{1}{2} \leq x \; \leq 1 \\ 0 \qquad otherwise \end{cases}$$

It represents the image at multi-resolution by decomposing it in four sub-bands in case of 2D wavelet decomposition:

LL – represents low horizontal and vertical frequency components

HH – represents high horizontal and vertical frequency components

LH – represents low horizontal and high vertical frequency components

HL – represents high horizontal and low vertical frequency components

To obtain the second level decomposition, we will apply the 2D-DWT on LL sub band obtained through first level decomposition as shown below:

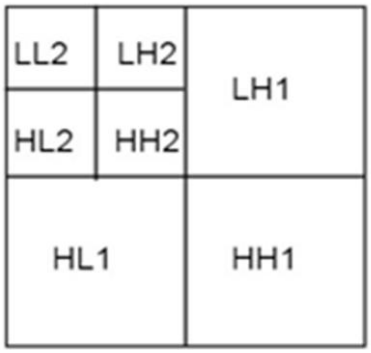



Figure 9 2D Level Decomposition

Discrete Wavelet Transform is preferred over Fast Fourier Transform, one of significant advantage of wavelets is that they are capable of perfectly reconstructing functions through

linear and polynomial shapes, for example: rect function, tria function, second order polynomials, etc. wavelets denoise the signal way better than conventional filters.

In addition to frequency information, discrete wavelet transform also provides time localization. There are different kinds of wavelets which provides different resolution and dilation properties so we can explore in-depth whereas in case of FFT, there are only sine and cosine functions which are in play. Some of different wavelets are Haar, Coiflet, orthogonal wavelets, biorthogonal wavelets [15] etc.

In wavelets, it is very easy to filter the particular frequency component as wavelets divide the frequency components in the above explained fashion.

# CHAPTER 5

## 5. WATERMARKING USING ENERGY EFFICIENT SCHEME

The energy efficient watermark scheme is proven to be more robust against wiener filter, geometric attacks. The energy efficient watermark must satisfy the power spectrum condition according to which the watermark's power spectrum should be directly proportional to the original signal power spectrum. PSC compliant watermarks are proven to be more robust. The watermark which are not based on power spectrum condition are vulnerable to wiener attacks whereas the watermark which are PSC complaint are highly resist to wiener attacks and the watermark can be recovered with very high perceptibility.

### 5.1 WATERMARK GENERATION ALGORITHM

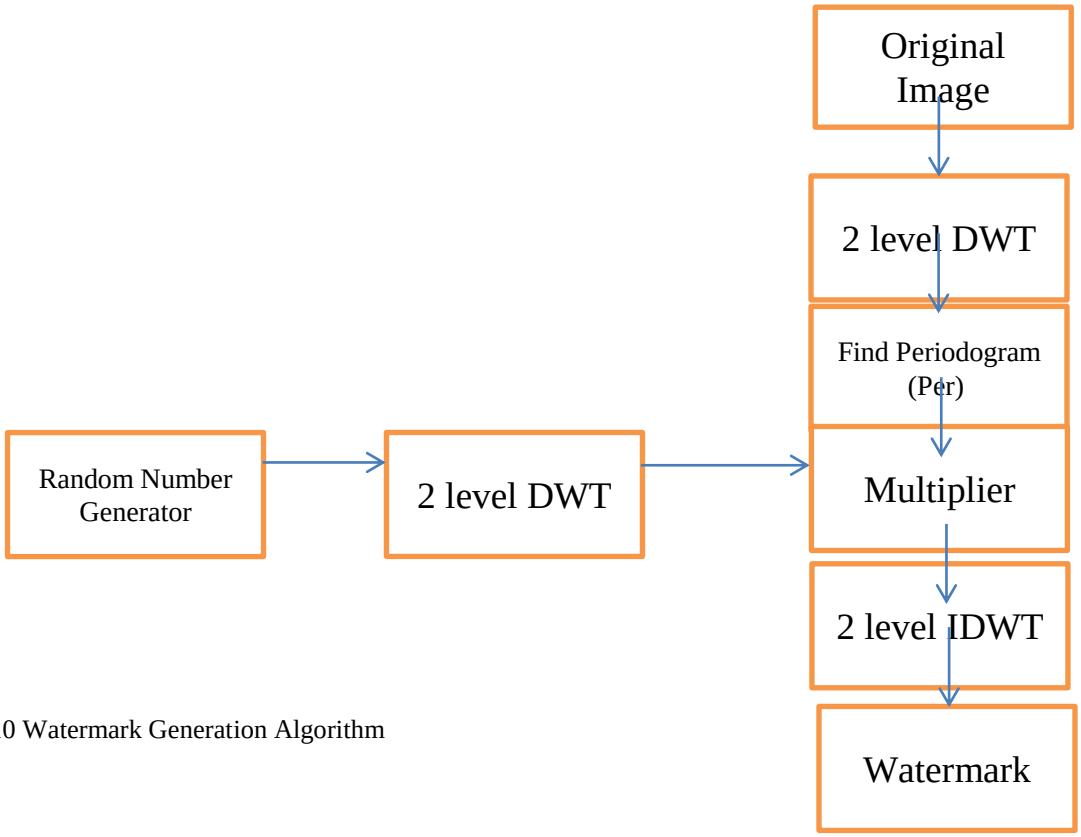



Figure 10 Watermark Generation Algorithm

In watermark generation algorithm, steps involved are:

1. First, we consider the original image and apply 2 level discrete wavelet transform and extract LL2 coefficients.
2. After that, we have find the periodogram of the resulting DWT by applying the following equation:

   $Per_{xx}[k1, k2] = |X[k1, k2]|^2/(N1*N2)$

Where, $X[K1, k2]$ is the 2D – DWT of $x[n1, n2]$.

3. We also generate random number and apply the 2 level discrete wavelet transform.
4. In the next step, multiply the output of random number generator and the periodogram as shown in figure given above.
5. In the resultant output, we apply the 2 level IDWT to generate the watermark signal.

## 5.2 WATERMARK INSERTION ALGORITHM

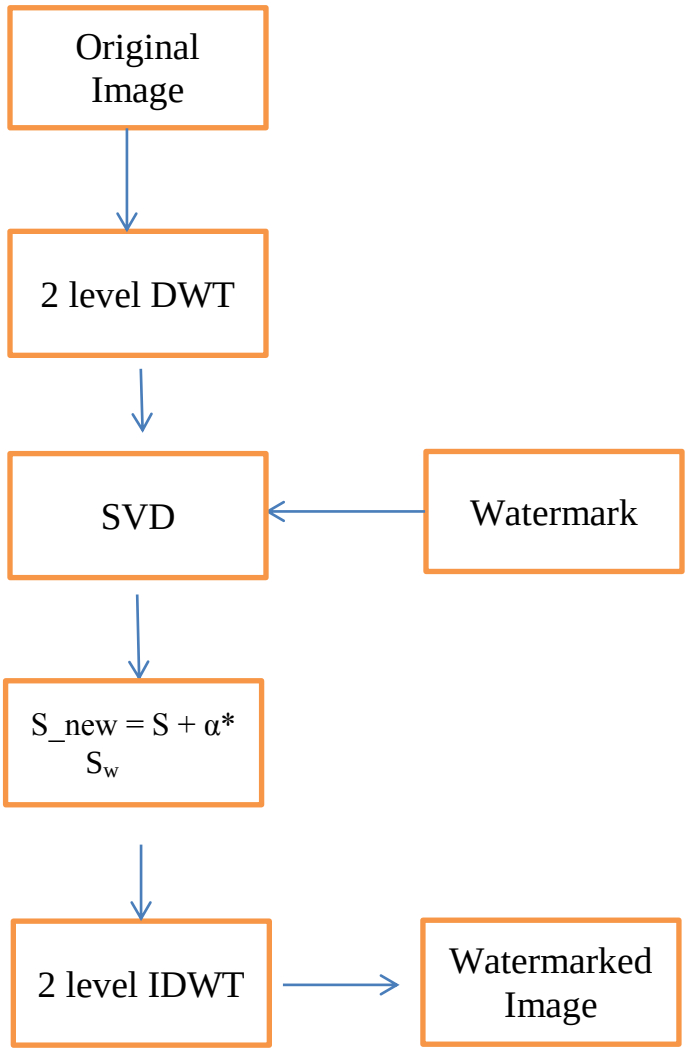



Figure 11 Watermark Insertion Algorithm

In watermark insertion Algorithm, steps involved are:

1. First, we consider the original image and apply 2 level discrete wavelet transform and extract LL2 coefficients.

2. Apply singular value decomposition on the LL2 coefficient matrix of original image, and store the singular values in $S$.
3. Take the watermark to be inserted and apply the 2 level discrete wavelet transform and extract the LL2 coefficients.
4. Apply singular value decomposition on the LL2 coefficient matrix of watermark to be inserted, and store the singular values in $S_w$.
5. Now modify the singular values of original image as per the equation given below:

$$S_{new} = S + \alpha * S_w \quad (7)$$

Where, α represents the embedding strength.

6. After that, inverse discrete wavelet transform is applied to regenerate the original image with modified singular values or to generate watermarked image.

## 5.3 WATERMARK EXTRACTION ALGORITHM

This is non-blind extraction scheme, the steps involved are:

1. Take the watermarked image and apply 2 level discrete wavelet transform and extract LL2 coefficients of watermarked image.
2. Apply singular value decomposition on the LL2 coefficient matrix of the watermarked image and store singular values in $S_{wI}$.
3. Now recover the singular values of watermark by the following equation:

$$Swrec = (S_{wI} - S)/\alpha \quad (8)$$

4. Apply the inverse singular value decomposition to reconstruct the LL2 coefficient matrix of watermark.
5. Then, apply inverse discrete wavelet transform to regenerate the watermark.

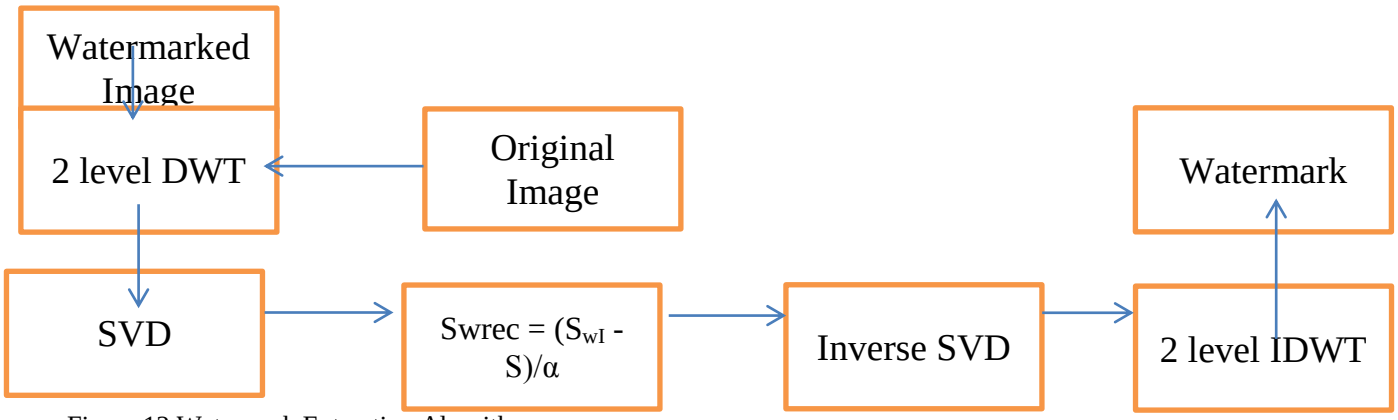



Figure 12 Watermark Extraction Algorithm

# CHAPTER 6

# 6. EXPERIMENTAL RESULTS

## 6.1 DETERMINATION OF α:

α is the embedding strength which indicates the strength of watermark in the watermarked image. If we increase the value α then the peak signal to noise ratio decreases and correlation coefficient increases, and with the increase in the value of α the perceptual quality of the video decreases so we have to choose the value of α such as it maintains the perceptual quality and offers desired peak signal to noise ratio, and the value of α used is 0.60.

## 6.2 ENERGY EFFICIENT WATERMARK AND NON ENERGY EFFICIENT WATERMARK

The energy efficient watermark generated by using the algorithm explained in section 5.1 is given below:

Figure 13 Energy Efficient Watermark

## 6.3 IMAGE SCALING AND RESCALING

In this experimental analysis, I have scaled the watermarked image to 50% of its size and then rescale it to 100% as given below

(a) (b)

Figure 14 (a) Scaled to 50% of its original size (b) Rescaled back to 100%

The extracted watermark after this attack is given below:

Figure 15 Extracted Watermark after Scaling and Rescaling Attack

## 6.4 JPEG COMPRESSION DISTORTION

In this experimental analysis, I have compressed the watermarked image by using JPEG Compression and the same is given below:

Figure 16 Watermarked Image after JPEG Compression

The extracted watermark after this attack is given below:

Figure 17 Extracted Watermark after JPEG Compression

## 6.5 ROTATION, BACK-ROTATION, CROPPING AND RESCALING

In this experimental analysis, first I have rotated the image and then back rotate it by giving negative rotation, after that I crop the image part and then rescale it to 100%.

The output at various stages is given below:

Figure 18 Rotated Watermarked Image by -5 degrees

Figure 19 Rotated Watermarked Image by 5 degrees

The extracted watermark after this attack is given below:

Figure 19 Extracted Watermark After Rotation, Back-Rotation, Cropping and Rescaling

## 6.6 NOISE ATTACKS

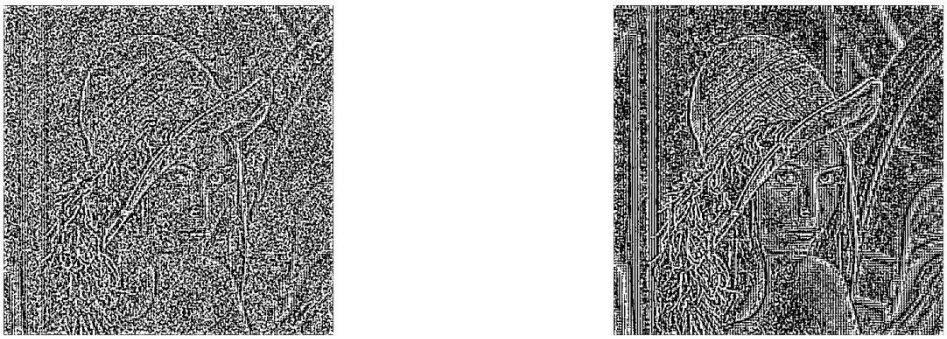
In this experimental analysis, I attacked the watermarked image by Gaussian noise and Salt n Pepper noise and the output at various stages is given below:

(a)

(b)

Figure 20 (a) Watermarked Image after applying Gaussian Noise (VAR = 0.01) (b) Watermarked Image after applying Salt n Pepper Noise (Noise Density = 0.1)

The extracted watermarks after this attack are given below:



(a) (b)

Figure 21 (a) Extracted Watermark after Gaussian Noise (VAR = 0.01) (b) Extracted Watermark after Salt n Pepper Noise (Noise Density = 0.1)

## 6.7 LINEAR AND NON LINEAR FILTERING ATTACKS

In this experimental analysis, I passed the watermarked image through low pass filter, high pass filter, median filter and average filter, the output at various stages is given below:

Figure 22 Watermarked Image after passed through Gaussian Low Pass Filter

The extracted watermark after low pass filter attack is given below:

‘

Figure 23 Extracted Watermark from the low pass filtered Watermarked Image

Figure 24 Watermarked Image after passed through High Pass Filter

The extracted watermark after high pass filter attack is given below:

Figure 25 Extracted Watermark from the high pass filtered Watermarked Image

Figure 26 Watermarked Image after passed through Median Filter

The extracted watermark after median filter attack is given below:

Figure 27 Extracted Watermark from the Median filtered Watermarked Image

Figure 28 Watermarked Image after passed through 3×3Average Filter

The extracted watermark after average filter attack is given below:

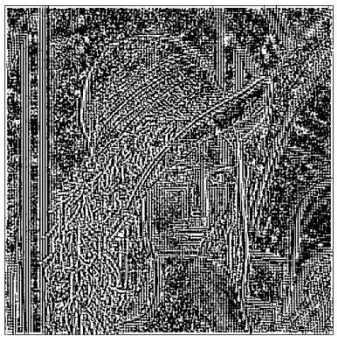


Figure 29 Extracted Watermark from the 3×3 average filtered Watermarked Image

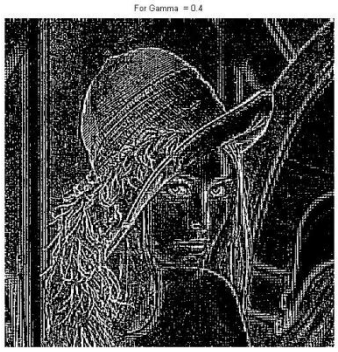
Table 1 shown below represents the performance parameters used for measuring the performance of algorithms for watermarking, the following results are for calculated for $\alpha = 0.6$

| | Energy Efficient Watermarking | | Non- Energy Efficient Watermarking | |
|---|---|---|---|---|
| **Attack** | **PSNR (dB)** | **SSIM** | **PSNR (dB)** | **SSIM** |
| **Image Scaling and Rescaling** | 51.4485 | 0.9002 | 30.3476 | 0.4588 |
| **JPEG Compression** | 38.1299 | 0.8744 | 27.5531 | 0.2375 |
| **Rotation, Back Rotation, Cropping and Rescaling** | 47.3359 | 0.7456 | 25.4331 | 0.2303 |
| **Gaussian Noise** | 37.6513 | 0.6258 | 26.7112 | 0.1836 |
| **Salt N Pepper Noise** | 39.1580 | 0.8977 | 26.7871 | 0.2630 |
| **Low Pass Filter** | 40.8170 | 0.9778 | 29.8120 | 0.2329 |
| **High Pass Filter** | 33.7327 | 0.9213 | 26.3958 | 0.2125 |
| **Median Filter** | 39.6127 | 0.9085 | 27.5461 | 0.2435 |
| **Average Filter** | 37.9942 | 0.8753 | 27.4927 | 0.2572 |

TABLE I Performance Parameters of Watermarking Scheme Against Attacks

## 6.8 WIENER ATTACK

The watermarks extracted from Wiener attack for different values of gamma (γ) are given below:

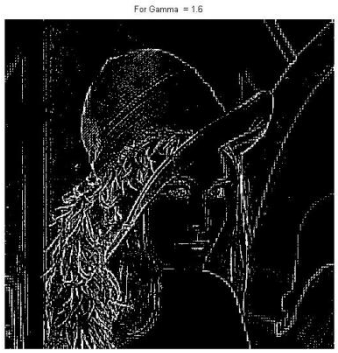
| Gain Factor (γ) | Watermark |
|---|---|
| γ = 0.2 |   |
| γ = 0.4 |   |
| γ = 0.6 |   |
| γ = 0.8 |   |

$\gamma = 1.0$

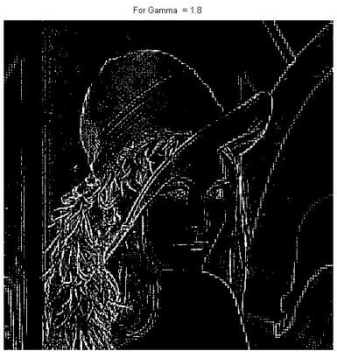

$\gamma = 1.2$


$\gamma = 1.4$


$\gamma = 1.6$



$\gamma = 1.8$




$\gamma = 2.0$

| | Energy Efficient Watermarking | | Non- Energy Efficient Watermarking | |
|---|---|---|---|---|
| **Gain Factor (γ)** | **PSNR (dB)** | **SSIM** | **PSNR (dB)** | **SSIM** |
| γ = 0.2 | 53.1259 | 0.9518 | 26.1683 | 0.2078 |
| γ = 0.4 | 50.1579 | 0.8852 | 25.3759 | 0.1818 |
| γ = 0.6 | 48.7029 | 0.8280 | 24.8888 | 0.1502 |
| γ = 0.8 | 47.7849 | 0.7810 | 24.5480 | 0.1073 |
| γ = 1.0 | 47.1309 | 0.7422 | 24.2575 | 0.0586 |
| γ = 1.2 | 46.6344 | 0.7104 | 24.1642 | 0.0298 |
| γ = 1.4 | 46.2292 | 0.6840 | 24.1629 | 0.0254 |
| γ = 1.6 | 45.8935 | 0.6616 | 24.2154 | 0.0334 |
| γ = 1.8 | 45.6094 | 0.6427 | 24.3268 | 0.0495 |
| γ = 2.0 | 45.3741 | 0.6266 | 24.1150 | 0.0605 |
| γ = 5.0 | 43.8212 | 0.5301 | 24.0654 | 0.00073383 |

TABLE II Performance Parameters of Watermarking Scheme Against Wiener Attack

# CONCLUSION

From the above discussion , I can conclude that energy efficient watermarking scheme is one of the finest scheme as it is robust to Wiener attack, geometric attacks such as rotation, scaling, cropping and rescaling, filtering operations such as low pass filter, high pass filter, median filter and average filter, additive white Gaussian noise, salt n pepper noise. The power spectrum condition makes the watermark robust against Wiener attack.

# FUTURE WORK

In the above discussed project, I have used the energy efficient scheme in order to make a robust watermarking scheme against Wiener attack, filtering operations, geometric attacks. The extraction used is non-blind so it requires original image for the extraction process. One can go for the extraction method in which the original image is not required. In the scheme, we have used discrete wavelet transform; we can also look out for some other transform which has more power to resist attacks such as Wiener, geometric and noise attacks. In this technique, we can also add the encryption key in order to increase the security of the inserted watermark so that only authorized users with the key can only access the watermark.

# REFERENCES


[1] Dr. György Molnár PhD., Dr. Zoltán Szűts PhD., "Advanced mobile communication and media devices and applications in the base of higher education". IEEE 12th International Symposium on Intelligent Systems and Informatics", September 11– 13, 2014, Pp 169-174, Subotica, Serbia.

[2] Pallavi V. Chavan, Dr. Mohammad Atique, Dr. Latesh Malik, "Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography", IEEE Conference on Elecrical, Electronics and Computer Science,2014.

[3] Ingemar J. Cox, *Senior Member, IEEE,* Joe Kilian, F. Thomson Leighton, and Talal Shamoon, *Member, IEEE, "Secure Spread Spectrum Watermarking for Multimedia", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 6, NO. 12, DECEMBER 1997*

[4] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad, "Video Watermarking Techniques for Copyright protection and Content Authentication", International Journal of Computer Information Systems and Industrial Management Applications, ISSN 250-7988 Volume 5 (2013) pp. 652–660.

[5] Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom, "Watermarking applications and their properties".

[6] G. Caronni, "Assuring ownership rights for digital images," in *Proc. Reliable IT Systems, VIS'95*.

[7] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," in *Proc. Infocom'94*, pp. 1278–1287.

[8] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image," in *Proc. 1990 IEEE Military Communications Conf.*, 1990, pp. 216–220.

[9] B. M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting," in *Proc. IEEE*, vol. 83, pp. 944–957, 1995.

[10] G. B. Rhoads, "Indentification/authentication coding method and apparatus," Rep. WIPO WO 95/14289, World Intellect. Property Org., 1995.

[11] G. J. Simmons. The prisoners' problem and the subliminal channel. In *Proc. CRYPTO'83*, pages 51–67. Plenum Press, 1984.

[12] I. J. Cox, S. Roy, and S. L. Hingorani, "Dynamic histogram warping of images pairs for constant image brightness," in *IEEE Int. Conf. Image Processing*, 1995.

[13] Jonathan K. Su, *Member, IEEE,* and Bernd Girod, *Fellow, IEEE,"* Power-Spectrum Condition for Energy-Efficient Watermarking", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 4, NO. 4, DECEMBER 2002

[14] Dipalee Gupta, Siddhartha Choubey, "Discrete Wavelet Transform for Image Processing", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, March 201.5, Pp. 598-602.

[15] Sudip Ghosh, Santi P. Maity, Hafizur Rahaman, "Multiplier-less VLSI architecture of 1-D Hilbert transform pair using Biorthogonal Wavelets for QCM-SS image watermarking", 2013 4th International Conference on Computer and Communication Technology (ICCCT)

[16] HyungJun Kim, C.C. Li, "Lossless and lossy image compression using biorthogonal wavelet transforms with multiplierless operations", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: ANALOG AND DIGITAL SIGNAL PROCESSING, VOL. 45, NO. 8, AUGUST 1998.

[17] Zihao Xiao, Yixuan Zhang, ChiFeng, "A robust and encrypted digital image watermarking method against print-scan".

[18] Li Liu, Xiaoju Li, "Watermarking Protocol for Broadcast Monitoring", 2010 International Conference on E-Business and E-Government.

[19] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish, Member, IEEE, and Orly Yadid- Pecht, Fellow, IEEE, "Hardware Implementation of a Digital Watermarking System for Video Authentication. IEEE transactions on Circuits and Systems for Video Technology", Pp 289-301 Vol. 23, no. 2, February 2013.
[20] Huang-Chi Chen, Yu Wen Chang, Rey-Chue Hwang, "A Watermarking Technique based on the Frequency Domain", Journal of Multimedia, Vol. 7, No.1, February 2012, Pp 82-89.