

**DOKUZ EYLUL UNIVERSITY  
GRADUATE SCHOOL OF NATURAL AND APPLIED  
SCIENCES**

**DIGITAL VIDEO WATERMARKING**

**by  
Kadir ÜNAL**

**August, 2011  
İZMİR**

# **DIGITAL VIDEO WATERMARKING**

**A Thesis Submitted to the  
Graduate School of Natural and Applied Sciences of Dokuz Eylul University  
In Partial Fulfillment of the Requirements for the Degree Master of Science  
in Electrical and Electronics Engineering Program**

**by**

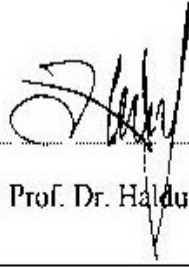
**Kadir ÜNAL**

**August, 2011**

**İZMİR**

## M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled “**DIGITAL VIDEO WATERMARKING**” completed by **KADİR ÜNAL** under supervision of **ASST. PROF. DR. HALDUN SARNEL** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.



Asst. Prof. Dr. Haldun SARNEL

Supervisor



Assoc. Prof. Dr. Olcay AKAY

(Jury Member)



Asst. Prof. Dr. Muhammet G. Cihitli

(Jury Member)



Prof. Dr. Mustafa Sabuncu

Director

Graduate School of Natural and Applied Sciences

## **ACKNOWLEDGEMENTS**

I would like to thank my advisor Asst. Prof. Dr. Haldun SARNEL for his valuable guidance and support.

I also would like to thank my family for their never ending support throughout my life.

Kadir ÜNAL

# DIGITAL VIDEO WATERMARKING

## ABSTRACT

The rapid growth of the digital technologies has introduced copyright protection problem for digital data and digital watermarking methods are proposed to solve it. A digital watermark is a secret message that is embedded to an original digital data with a secret key. The copyright owner proves his/her ownership by extracting the watermark from the digital data in the case of an illegal usage of the digital data. In this thesis, digital video watermarking methods were studied. Two different video watermarking methods, the discrete cosine transform based method and the discrete wavelet transform based method, are implemented. In addition, a hybrid method using both transforms together is developed and proposed in the thesis. The watermark is divided into pieces and each piece is embedded into frames of digital videos using secret keys and developed security algorithms. The performances of the three watermarking methods are compared with each other under several attacks such as frame dropping, frame averaging, noise addition, video compression, image enhancement and median filtering. A video watermarked by the hybrid method gains the power of the diversity of different ways of watermarking. This power grants an efficient and more accurate watermark reconstruction capability from a video undergone an attack from a large group of types. In the thesis, the proposed hybrid method is proved to be superior to the other methods.

**Keywords:** Digital video watermarking, discrete cosine transform (DCT), discrete wavelet transform (DWT), hybrid method, copyright protection

## SAYISAL VİDEO DAMGALAMA

### ÖZ

Hızla gelişen sayısal teknolojiler, sayısal veriler için telif hakkı koruma problemini ortaya çıkarmıştır ve sayısal damgalama yöntemleri bu problemin çözümü olarak önerilmektedir. Sayısal damga, orijinal sayısal verinin içerisine gizli bir şifre ile gömülmüş bir bilgidir. Telif hakkı sahibi, sayısal verinin izinsiz kullanılması durumunda damgayı sayısal veriden çıkartarak onun kendisine ait olduğunu ispatlar. Bu tezde sayısal video damgalama yöntemleri üzerine çalışılmıştır. İki farklı video damgalama yöntemi, ayrık kosinüs dönüşüne dayalı ve ayrık dalgacık dönüşümüne dayalı yöntemler gerçekleştirilmiştir. Buna ek olarak, her iki dönüşümü birlikte kullanan bir hibrit yöntem geliştirilmiştir ve tezde önerilmektedir. Sayısal damga parçalara bölünür ve her bir parça sayısal videonun çerçevelerine gizli şifreler ve geliştirilen güvenlik algoritmaları kullanılarak gömülür. Üç yöntemin çerçeve azaltma, çerçeve ortalamaları alma, gürültü ekleme, video sıkıştırma, görüntü iyileştirme ve medyan filtreleme gibi çeşitli saldırılar altındaki performansları birbiriyle karşılaştırılmaktadır. Hibrit yöntemle damgalanmış bir video farklı yollardan damgalama çeşitliliğinin gücünü kazanır. Bu güç, büyük bir tür grubundan gelen saldırılara uğramış bir videodan verimli ve daha doğru bir sayısal damga çıkartma yeteneğini kazandırır. Tezde, hibrit yöntemin diğer yöntemlere göre üstünlüğü ispatlanmaktadır.

**Anahtar sözcükler:** Sayısal video damgalama, ayrık kosinüs dönüşümü (DCT), ayrık dalgacık dönüşümü (DWT), hibrit yöntem, telif hakkı koruma

## CONTENTS

	<b>Page</b>
M.Sc THESIS EXAMINATION RESULT FORM .....	ii
ACKNOWLEDGEMENTS .....	ii
ABSTRACT .....	iv
ÖZ .....	v
<b>CHAPTER ONE - INTRODUCTION .....</b>	<b>1</b>
1.1 Background .....	1
1.2 Literature Overview .....	2
1.3 Outline .....	5
<b>CHAPTER TWO - DIGITAL VIDEO WATERMARKING.....</b>	<b>6</b>
2.1 Introduction to Digital Video Watermarking.....	6
2.2 General Framework .....	8
2.3 Classification.....	9
2.3.1 Spatial Domain Watermarking .....	10
2.3.2 Frequency Domain Watermarking.....	10
2.4 Requirements.....	11
2.4.1 Robustness .....	11
2.4.2 Imperceptibility.....	12
2.4.3 Security.....	12
2.4.4 Capacity.....	12
2.5 Types of Watermarking .....	13
2.5.1 Private Watermarking .....	13
2.5.2 Semi-Private Watermarking .....	13

2.5.3 Public Watermarking.....	13
2.6 Applications of Watermarking.....	14
2.6.1 Copyright Protection .....	14
2.6.2 Copy Protection .....	14
2.6.3 Content Authentication.....	14
2.6.4 Fingerprinting .....	15
2.6.5 Broadcast Monitoring.....	15
2.7 Attacks .....	15
2.7.1 Simple Attacks.....	16
2.7.2 Detection-Disabled Attacks.....	16
2.7.3 Ambiguity Attacks.....	16
2.7.4 Removal Attacks.....	17
<b>CHAPTER THREE - USE OF TRANSFORMS IN DIGITAL VIDEO WATERMARKING .....</b>	<b>18</b>
3.1 Discrete Cosine Transform .....	18
3.2 Discrete Wavelet Transform .....	22
<b>CHAPTER FOUR - THE PROPOSED HYBRID METHOD with DCT and DWT .....</b>	<b>26</b>
4.1 Introduction of Proposed Method.....	26
4.2 Watermark Embedding.....	28
4.2.1 Discrete Cosine Transform based Method .....	29
4.2.2 Discrete Wavelet Transform based Method .....	31
4.2.3 Hybrid Method based on Discrete Cosine and Wavelet Transforms .....	34
4.3 WatermarkRecovering.....	36
4.3.1 Discrete Cosine Transform based Method .....	37
4.3.2 Discrete Wavelet Transform based Method .....	40



4.3.3 Hybrid Method based on Discrete Cosine and Wavelet Transforms.....	42
<b>CHAPTER FIVE - EXPERIMENTAL RESULTS .....</b>	<b>45</b>
5.1 Details of Tests.....	45
5.2 Tests for Robustness Requirement.....	48
5.2.1 Noise Addition Attacks.....	49
5.2.2 Frame Dropping Attacks.....	52
5.2.3 Frame Averaging Attacks.....	55
5.2.4 Video Compression Attacks.....	57
5.2.5 Median Filtering Attacks.....	60
5.2.6 Image Enhancement Attacks.....	62
5.2.6.1 Intensity Adjustment Attack.....	63
5.2.6.2 Contrast Enhancement Attack.....	65
5.3 Tests for Imperceptibility Requirement.....	67
5.4 Capacity Properties.....	71
<b>CHAPTER SIX - CONCLUSION AND FUTURE WORK.....</b>	<b>73</b>
<b>REFERENCES .....</b>	<b>76</b>

## **CHAPTER ONE**

### **INTRODUCTION**

#### **1.1 Background**

Storing and transmitting digital data have become increasingly available throughout the world. With the rapid growth of the Internet, digital multimedia can be easily distributed via the Internet. Also, this makes the digital video technologies and applications popular in recent years. In many applications digital videos are produced and broadcasted over the Internet. This gives chances to people communicate easier and faster as compared to past years.

Besides the benefits of the development of Internet, it also brings some problems. The digital data are not reliable precisely. The video owners cannot be sure that the video was not manipulated and content is the same with the original one, because the content of the data can be easily manipulated with some tools and software methods. Also, another problem is illegal copying of the digital data. A video can be easily reached by people over the TV or Internet and it can be copied and used for different aims. In this context, the content owners are concerned about illegal copying of their content. The main problem is to protect digital multimedia intellectual copyright.

Digital watermarking is one of the solutions for copyright protection of digital data. As a brief definition, watermarking is the embedding of additional secret data into the original digital data. A digital content can be used as original source and secret watermark data are embedded to that content. Then, this video can be distributed in a medium and may receive some attacks. Ideally, that data must remain present after distribution or some attacks. So, the owner of the original data protects copyright of his/her data even after its transmission or distribution. And also proves his/her ownership by extracting the watermark from the watermarked data.

## 1.2 Literature Overview

As a method of intellectual property protection, many digital watermarking schemes have been proposed in literature for digital images and videos. In general, watermarking methods can be roughly divided into two categories: spatial domain watermark and transformed domain watermark.

A simple and the earliest example of spatial domain methods use the technique that the watermark was embedded to the least significant bit (LSB) of the original image or frame of a video to produce the watermarked image. Schyndel *et al.* (1994) proposed a method in which the watermark is embedded to some proper locations of the original image/frame. The correlation is examined with the original watermark and extracted watermark in the watermark recovering process. This watermarking method was vulnerable to attacks. Bruyndonckx *et al.* (1995) proposed a watermarking scheme based on pixel region classification. Pixels are classified in terms of regions of hard, progressive or noise contrast. Then, watermark is embedded by changing the gray levels of the pixels with a rule according to aforementioned pixel regions.

Wong (1998) presented a watermarking scheme, which embeds a binary watermark into the LSB of each pixel in the image. The original image is divided into blocks and each block is modified by setting the LSB of each pixel in the block to zero. A cryptographic function is computed from the modified block and the width and height of the image. Then, the watermark for each block is determined with bit operations (e.g. exclusive OR operation). After bit operations, the resulting watermark is encrypted and inserted into the LSB of the modified block.

Frequency domain methods consist of a frequency transform and the watermark is embedded by altering the frequency coefficients. Cox *et al.* (1997) proposed a method that 1000 random samples were embedded to the largest DCT coefficients of the image/frame. In the extraction process, if the correlation between the original image/frame and the watermarked frequency coefficients was higher than a threshold value, the watermark is recovered.

A Discrete Wavelet Transform (DWT) based watermarking method was also proposed (Xia, Boncelet, and Arce, 1997). The watermark was modeled as noise signal and was added to the middle and high frequency bands of the image/frame. Recovering watermark is based on correlation between original image/frame and the extracted watermark.

Bartolini *et al.* (1998) first generated a watermarked image from DCT coefficients. Embedding process is based on spatial masking. Kundur *et al.* (1997) embedded the watermark in the wavelet domain. These techniques are more robust as compared to spatial domain methods.

Delaigle *et al.* (1998) proposed a unique watermarking scheme based on the human visual system. Binary m-sequences were generated and then modulated on a random carrier. This image is used as the watermark, and then masking was applied in terms of contrast between the original image/frame and the modulated image/frame. The masked watermark was added to the original image/frame to form the watermarked image/frame.

Ruanaidh *et al.* (1997) and Ruanaidh *et al.* (1998) proposed a method in which embedding is based on Fourier-Mellin transform. This transformation is equivalent to mapping the Fourier spectrum of an image into a Log-Polar coordinate system and taking again a Fourier transform of the result. The advantage of the method is that the watermarked image is resistant to rotation, translation and scaling. However, the disadvantage of this method is that the quality of the original image/frame is degraded because of the transformation used.

In recent years, the researchers start to work on a more challenging watermarking method called *digital video watermarking*. Most of the proposed digital video watermarking techniques are based on the techniques of digital image watermarking. However, digital video watermarking introduces some issues which are not present in image watermarking. Due to large amounts of data and inherent redundancy between frames, video signals are highly susceptible to pirate attacks (J.Lee and S.H.Jung, 2001). So, researchers proposed more complex and complicated methods which contain more parameters which are not present in image watermarking.

A real-time watermarking method based on a single bit (Busch et al, 1999) is encoded in an image block in the discrete cosine transform (DCT) domain by exchanging a selected sub-band of the DCT coefficients of that block so that the relationship amongst the coefficients comprising that sub-band encodes the bit.

Hartung and Girod (1999) describe a method of watermarking into both compressed and uncompressed MPEG-2 videos based on spread spectrum methods. For compressed domain watermarking, they decode the video to obtain the DCT coefficients of each frame and insert the watermark by modifying those DCT coefficients.

Langelaar and Lagendijk (2001) proposed a compressed domain watermarking method called Differential Energy Watermark (DEW). In this method the video is divided into groups of blocks and each of the blocks is further divided into two groups, and the size of the groups is determined by the watermark embedding key. By comparing the energy of selected DCT coefficients within the groups, a single watermark bit is expressed.

Chetan and Raghavendra (2010) proposed a robust Discrete Wavelet Transform (DWT)-based blind digital video watermarking scheme with scrambled watermarks based on scene changes. It has been proposed for authentication of digital video, which embeds different parts of a single watermark into different scenes of a video. The algorithm is robust against the attacks of frame dropping, averaging and compression and has been compared with an existing DWT based watermarking scheme and is found to exhibit better robustness.

A hybrid scene-based video watermarking scheme with error correcting code and genetic algorithm is proposed by Chan (2004). The watermark is divided into different parts and embedded in the frames of different scenes in the video with hybrid approaches. At the same time, error correcting code is extracted from the video channel and embedded into the audio channel.

In this thesis, three different digital video watermarking methods are implemented and their performances are tested for comparison. The first method is a DCT based

method, the second one is a DWT based method, and the third one is a combined method. The hybrid method developed and proposed in this thesis uses one of the three methods to embed watermark into a frame: the DCT based method, the DWT based method, and the combined method. The combined method uses the DCT for the upper half of a frame and the DWT for the lower half. The selection of the watermarking method for the current frame is made randomly. Therefore the same watermark data are embedded to many different frames in video using each of the three methods. The watermark is divided to sub pieces and these pieces are embedded to frames. For the DCT based method, the selection of blocks into which watermark bits are to be embedded is done with an algorithm controlled by a secret key. In DWT based method, the detail bands which are used for watermarking is selected by the user. Some secret keys are used for generating pseudo random number sequences that represents watermark bits in embedding and recovering stages for all three methods. They make the proposed method more secure. Also, after recovering stage, data fusion algorithm is developed and a final recovered watermark data is obtained with an algorithm. The performances of the three watermarking methods are compared with each other under several attacks. Frame dropping, frame averaging, noise addition, video compression, image enhancement and median filtering attacks are performed on the watermarked video. The proposed hybrid method is proved to be superior to the other methods.

### **1.3 Outline**

This thesis is presented in six chapters. Chapter 1 presents introduction. Chapter 2 provides a general framework of digital video watermarking. Chapter 3 addresses background concepts on the use of transforms in digital video watermarking. Chapter 4 presents the proposed hybrid method based on DCT and DWT. Chapter 5 presents and discusses the experimental results obtained during computer simulations using the method implemented. Chapter 6 finishes this thesis by conclusions and suggestions for future work.

## CHAPTER TWO

### DIGITAL VIDEO WATERMARKING

#### 2.1 Introduction to Digital Video Watermarking

In recent years, the digital video is becoming popular more than ever due to the spreading of video-based applications such as broadcasting on the Internet. This naturally causes unauthorized copying and distribution of digital videos.

Researchers proposed many methods on preventing illegal and malicious copying and distribution of digital images and these methods are called digital image watermarking. In recent years, digital image watermarking methods have matured and with developing of digital video technologies, researchers have started to work on copyright protection issue of video contents. This resulted in development of methods called *digital video watermarking*.

Digital video watermarking methods are actually based on digital image watermarking methods. The transforms and techniques are nearly the same, but video watermarking techniques have to face many challenges which are not present for image watermarking. The main challenges are large volume of inherently redundant data between frames, the unbalance between the motion and motionless regions, real-time requirements in the video broadcasting (T.Jayamalar and V.Radha(2010).

Digital videos are much susceptible to some attacks such as frame dropping, frame averaging, and statistical analysis. Digital video watermarking methods must be robust to these attacks, so these methods must have more computational complexity than digital image watermarking methods. As a straightforward simple method each frame can be watermarked with same data but the watermark data can be detected with statistical analysis and the visual quality is distorted in this case. As a different method, independent watermark data can be embedded to frames. But frame

averaging attack causes distortion especially in motionless frame intervals of the video. Also, watermark data may be lost after frame dropping attacks, some pieces of the watermark data may be totally impossible to recover. So, the methods proposed must take into account all these issues.

Many digital video watermarking methods have been proposed in the literature. The methods can be grouped as compressed and uncompressed domain watermarking methods. For uncompressed domain methods, the watermark data are embedded into the raw uncompressed video. Watermark data are considered as narrow band signal and video is considered as wide band signal. Narrow band signal is spread for increasing redundancy and then modulated with binary pseudo noise sequence. The reason for adding pseudo-noise is to prevent detection and attack of the watermark data. In the recovering stage, by using the same pseudo-random signal in the embedding stage, watermark data can be detected and recovered. For compressed domain methods, watermark data is embedded to compressed videos. H.261, H.263, MPEG-2, and MPEG-4 compression methods are generally used for video compression. Watermarking for compressed video data in real time is very challenging because of computation requirements. So, compressed domain methods are more complex than uncompressed domain methods.

Video watermarking methods can also be classified in two main groups based on domain that the watermark is embedded. These methods are; spatial domain and frequency domain methods. Spatial domain methods are based on modification of pixels values in embedding stage of the watermarking. There is no transform applied to original content. So, these methods are very simple and have low computational cost. This feature is important for real-time operations and spatial domain methods are preferred for these operations. The most common method is LSB modification method. The LSB is modified for embedding the watermark data. This method is very simple and the visual quality of the watermarked video is almost same with the original video. But, these methods are vulnerable to attacks and watermark data can be easily distorted. The other common method is based on correlation-based methods. A pseudo random sequence is added to original content in the embedding



stage and the same sequence is also used in recovering stage. By comparing the pseudo random sequence and watermark data, the watermark can be detected and recovered. This method can be improved by using strength constant.

Frequency domain methods are based on modification of frequency coefficients. The original content is transformed to frequency domain and coefficients in frequency domain are used for embedding and recovering the watermark data. The most common transforms are the discrete cosine transform, the discrete wavelet transform and discrete Fourier transform. The frequency domain methods are more robust and have more computational complexity. These methods can be used separately or some of them can be used together. Some hybrid methods take advantages of these individual methods by joining them into one.

## **2.2 General Framework**

Digital watermarking can be summarized as shown in Figure (2.1). The secret data, watermark, is embedded to original digital data with a secret key. This secret key is only known by the content owner. It is impossible to recover the embedded secret data without knowing the secret key. After embedding the watermark data to original video, this video is distributed over Internet or passed through in any transmission channel. After that, there may be some attacks on the watermarked data. These attacks may damage the watermark. In the recovering stage, the watermarked data and the secret key are used for extracting the secret data from the video as shown in Figure 2.2. If the watermark data is recovered, the content owner can prove his/her ownership of the video. Thus, digital watermarking protects an owner's intellectual property rights of digital content.

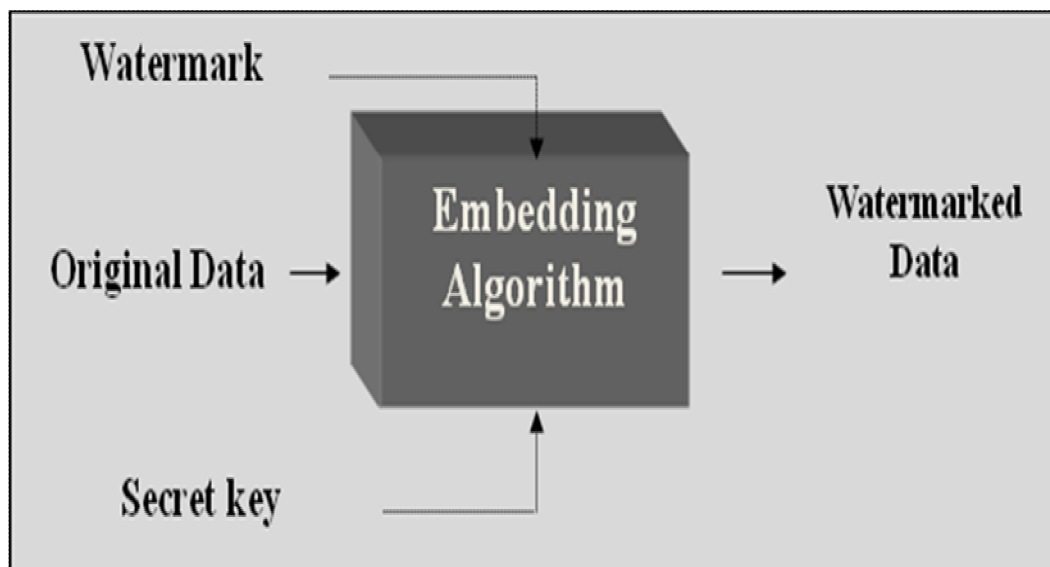


Figure 2.1 General framework of watermarking algorithm

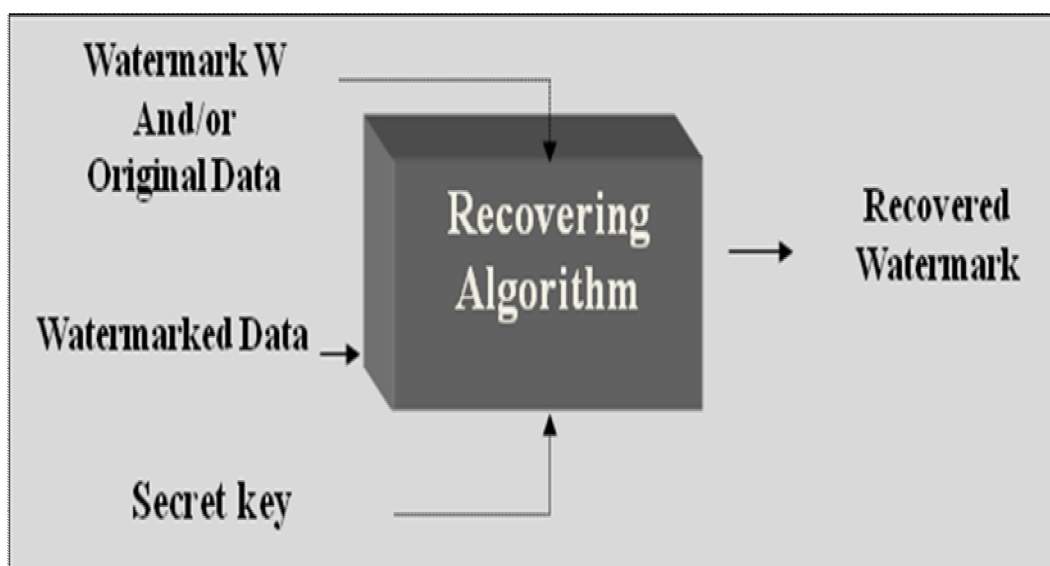


Figure 2.2 General framework of watermark detection algorithm

### 2.3 Classification

Watermarking methods can be examined in two main classes. One of them is spatial domain watermarking methods. There is no transformation for these methods and pixels' values are modified directly for watermarking. The other class is

transform domain watermarking methods. The original content is transformed to a frequency domain and the frequency coefficients are modified for watermarking.

### ***2.3.1 Spatial Domain Watermarking***

For spatial domain methods, watermarking is performed by modifying values of pixels of video frame or image. There is no transformation applied to original content. The most common algorithm using spatial domain watermarking is LSB modification. This method is the easiest method because of its simplicity. The human eyes are not very attuned to small variance in color and therefore processing of small difference in the LSB will not be noticeable. Also, a surprising amount of information can be hidden with little perceptible impact on the original content.

Although LSB modification method is simple to apply, it consists of some drawbacks. Although it may survive transformations such as cropping, the watermark can be easily distorted by addition of noise or lossy compression. As a simple attack, setting all LSB of each pixel to 1 also distorts the watermark with negligible impact on the original object. As a summary, although the method is simple and imperceptibility of the watermark is almost perfect, robustness of this method is not enough and watermark is vulnerable to attacks.

### ***2.3.2 Frequency Domain Watermarking***

The essence of these methods is similar with spatial domain watermarking; values of the transformed coefficients are modified to embed watermark data. The original content is transformed with a frequency domain method and frequency domain coefficients are obtained. Then, some algorithms are applied on the coefficients and watermark data are embedded in the original content. Mostly, since high frequencies will be lost by compression or scaling, the watermark data is applied to lower or medium frequencies, or adaptively applied to frequencies consisting of important elements of the original image.

The most common transforms are the DCT and DWT. In DCT methods, the image/frame is broken up into different frequency bands and the lower or medium band frequency coefficients are modified to embed watermark data. The low or medium frequency bands are chosen for embedding watermark data because modification on these bands is less distorting and more robust. Also, the method is more immune to compression and noise attacks. In DWT methods, the original content is divided into sub pieces. These pieces are lower resolution approximation image, horizontal, vertical and diagonal frequency components. The process can then be repeated to compute multiple “scale” wavelet decomposition. The DWT based methods more accurately model aspects of the human visual system as compared to the DCT based methods. The watermark data are embedded to less sensitive regions and imperceptibility of the watermark data are relatively high. Also, the robustness of these methods is satisfactory.

## **2.4 Requirements**

Digital watermarks can be classified and compared on the basis of certain characteristics and properties. In general, they are described as robustness, capacity, imperceptibility, security, and other restrictions. The main characteristics of the watermark method can be classified according to following requirements (Kutter and Hartung, 2000).

### **2.4.1 Robustness**

Robustness means resistance to common operations applied in the imaging, motion picture, or audio field (Fridrich, 1998). After some distortions and malicious attacks, the watermark should be recoverable even after such distortions occurred. The ideal watermark must also be highly robust, entirely resistant to distortions. But there is no ideal watermarking method which is entirely resistant. The robustness of a watermarking scheme can vary from one operation to another. Each of the watermarking methods has robustness and weakness to the attacks. A method can be robust to any signal compression methods, but the watermark may be vulnerable to

geometric distortions (Y. Meng and E. Chang , 2003). The requirements change from application to application, for example; if the watermarking method is robust to image compression, the watermark data are embedded to the perceptually significant parts of the original digital data so robustness against signal distortion is better achieved. This depends on the behavior of lossy compression algorithms, which operate by discarding perceptually insignificant data not to affect the quality of the compressed image, audio or video.

#### ***2.4.2 Imperceptibility***

The imperceptibility means perceptual similarity between the original and watermarked data. The perceptual characteristic of the original data should not to be changed after watermark data are embedded. The imperceptibility is tested by some test which is based on human visual system. Since the human beings can't distinguish watermarked data from the original, the tests are subjective and they are all classified as imperceptible.

#### ***2.4.3 Security***

The security means that the watermark cannot be reachable even if the attacker has all the information about the watermarking method. The secret key should keep the watermark as a secret. The complexity is also related with the security, that is, the algorithm for recovering watermark should work with secret and safe key to discourage the attackers.

#### ***2.4.4 Capacity***

Capacity refers to the amount of watermark information that can be stored in a data. This can range from a single bit up to multiple paragraphs of text. A decision has to be made for the right application because there is a tradeoff between capacity, robustness and imperceptibility requirements and this trade off should be taken into account while the watermarking method is being proposed. If the robustness is the

most important characteristic of the method, capacity should be relatively higher but in this case the imperceptibility decreases. Vice versa, if the imperceptibility is more important, the information should be low, so the capacity gets lower.

## **2.5 Types of Watermarking**

Digital watermarks can be grouped as three different types. Their difference is based on the combination of inputs and outputs in the recovering stage for a watermarking scheme (Hartung and Girod, 1999).

### **2.5.1 *Private Watermarking***

This watermarking method is also called non-blind watermarking. At least the original image is required in the recovering stage. This type of watermarking methods is used for applications for which the main question is that if the original data are watermarked or not. This watermarking type is more robust than the other types since, little information is embedded in the original data.

### **2.5.2 *Semi-Private Watermarking***

This watermarking method is also called semi-blind watermarking. In contrast to private watermarking, the original data are not required in the recovering stage. The main aim is the same as the private watermarking. Digital data are examined if there is watermark data or not. This scheme is preferred for copyright protection applications.

### **2.5.3 *Public Watermarking***

This watermarking method is also called blind watermarking. The original data and the watermark data are not required in the recovering stage. Solely the key, which is typically used to generate some random sequence used during the embedding process, is required. These types of schemes can be used easily in mass market electronic equipment or software.

## **2.6 Applications of Watermarking**

The main aim of the digital watermarking is copyright protection. But, there are more application areas of the watermarking and the purpose of the watermarking is also different from application to application, so the requirements of these methods also change. The main application areas are copyright protection, copy protection, content authentication, fingerprinting, and broadcast monitoring.

### ***2.6.1 Copyright Protection***

The most prevailing applications of digital watermarking are for copyright protection. The objective of this application is to embed a watermark in a digital data to prove the ownership of that data. Many digital data are freely shared on the Internet and so the rightful owners want to protect their intellectual property. For this application, the most important requirement of the watermarking method is robustness. The watermark must be robust to attacks and can be detectable when the content owner wants to extract the watermark data to prove his/her copyright.

### ***2.6.2 Copy Protection***

The aim of these applications is to disallow unauthorized copying of the digital data. The watermark data indicates the copy status of the digital data. If the watermark has the never copying information, the compliant systems disallow copying of the digital data. DVD systems and digital music distribution services can use this type of watermarking applications. Recording device may inhibit recording a signal if detected watermark indicates that it is prohibited.

### ***2.6.3 Content Authentication***

In authentication applications, the objective is to detect if the original digital data has been altered. The watermark data are generally fragile and the robustness

requirement is asked to be lower than the other applications. Since a simple attack can distort the digital data easily, the content owner can understand whether the original data is changed or not. As a different approach for this type of applications, a specific attribute can be embedded and in recovering stage, content owner can check the data if they still contain the same attribute or not.

#### **2.6.4 Fingerprinting**

These applications deal with taking each copy of your content and making it unique to the person who receives it. This way, if the work is shared, you know exactly which person spread the work initially. The aim of these applications is to identify the source of an illegal copy; this can be achieved by embedding unique watermark in each copy. Watermarks also require a high robustness against attacks for these applications.

#### **2.6.5 Broadcast Monitoring**

Watermarking is an innovative technology for broadcasters. A broadcaster can use this application type of watermarking by embedding a digital watermark in audio or video content at the time of production or broadcast. It allows content owners, for example, to identify with granular precision when and where content is broadcast, who is broadcasting and for how long.

The imperceptibility of watermarks is an important requirement for these applications. The modifications are indiscernible to human senses, but watermark can easily be detected and recovered.

### **2.7 Attacks**

There are many possible types of exposed to the watermarked data. The aims of these attacks are different from each other. Some attacks are applied to detect watermark data, but the aim of some attacks is not to detect watermark data, just



distortion of the signal and make recovering watermark process impossible. The watermarked data are undergone some attacks and these attacks can be classified into four main groups as follows.

### ***2.7.1 Simple Attacks***

These attacks are based on distortion of the whole digital data. Watermark data are not specifically known, the whole data are damaged and detection of watermark data may fail in recovering stage. Noise addition, cropping, compression attacks are more common attacks in this category.

### ***2.7.2 Detection-Disabled Attacks***

The main goal of these attacks is to remove or destroy the watermark. The distorted watermark may be impossible to detect in recovering process after these attacks. The most common attacks are shifting, rotating, cropping of the original data, pixel operations (e.g. removing, insertion) for this category. The distorted watermark data can be recovered with increased intelligence and complexity of the watermark detection algorithms. These attacks may be used for copyright protection, copy protection and fingerprinting applications.

### ***2.7.3 Ambiguity Attacks***

These attacks are based on confusing the recovering of the watermark; this is achieved by producing fake watermarked data and embedding them in the original data or the attacker can embed a valid authentication watermark to discredit the authority of the watermark. There may be more valid watermark data in the original data and it cannot be known which watermark is the first, authoritative watermark.

#### ***2.7.4 Removal Attacks***

The aim of these attacks is to find the watermark data, remove it and construct a copy with no watermark data. This can be achieved by using several watermarked data and then estimation is done. The positions of the watermark may be estimated and watermark may be removed easily. These attacks cause big problems for fingerprinting applications.

## CHAPTER THREE

### USE OF TRANSFORMS IN DIGITAL VIDEO WATERMARKING

#### 3.1 Discrete Cosine Transform

DCT is the most common frequency transform for digital image processing, digital video processing and signal processing. It transforms a signal from spatial domain to frequency domain. The main advantages of DCT are that small bit error rate, high compression ratio, good information integration ability and good synthetic effect of calculation complexity. Also, due to good performance, DCT is the base of several standards of multimedia video frequency compression (H. 261, H. 263 and MPEG, etc.).

The DCT equation can be expressed as in Equation (3.1)

$$D(i, j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x, y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right]$$
$$C(u) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } u = 0 \\ 1 & \text{if } u > 0 \end{cases} \quad 3.1$$

$p(x,y)$  is the value of element  $(x,y)$  of the image represented by the matrix  $p$ .  $N$  is the size of the block that the DCT is done on. The equation calculates one entry  $(i,j)$  of the transformed image from the pixel values of the original image matrix. Because the DCT uses cosine functions, the resulting matrix depends on the horizontal, diagonal and vertical frequencies. Therefore an image with a lot of sharp intensity changes has a very random looking resulting matrix, while an image of a single intensity, has a resulting matrix with a large value for the first element (DC component) and zeroes for the other elements.

DCT is also very popular transform domain watermarking technique. The DCT divides the original data into different frequency bands which are the high, middle and low frequency bands. Then, the content owner makes his/her choice that which band will be used for watermark embedding. In the literature, the most common used band is the middle frequency band. If watermark is embedded to high frequency band, it will be removed after compression and noise attacks. The most visually important region of the digital data is the low frequency band. The low frequency band determines the visual details of the digital data. The human eyes are more sensitive to noise in lower-frequency band. The energy of natural image is concentrated in the lower frequency range. So, if the watermark is embedded to this band, the visual quality of the digital data is distorted and imperceptibility requirement of watermarking cannot be afforded.

Numerous watermarking techniques based on DCT are proposed. Although some of the watermarking techniques embed the watermark in the DC component, i.e the lowest frequency component, most techniques utilize the comparison of middle band DCT coefficients to embed a single bit of watermark information into a DCT block. The frequency bands are shown in Figure 3.1. The left-top coefficient is the DC value while the others stand for AC components. And middle-band frequencies ( $F_M$ ) of an  $8 \times 8$  DCT block is highlighted.

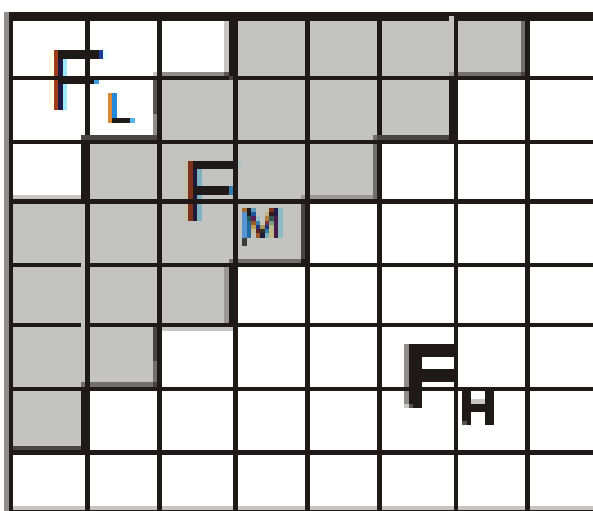


Figure 3.1 Definitions of DCT regions

As can be seen from the figure above, a DCT block consists of three frequency bands. The left-top region is called  $F_L$  and contains the lowest frequency components. The right-bottom region is called as  $F_H$  and denotes the highest frequency components of the DCT block. The center region of the block is the medium frequency band and is called as  $F_M$ .

As mentioned before,  $F_M$  is the middle frequency band and is chosen for embedding copyright data. This prevents to distort the visual quality of the watermarked data because of not choosing the low frequencies and with this selection watermarking is more resistant to lossy compression by avoiding using of high frequency bands.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Figure 3.2 Quantization values used in JPEG compression

There are two main watermarking methods that use middle band frequencies. The first one is to swap two specific coefficients in the middle band and the second is to add a pseudo random sequence in the middle frequency band of the image/frame. The first method is based on swapping the mid frequency band coefficients. Two locations are chosen from the middle frequency band as the region for comparison. During JPEG compression DCT coefficients in a block are divided by a set of quantization values shown in Figure 3.2. The two coefficients which have same

quantization values are chosen for embedding one watermark bit of information. As can be seen from the table the coefficients at (1,2) and (3,0) or (4,1) and (3,2) have same quantization values and can be used for comparison. The key point of this method is to swap or not change the coefficients based on the watermark data. If the watermark datum is '0', the one of the coefficients must be lower than the other one. If so, there is no operation on DCT block, otherwise the coefficients are swapped to provide that the first coefficient is lower than the second one. As the same logic before, if the watermark datum is '1', the first coefficient must be higher than the second one. If so, there is no operation on DCT block, otherwise the coefficients are swapped to provide that the first coefficient has higher value than the second one. The swapping of the coefficients does not make significant differences on the original data. Because, the middle band coefficients have similar magnitudes. By using this method, the watermark data can be detected in the recovering stage by comparing the values of the coefficients. But, attacks can change the values of the coefficients and the relation between the coefficients may be damaged. To avoid this situation, and improve the robustness of the method, "strength constant" is added to coefficient which has the higher value after swapping the coefficients. This makes the method more immune to noise attacks and detection errors are reduced. The "strength constant" parameter must be chosen carefully. Increasing this value reduces the image/frame quality but increases the robustness of the method.

The second watermarking method is based on adding a pseudo random sequence in the middle frequency band of the image/frame. To improve the robustness of the method, "strength constant" is added to the coefficients. The higher "strength constant" causes the lower image/frame quality. So, imperceptibility and image/frame quality must be considered and "strength constant" has to be determined. The watermark embedding equation of CDMA (code division multiple access) watermark into DCT middle frequencies is shown in Equation (3.2).

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) + kW_{x,y}(u,v), & u,v \in F_m \\ I_{x,y}(u,v), & u,v \notin F_m \end{cases} \quad 3.2$$

As can be seen from Equation (3.2), for each DCT block, the middle frequency band coefficients are added to the pseudo random sequence  $W$ , multiplied by “strength constant”. The low and high frequency bands are not changed. Then, inverse DCT is applied and watermarked data are ready to use. This method can be modified by slightly changing the embedding process. Its expression is given in Equation (3.3).

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) (1 + kW_{x,y}(u,v)), & u,v \in F_m \\ I_{x,y}(u,v), & u,v \notin F_m \end{cases} \quad 3.3$$

This modified method adjusts the robustness of the watermarking based on the value of the coefficients being used. This slight modification scales the strength of the watermarking based on the size of the particular coefficients being used.

For detection of the watermark in these methods, the image/frame is divided into  $8 \times 8$  blocks, and the DCT is applied to the blocks. The same pseudo random sequence is then compared to the middle frequency values of the transformed block. If the correlation between the sequences exceeds some threshold, a “1” is detected for that block; otherwise a “0” is detected.

In this thesis, the method of adding pseudo random sequence is used for DCT based watermarking. The data are transformed and middle frequency band coefficients are modified by adding a pseudo random sequence after multiplying with strength constant. The low and high frequency bands remain the same and there is no operation on these bands.

### 3.2 Discrete Wavelet Transform

The DWT is one of the most common frequency transforms for digital image processing, digital video processing and signal processing. It transforms a spatial-domain digital data to frequency domain. The most important advantage of the

methods which use the DWT is being the best model in accordance with human visual system as compared to other frequency domain transforms.

The basic idea of the DWT is to decompose an image/frame into a sub-image of different spatial domain and independent frequency districts. Original image/frame is separated into a lower resolution approximation region, horizontal, vertical and diagonal frequency bands. The low frequency band is utilized in the next level of the DWT. That is, the decomposition continues with lower resolution approximation region in the same manner. In the DWT, the most important information has high amplitudes and the less important information has low amplitudes. Thus, data compression can be achieved by discarding these low amplitudes.

If the information of lower resolution approximation region is decomposed by DWT, the sub-level frequency regions will be obtained. A two-dimensional image after two-times the DWT decompositions is illustrated in Figure 3.3. An original image can be decomposed into frequency regions of LL1, HL1, LH1, HH1. The low-frequency region LL1 can be further decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this, the original image can be decomposed for  $n$  level wavelet transformation.

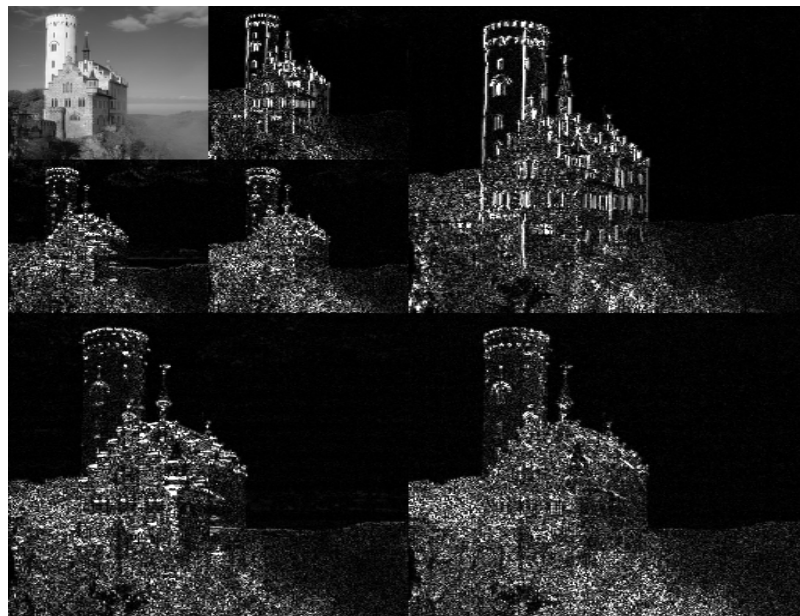


Figure 3.3 Two-level discrete wavelet transform



The lower resolution approximation region of an image/frame consists of the most important information of original image/frame. The frequency regions of LH, HL and HH respectively represent the horizontal, vertical and diagonal details of the original image.

There are many advantages of the DWT. These can be listed as follows:

- Watermarking in the wavelet domain is compatible with the JPEG 2000 compression standard.
- The DWT helps the content owner to localize the features to which the human eye is more sensitive. When a DWT is applied to a digital data, the edges and textures are represented by large coefficients in high frequency sub-bands: the human eye is less sensitive to modifications of these coefficients.
- The capability to localize information in time and frequency: in the case of 2-D intensity images the time domain is the spatial location of pixels and the frequency domain is the intensity variation around a pixel. The wavelet functions have a compact support and are local both in frequency and in time. This localization makes a watermark scheme based on wavelets more robust.
- The DWT requires a lower computational complexity than the Fourier or the cosine transform.

The magnitudes of the DWT coefficients are larger in the lowest bands (LL) at each level of decomposition. Embedding the watermark in the higher level sub bands increases the robustness of the watermark. However, the image visual fidelity may be lost. Similar to DCT based methods, adding a pseudo random sequence to the coefficients is the most common way in the DWT based methods. Watermark is generally embedded to the vertical and horizontal frequency bands by adding a unique pseudo random sequence for each watermark bit. In the recovering stage, the same pseudo random sequence is compared with watermarked data and if the correlation exceeds a threshold value, this single bit of watermark is recovered successfully. Before adding the pseudo random sequence to original content, “strength constant” is used, so robustness of the method is improved. The robustness

and imperceptibility requirements are examined and optimum “strength constant” can be determined.

In this thesis, adding a pseudo random sequence method is used for DWT based method. The data are transformed, then vertical or/and horizontal frequency coefficients are chosen for embedding a piece of watermark data. Then, coefficients of the entire selected band are modified by adding a unique pseudo random sequence for each watermark bit after multiplying with strength constant. Each pseudo number sequence is multiplied with strength constant and added to these frequency bands cumulatively. The lower resolution approximation region (LL) and diagonal details region (HH) remains the same and there is no operation on these bands. The robustness and imperceptibility are optimized by not modifying these bands and choosing the strength constant as optimal.

## CHAPTER FOUR

### THE PROPOSED HYBRID METHOD with DCT and DWT

In the literature, there is no watermarking method which is capable of resisting to all watermark attacks. So, hybrid methods have been used in literature recently. The aim of these methods is to take the advantages of the different transforms and making the method more robust. Of course, hybrid methods cannot resist all attacks. Different embedding and recovering algorithms are used to prevent the watermark data from being detected and distorted.

In this chapter, the proposed hybrid method is explained in detail. The selection of hybrid method is done because of its advantages. The visual detection of the watermark is harder for hybrid methods and it is more difficult to detect watermark data statistically. Also, we use frequency domain transformations because of their advantages mentioned before. DCT and DWT are used together in this method. So, this method takes advantages of each method. In other words, each method resists some specific attacks successfully and combining these methods provides more robustness against attacks. This hybrid method consists of some keys which are used in embedding and recovering stage. These keys provide more security and recovering watermark data is not possible without knowing these secret keys. The proposed method also provides flexibilities to content owner about choosing the piece number, frequency bands and pixel blocks. In the following sections, the details of the method are explained.

#### 4.1 Introduction of Proposed Method

In this thesis, the method proposed is based on hybrid watermarking approaches. DCT based and DWT based methods are used together. Besides this combination, some security algorithms are applied in embedding and recovering stages. Instead of embedding whole watermark data to all frames, watermark data is decomposed into small pieces and embedded to frames piece by piece. In embedding algorithm, it is

decided to which watermark piece is embedded to which frame. A different secret key is used to decide for this. This key is also known by content owner. This process does not only increase the security of the watermark detection but also improves the imperceptibility requirement of watermarking by embedding less data to each frame.

In addition to the watermark data decomposition, some smart algorithms are used both in DCT based and DWT based watermarking stages. These algorithms make the watermark data more robust and the watermark data can only be recovered by knowing the details of these algorithms and secret keys used in the method.

An overview of the hybrid method is shown in Figure 4.1. In this framework, a digital video and a digital black and white watermark image are taken as the input, and the watermark data are then decomposed into pieces. In embedding stage, a watermark piece and an embedding algorithm are chosen and frames are processed with the chosen transform method. A frame can be processed by DCT or DWT, or both. The random generator is seeded by a key which is only known by the content owner. The sequence of the selections is related with the key. So, content owner only knows which transform method is used. After seeding with a key, the algorithm selects the method and watermark pieces for each frame randomly.

Each frame contains one of the watermark pieces and again only the content owner knows which piece it is. Selection of the embedding algorithm is made using the secret keys and in recovering stage, the same keys are needed to detect the embedded watermark piece. The watermark data are embedded to all color bands of each frame, thus it can be recovered from other color bands if one of the color bands is undergone attacks. This provides us with backup mechanism for the watermark data.

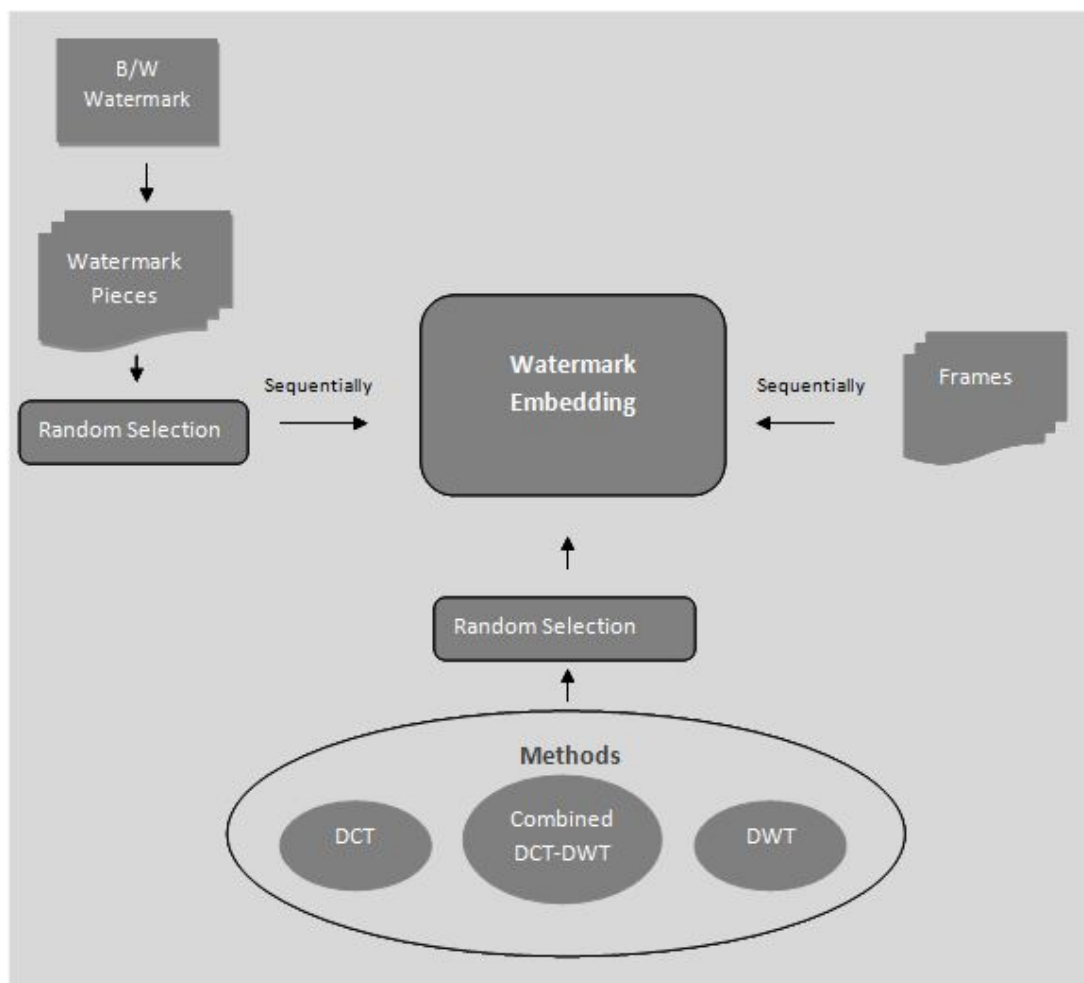


Figure 4.1 Overview of the hybrid method

## 4.2 Watermark Embedding

In watermark embedding stage, firstly, watermark data are decomposed to pieces. Number of the pieces can be adjusted in the software by considering the sizes of the video and watermark data. Larger number of pieces means better imperceptibility because less data are embedded to each frame in this case. This also makes malicious detection of watermark by statistical analysis on the frames harder because the same watermark data are not embedded to each frame. After decomposing watermark data, it is determined that which piece is to be embedded in the current frame. A random number generator is used for this. The seed of the generator is a secret key making the method more robust and complex.

There are 3 methods to embed a piece of watermark in the current frame: DCT, DWT, and a combination of the both transforms. Similar to that in the watermark decomposition stage, a different key is used as seed for a random number generator that makes the decision for the transform method to be used. There is also a block selection algorithm for DCT method and band selection flexibility for DWT. These two make the method more secure and their details are presented in the following sections.

#### ***4.2.1 Discrete Cosine Transform based Method***

If the current frame is to be processed with the DCT, the frame is divided into 8x8 blocks. Then, the block is transformed into frequency domain using the DCT. The middle-band frequency coefficients are determined for watermark embedding. In a 8x8 block, there are 22 middle band coefficients and these coefficients are used for watermarking. Low frequency band and high frequency band coefficients are not changed during watermark embedding. The low frequency coefficients are not used because this band involves the most visually important parts of the frame. Also, the high frequency coefficients are not used because this band can be removed through compression and noise attacks.

After the 8x8 blocks are determined, an algorithm is used to determine which blocks will contain the watermark data. The algorithm takes watermark size and frame size as inputs and gives out an array of blocks in which watermark data are to be embedded. In other words, only a subset of blocks in the current frame is chosen randomly using a secret key for watermark embedding. This secret key determines both the locations and order of the blocks in the array. In recovering stage, the same algorithm is used to determine these blocks that contain the watermark data. It is not possible to recover the watermark data without knowing the algorithm and the secret key.

Embedding is performed based on the method of adding pseudo random sequence. One pseudo random sequence is generated for embedding watermark data bit '0' and

another pseudo random sequence for embedding watermark data bit '1'. Because the watermark data are embedded to middle band coefficients, the length of the pseudo random sequences is equal the middle band coefficients of an 8x8 pixels DCT block. An 8x8 DCT block consists of 22 middle band coefficients, so the length of each pseudo random sequence is 22 elements. A secret key is used for creating these sequences. The same key is needed in recovering process to generate the same pseudo random sequences. This scheme provides us with a more secure method. The equation of the embedding process is given in Equation (4.1).

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) + kW_{x,y}(u,v), & u,v \in F_M \\ I_{x,y}(u,v), & u,v \notin F_M \end{cases} \quad 4.1$$

$I_{x,y}(u,v)$  represents the middle band frequency coefficient. The pseudo random sequence  $W_{x,y}(u,v)$  is multiplied by the strength constant  $k$ .  $F_M$  denotes middle-band frequency band. If the watermark data bit is '1', the related pseudo random sequence is multiplied by the strength constant and added to middle band coefficients of the selected block. For watermark data bit '0', all operations are the same except the pseudo random sequence for watermark data bit '0' is used instead. The watermarked block is then back-transformed to spatial domain by using inverse DCT. After all data bits in the given piece of watermark are embedded into the chosen blocks in the current frame, embedding stage is completed and the next frame and next piece of watermark go through the same process.

The method proposed here has several advantages compared to the conventional DCT based method. The pseudo random sequences are generated by a secret key and this improves the security of the method. Also, all blocks are not modified and the modified blocks are selected again with an algorithm that uses a secret key. This makes the identification of the watermarked blocks harder for an attacker. Using strength constant also improves the robustness of the method but this parameter should be selected carefully. A high value of strength constant causes more robust

method at the cost of more distortions on the original video. The overview of this algorithm is given in Figure 4.2.

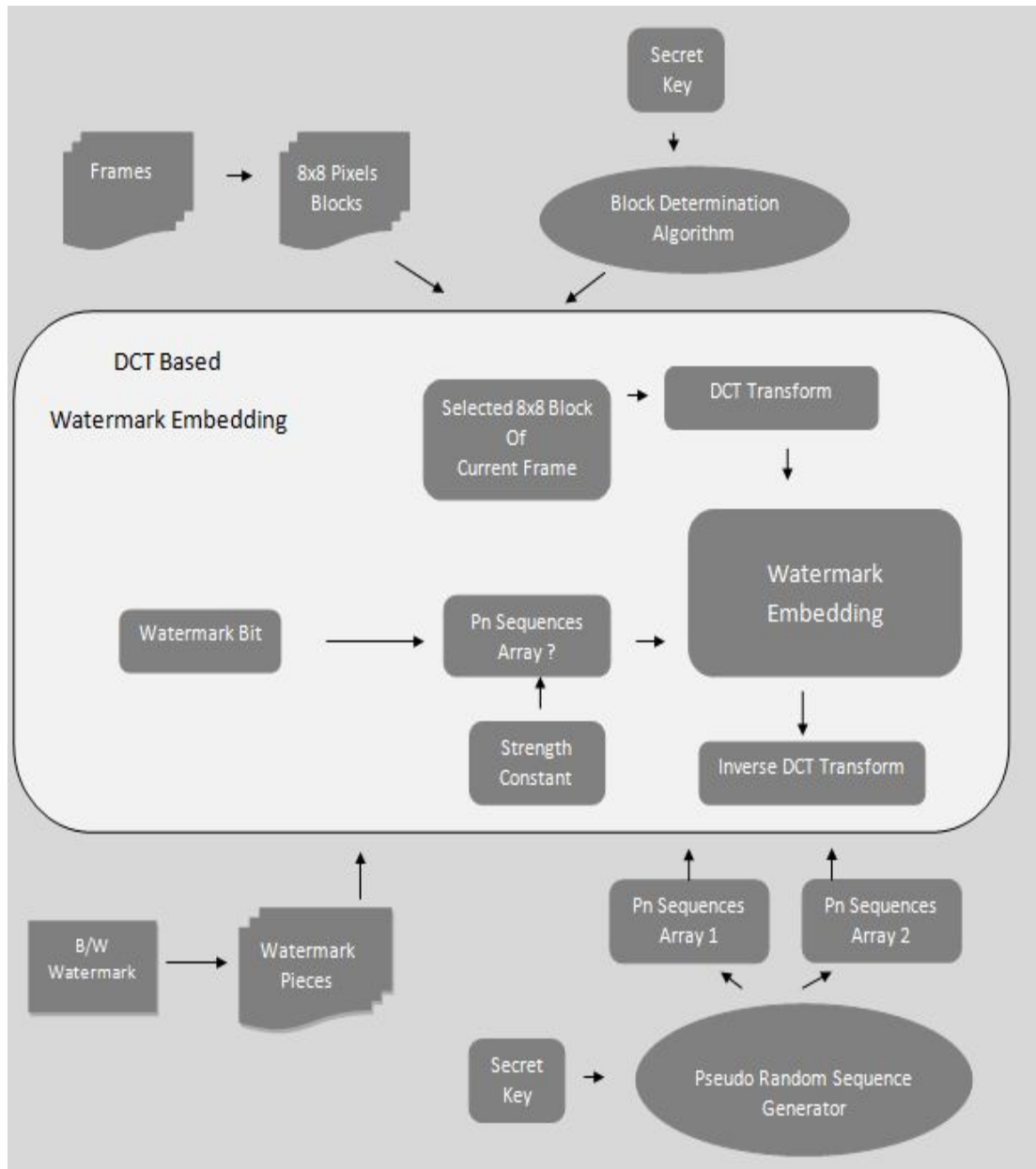


Figure 4.2 Watermark embedding method using DCT

#### 4.2.2 Discrete Wavelet Transform based Method

If the current frame is to be processed with DWT, it is transformed to frequency domain. 1-level Wavelet transform is done in the method implemented in this thesis



for simplicity and avoiding computational complexity. Also, capacity and quality requirements are important parameters when the level of DWT is determined. Figure 4.3 shows the 1-level DWT of a frame by frequency bands. Embedding is performed based on the method of adding pseudo random sequence. After the frame is transformed using DWT, the lower resolution approximation band and diagonal detail band are not modified in embedding watermarks. The content owner chooses one of the horizontal and vertical detail bands or both of them for watermarking.

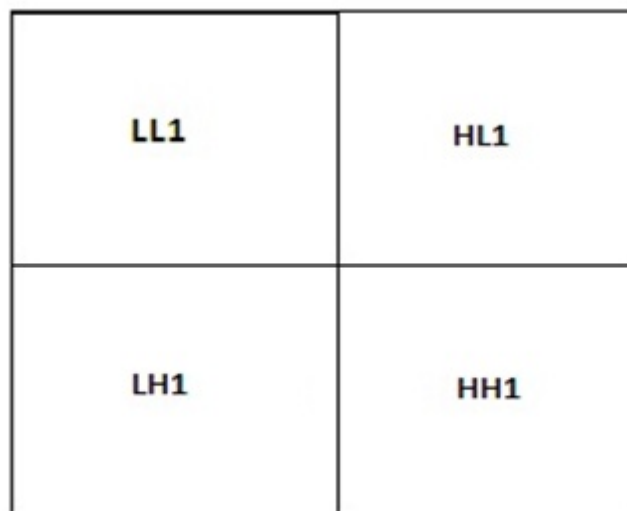


Figure 4.3 Detail bands of 1-level DWT

A pseudo random sequence is generated using a generator and this generator is seeded with a secret key. This secret key is also used in recovering stage and the same sequence can be generated only with using this key. So, this key makes the method more secure. Because the watermark data are embedded to the entire vertical or horizontal detail band coefficients, the length of the pseudo random sequences is equal to length of these bands. For all watermark bits, different pseudo random sequences are generated with length of these frequency bands.

After the current frame is transformed to frequency domain using 1 level Haar DWT, an image is represented by 4 different bands. The method offers flexibility about the bands to be used in embedding process. Horizontal detail band or vertical detail band can be used together for embedding watermark or only one of them can

be selected. The band selection information is also needed in recovering stage. This makes the method more secure and give a chance to content owner to consider the watermarking requirements (imperceptibility or robustness) and decide the band used.

Watermark data are kept in an array and all bits are embedded to the selected band one by one. Only watermark bits '0' (black pixels in the binary watermark image) are used for watermark embedding for this method to improve imperceptibility requirement of watermarking algorithm. If the watermark data bit is '0', the pseudo random sequence is multiplied by the strength constant and then added to related band. Then, the second bit is used as input. If this bit is "0", then another pseudo random sequence is multiplied by the strength constant and added to related band. If the watermark data bit is '1', there is no data embedded to related band. This is repeated for the all bits in the watermark piece to be embedded into the current frame. Pseudo random sequences for the watermark bits are generated beforehand. After all watermark data are embedded to the selected frequency band(s), the frame which is in frequency domain is transformed to spatial domain by the inverse DWT. These stages for watermark embedding are done for all frames sequentially.

The visual quality of the video may reduce dramatically for DWT based methods because some data are embedded cumulatively to the selected detail band(s) for each watermark data bit. If the size of the watermark piece is high, the embedded data distorts the visual quality of the video too much. Therefore, in the DWT based method implemented in this thesis, no watermarking is performed for watermark bits '1' to improve visual quality of the video.

The band which contains the watermark data is known by the content owner and in recovering stage this info is needed. Also, the seed of the pseudo random generator should be known in recovering stage. These parameters improve the security of the method. The overview of this method is shown in Figure 4.4.

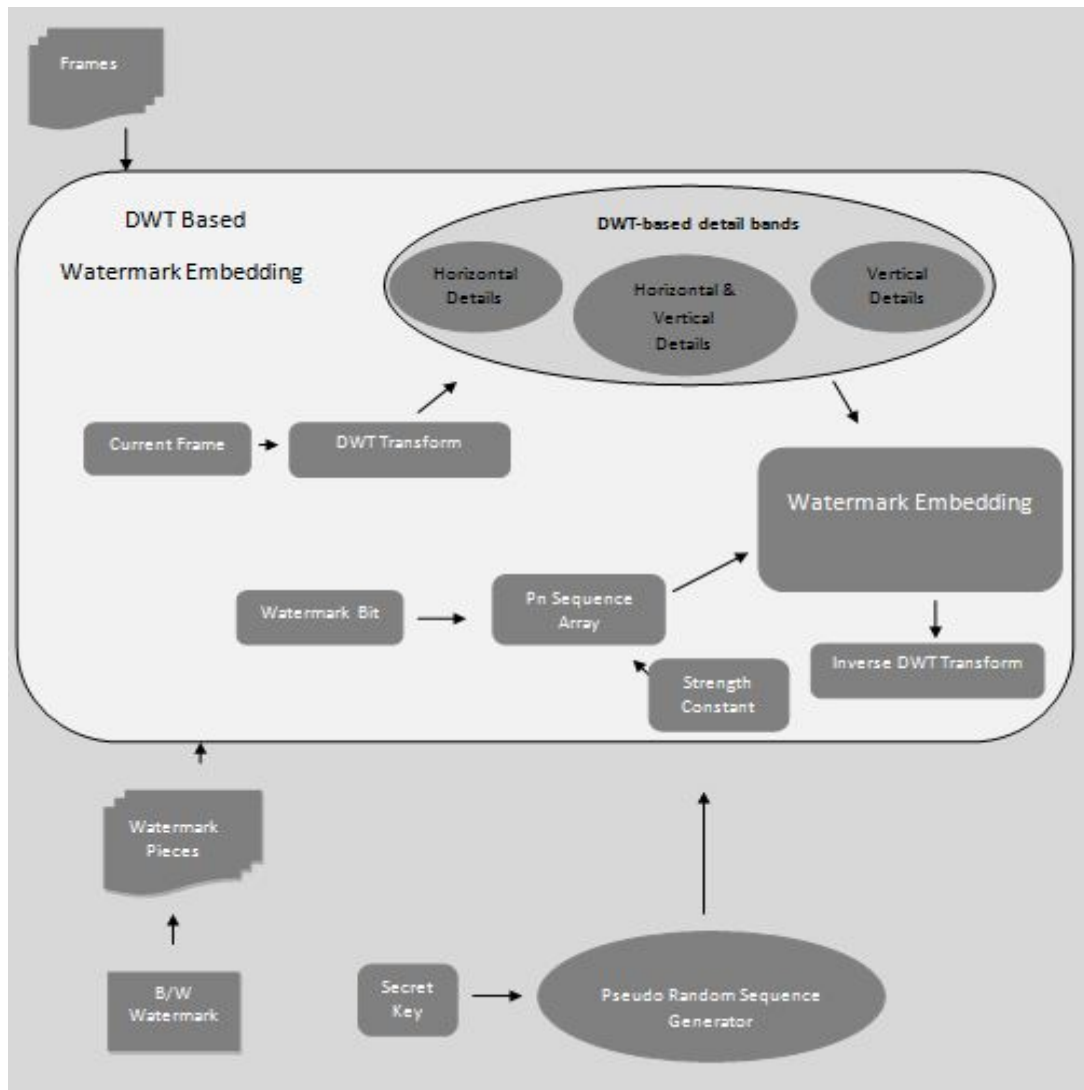


Figure 4.4 Watermark embedding method using DWT

### 4.2.3 Hybrid Method based on Discrete Cosine and Wavelet Transforms

The hybrid method quoted throughout this thesis means that it uses the DCT or DWT, or both of them together to watermark a frame. Selection among these possibilities is made randomly for each frame. The hybrid method is expected to perform better by exploiting the advantages of the both transform based methods. When some watermark pieces embedded in video using one transform based method are removed or distorted by an attack, their copies embedded into the remaining frames using the other transform based method may still survive and help to recover

the entire watermark data. This makes our hybrid method more resistant against attacks.

The algorithms and parameters which are aforementioned in preceding sections are the same with the hybrid method. In embedding stage, frames are taken sequentially, and one of the three different embedding methods and the watermark piece for the current frame are determined randomly by software. The current frame can be processed with the DCT based method or DWT based method or the combined DCT-DWT method.

If the DCT based or DWT based method is selected, the watermark piece is embedded to the entire frame using the known DCT based or DWT based method. If the combined DCT-DWT method is selected, the current frame is divided into two equal parts along horizontal direction and each part is processed separately. The upper half of the frame is processed using the DCT based method. The secret keys and block selection algorithms are logically the same except that the number of 8x8 blocks in a frame is halved because only one half of a frame is considered. In return, the watermark capacity of a frame is also halved. Therefore, this brings in a trade-off between improved robustness gained by the combined DCT-DWT method and the watermark capacity. The lower half of the frame is processed using the DWT based method. Pseudo random sequences and band selection flexibility are the same as that of the known DWT based method except that the operations are performed in the frequency domain of the half of a frame. The overview of this method is shown in Figure 4.5.

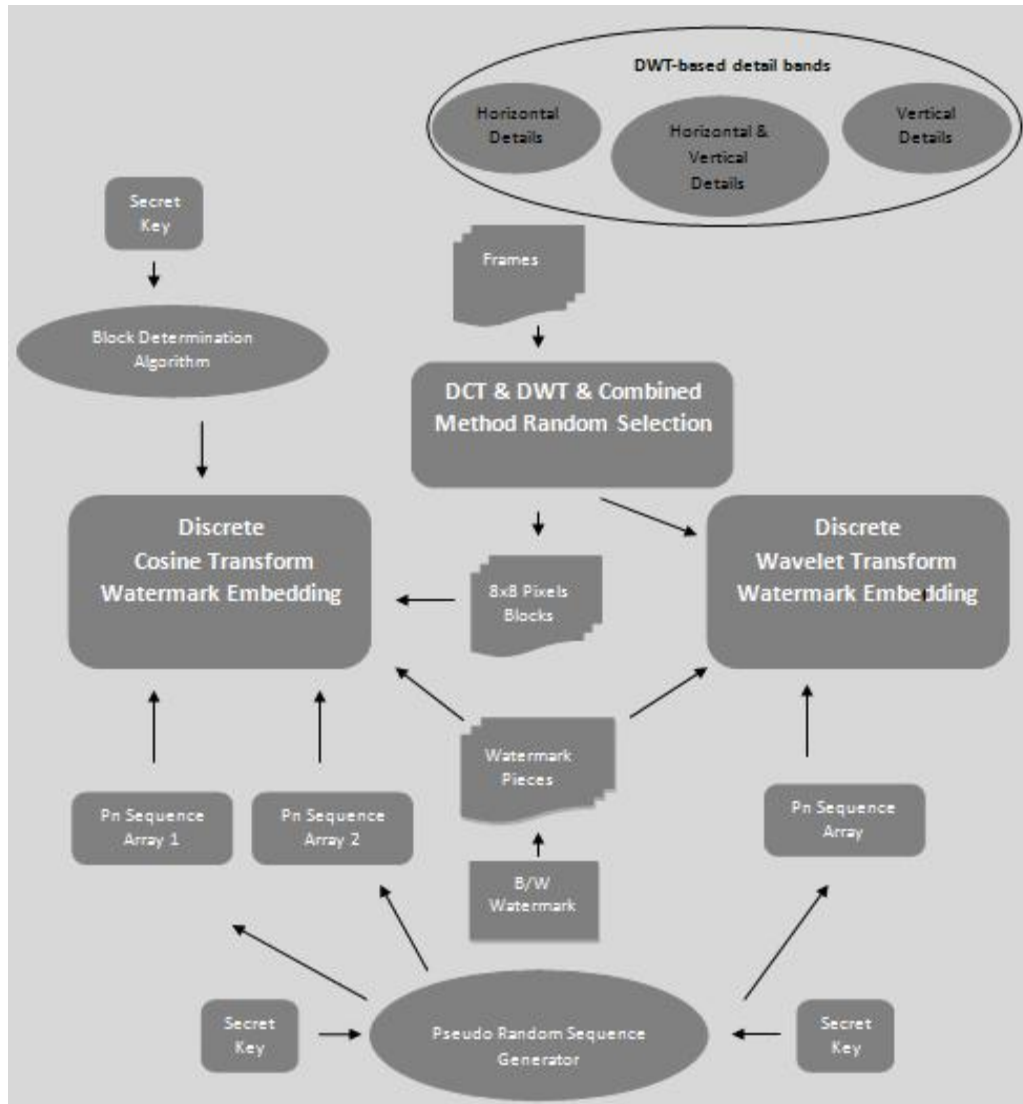


Figure 4.5 Watermark embedding algorithm of the proposed hybrid method

### 4.3 Watermark Recovering

In watermark embedding stage, the watermark data were embedded into a frame by one of the DCT based, DWT based and DCT-DWT based methods. So, in recovering stage, the same transform can only help to recover the watermark piece from a frame. The recovering process includes three stages. The watermarked video is used as input for the DCT based, DWT based and combined DCT-DWT based watermark recovering methods separately. All three methods have to be tried to recover watermark data from each frame because original watermarked frame order

may be void after some attacks that drop several frames from original video or change order of frames in video. Some attacks can especially distort the watermark data embedded in a frame using one of the frequency domain transforms (DCT or DWT). In this case, the advantage of the combined transform based watermarking in the hybrid method appears. If one of the transform based methods cannot resist to some attacks, the other transform based method may hopefully resist and the watermark data can be recovered from the other half frame associated with that transform.

#### ***4.3.1 Discrete Cosine Transform based Method***

The watermarked video, the number of pieces of the watermark data and the original watermark data itself are inputs for the recovering stage. Each frame is examined in recovering stage and it is determined whether the current frame contains a watermark piece or not. If a frame is watermarked using a method other than the DCT based method, obviously, no watermark data will be recovered. After all frames of the watermarked video are processed the entire watermark data can be reconstructed.

Each frame is again divided into 8x8 blocks and middle band frequency coefficients are used for recovering watermark data bits. The same algorithm which is used in embedding stage for determining the blocks to be watermarked is again used in recovering stage. The blocks are determined and their location information is kept in an array. The same pseudo random sequences representing '1' and '0' watermark data bits are also needed in recovering stage. The same secret key is used again in this stage and pseudo random generator is run with this key. The pseudo random sequences are kept in arrays. There is no way to recover the watermark data without knowing the secret keys and using the algorithm for block selection. This makes the method more robust and secure. After the parameters of the method are generated and saved, each block which is determined by block selection algorithm in the current frame is transformed into frequency domain with DCT. Then the middle band coefficients are correlated with the two pseudo random sequences which are

generated for watermark data bits '0' and '1'. The two correlation values are compared with each other and the more correlated sequence is accepted as recovered possible watermark data bit. This higher correlation value denoted by  $C_b(i)$  for  $i$ th bit of the watermark piece is saved. After all blocks are examined, a digital data that is a possible piece of the watermark data is formed by concatenating the recovered possible watermark data bits. This datum is compared to each of the real watermark pieces by computing a binary correlation to see whether or not the recovered possible watermark datum is similar enough to one of them. The index of the maximum correlated piece, correlation value and the recovered possible watermark data are the outputs of this recovering process. If the maximum correlation value does not exceed a predefined threshold value  $T_p$ , the recovered data is assumed to be noise, and that the frame from which this possible watermarked data has been recovered is not watermarked, or the watermark data is distorted. The recovered possible watermark data is ignored in this case. This recovering process is repeated for all frames. The recovered data which have higher correlation than the threshold value are kept in an array. The block diagram of this recovering algorithm is shown in Fig. 4.6. The reconstruction of the entire watermark data following the recovering stage is based on a data fusion method that works on the individual recovery results from the video frames. This data fusion method is explained below.

The recovered watermark pieces are grouped according to watermark piece index. So, a watermark piece can be reconstructed by evaluating the results in the group of the same index. First, all recovered data are tested bit by bit. If a bit has a correlation value  $C_b(i)$ , higher than a predefined bit correlation threshold value  $T_b$ , this bit is assumed as a correctly recovered bit. If not, this bit is regarded as unknown and replaced by a '0' by default. Then, individual bits of a watermark piece to be reconstructed are determined by validation across the results in the group of the same index as follows. The majority (greater than 70%) of results for  $i$ th bit of recovered watermark pieces in the group is assigned to  $i$ th bit of the reconstructed watermark piece of the same index.

The threshold values are parametric and can be easily changed in software. Depending on the video data and distortion in the video, the recovering process can be repeated several times to find optimum values of these parameters in order to detect watermark data.

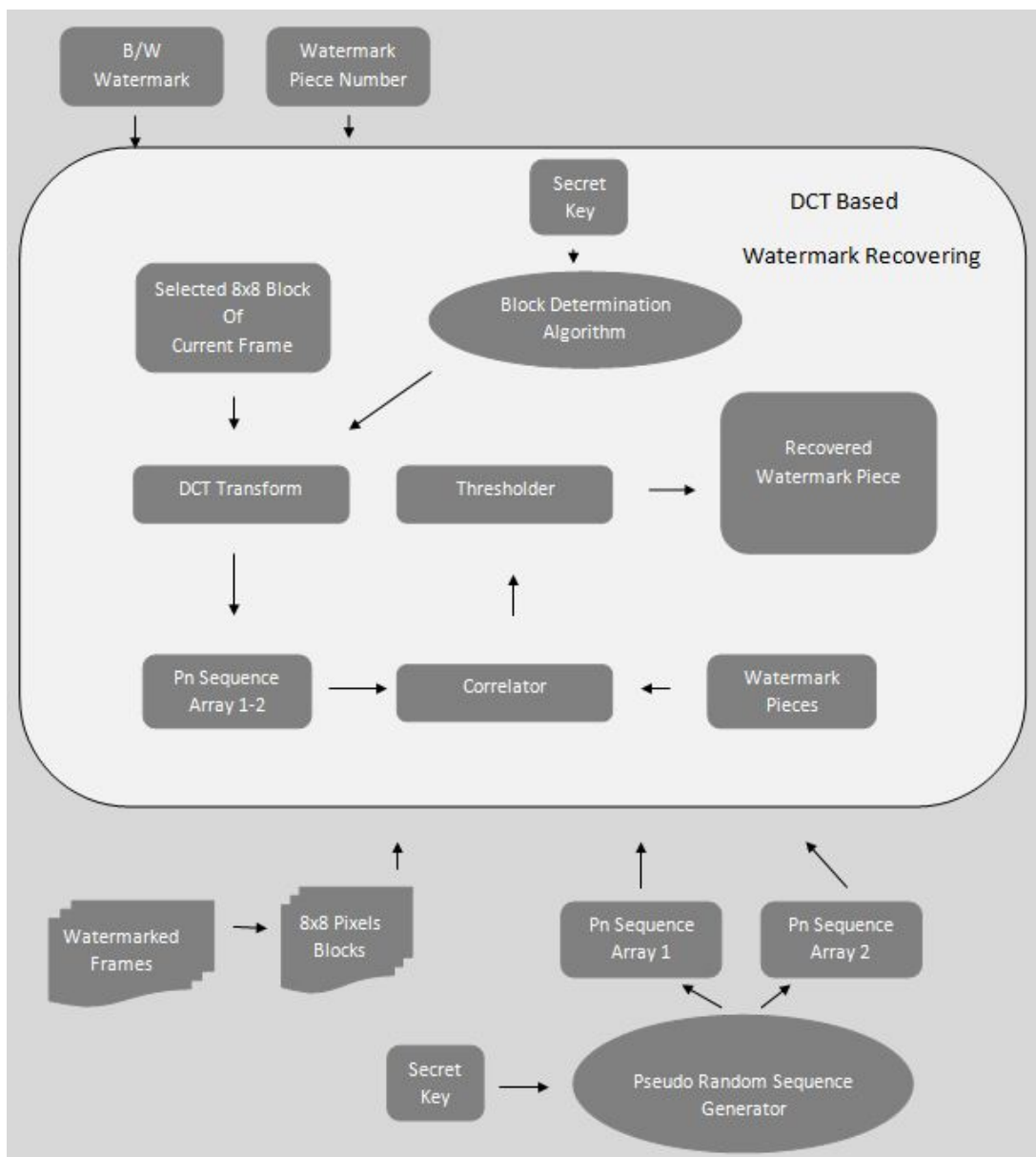


Figure 4.6 Watermark recovering method using DCT



### 4.3.2 *Discrete Wavelet Transform based Method*

The watermarked video, the number of pieces of the watermark data, the watermarked band and the original watermark data itself are inputs for the recovering stage. Each frame is examined in recovering stage and it is determined whether the current frame contains a watermark piece or not. If a frame is watermarked using a method other than the DWT based method, obviously, no watermark data will be recovered. After all frames of the watermarked video are processed the entire watermark data can be obtained.

The frame is transformed to frequency domain using 1-level DWT. The wavelet coefficients are different from each other depending on their degree of detail. After decomposition at each level, four sub images are generated. One of them is the lower resolution approximation sub image, and the others are horizontal, vertical and diagonal detail coefficients. In embedding stage, a parameter had to be set to indicate the selection of the band which contained the watermark data. This parameter has to be known in the recovering stage so that the related bands are examined for watermark detection. This makes contribution to the security improvement of the method. The pseudo random sequence representing watermark data bits are also generated using the secret key which was used in the embedding stage. This is also one of the key points of the method and improves the security.

In watermark embedding stage, it is determined which detail band is used for watermarking. Either horizontal or vertical detail bands or both of them can be used. Then, the frame is DWT transformed with 1-level and the watermarked band coefficients of the transformed frame are used for recovering. The watermarked band coefficients of each frame are correlated with every pseudo random sequence representing every bit in the entire watermark one by one. If the correlation value for  $i$ th bit of  $n$ th watermark piece is higher than a predefined threshold value  $T'_b$ , this bit is identified with a probability as the given watermark data bit. Otherwise, given watermark bit cannot be identified and assumed a '0' by default. After determining and concatenating all of its bits in this manner,  $n$ th watermark piece can be

recovered. These data are compared to  $n$ th real watermark piece by computing a binary correlation value  $C_p(n)$ , to see how similar the recovered watermark piece is. This process is repeated as many times as the number of watermark pieces and gives  $C_p(n)$  values among which the maximum value is found. The real watermark piece giving the maximum correlation is decided as the watermark piece embedded in that frame. The index of the maximum correlated piece, correlation value and the recovered possible watermark data are the outputs of this recovering process. If the maximum correlation value does not exceed a predefined threshold value  $T_p'$ , the recovered data is assumed to be noise and that frame is assumed not watermarked (or the watermark data are distorted). The recovered possible watermark data are ignored in this case. This recovering process is repeated for all frames. The recovered data which have a higher correlation value than the threshold are kept in an array. The block diagram of this recovering algorithm is shown in Figure (4.7). The reconstruction of the entire watermark data following the recovering stage is performed by a data fusion method similar to that in the DCT based method as follows.

The recovered watermark pieces are grouped according to watermark piece index. So, a watermark piece can be reconstructed by evaluating the results in the group of the same index. Individual bits of a watermark piece to be reconstructed are determined by validation across the results in the group of the same index as follows. The majority (greater than 70%) of results for  $i$ th bit of recovered watermark pieces in the group is assigned to  $i$ th bit of the reconstructed watermark piece of the same index.

Depending on the video data and distortion in the video, the recovering process can be repeated several times to find optimum values of these parameters in order to detect watermark data.

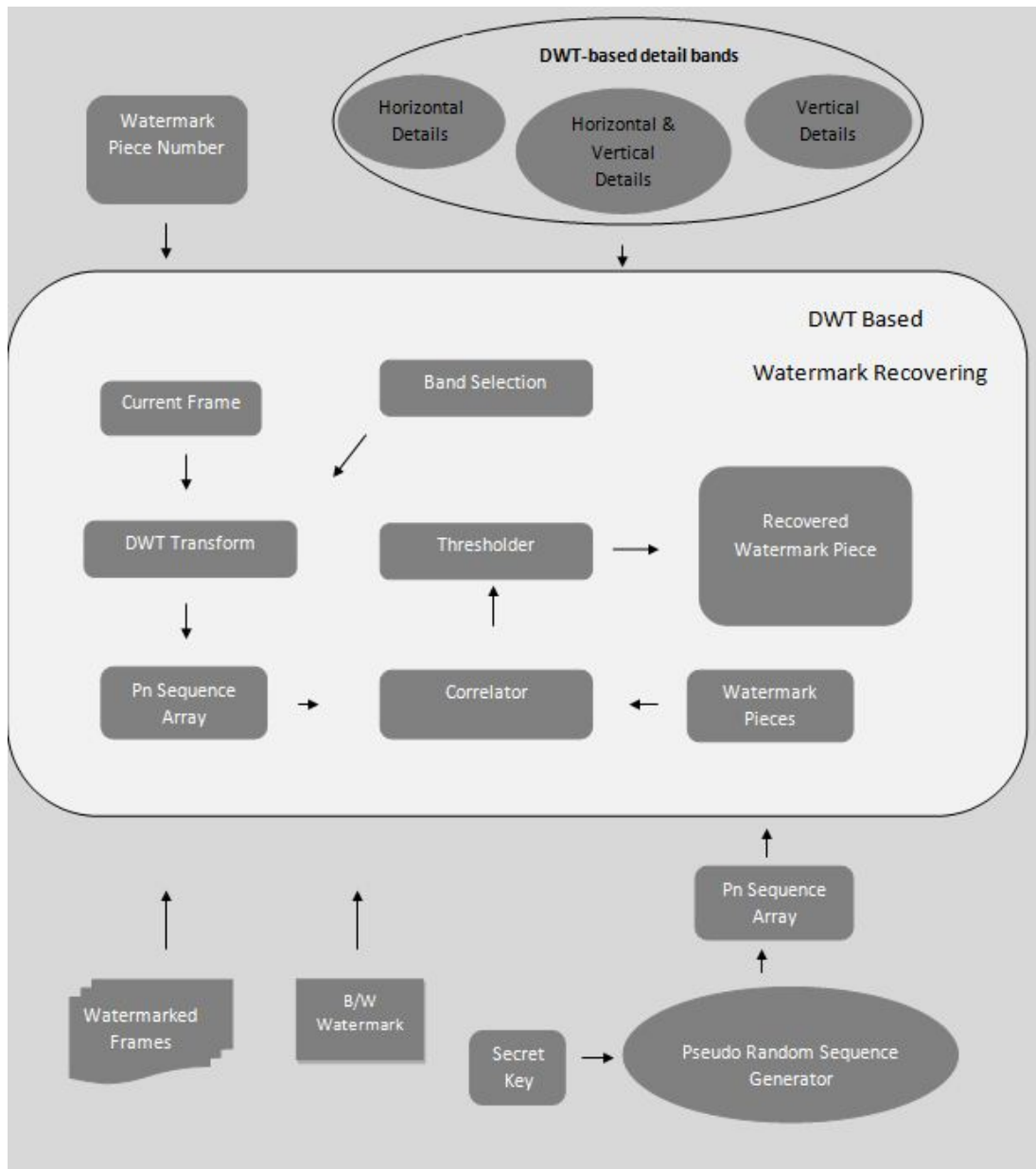


Figure 4.7 Watermark recovering method using DWT

### 4.3.3 Hybrid Method based on Discrete Cosine and Wavelet Transforms

The watermark recovering stage in the hybrid method is a combination of the recovering stages in the DCT based and DWT based methods. The watermarked video, the number of pieces of the watermark data, the original watermark data and the watermarked band information for DWT are inputs for the recovering stage. In hybrid method, watermarked video has frames which are processed with DCT based,

DWT based, and combined DCT-DWT methods. In recovering stage, watermark data can be recovered using one of these methods.

Recovering stage of the DCT based and DWT based methods are the same as those mentioned in Sections 4.3.1 and 4.3.2. If watermark data are to be recovered using combined DCT-DWT method, firstly, each frame is divided into two equal pieces by a horizontal line. Recovering possible piece of the watermark data from the upper part is the same as that of the DCT based method and from the lower part is the same as that of the DWT based method. The outputs of these two independent recovering processes are stored separately.

In hybrid method, the same embedded piece of watermark data can be recovered by not only combined DCT-DWT method, but also by the DCT based method and/or the DWT based method from several frames in a watermarked video. So, the video watermarked by the hybrid method has the power of the diversity of different ways of watermarking. This power grants an efficient and more accurate watermark reconstruction capability from a video undergone an attack from a large group of types.

The watermarked video may undergo some attacks and some parts of the video may be distorted. In this case, one of the transform based methods may not be resistant to these attacks but the watermark data can be recovered with the help of the other method. The vulnerability of one watermarking technique used in the hybrid method to a specific type of attack can be compensated through the other technique bearing robustness to that attack. The block diagram of this recovering algorithm is shown in Fig. 4.8.

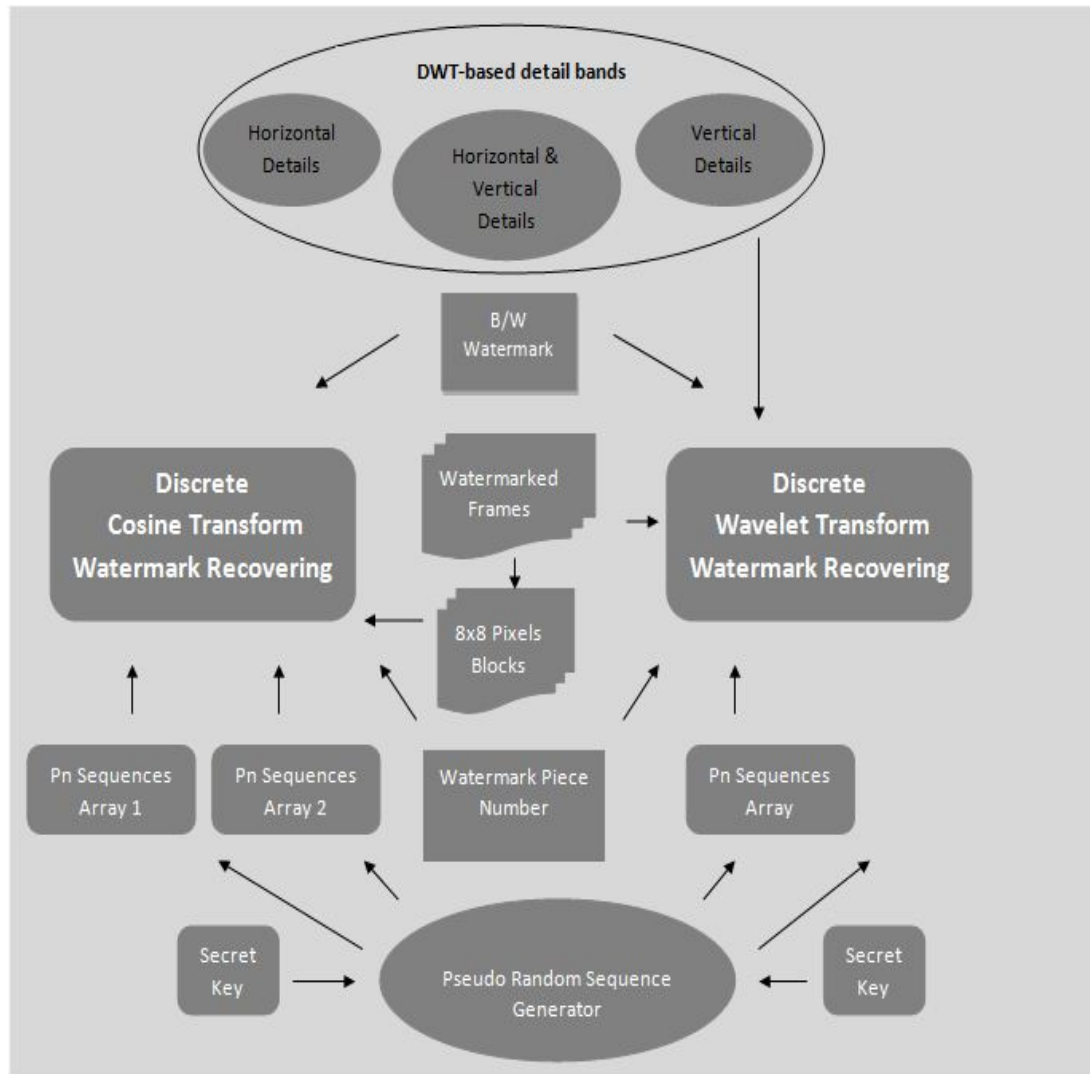


Figure 4.8 Watermark recovering using the hybrid method

## CHAPTER FIVE

### EXPERIMENTAL RESULTS

In this chapter, the experimental results of the proposed hybrid method are presented. In the hybrid method, DCT based, DWT based and combined DCT-DWT based methods are used together and a piece of watermark data are embedded to each frame using one of these methods.

While the DCT based method embeds watermark data into every frame of video using the DCT of blocks, in the DWT based method, the transformation is simply switched to the DWT of entire frame. As to the combined method, the same watermark data is embedded to the upper half of a frame by the DCT and to the lower half by the DWT. Also, for the DWT based and combined methods, we use both horizontal and vertical detail bands for embedding a watermark piece.

After embedding watermark data into a video, the watermarked video is undergone some attacks and results of the watermarking methods are compared with each other. These results are presented with tables and graphs in the following sections.

For a video watermarked by the hybrid method, the watermark data can be recovered using one of the DCT based, DWT based and combined DCT-DWT based methods. In the following sections, the results which are obtained using these methods are presented in detail.

#### 5.1 Details of Tests

A digital video with 104 frames of size 640x480 is used in the tests. Also, two different watermark data are used. The dimensions of the watermark data are 20x20 and 24x24 pixels. A sample frame from the original test video and the watermark data used in the tests are shown in Figures 5.1 and 5.2, respectively.



Figure 5.1: A sample frame from the original test video

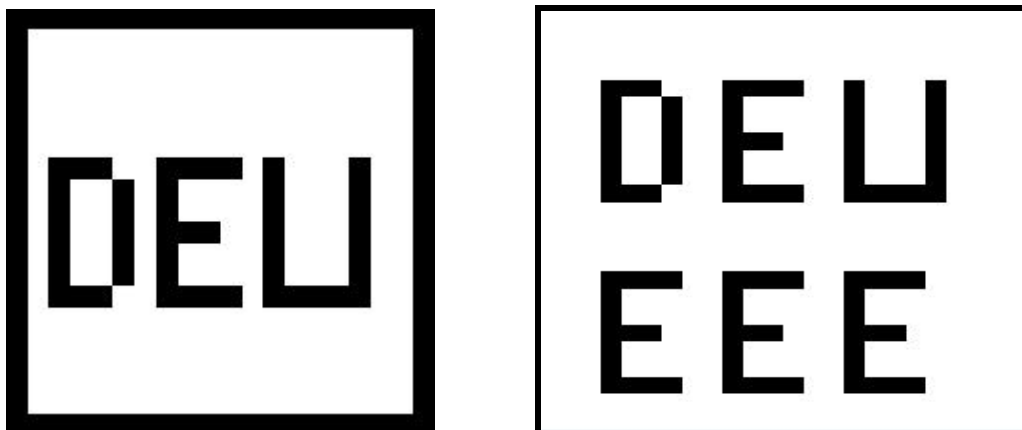


Figure 5.2 Watermark image 1 and 2 used in the tests

The tests are performed in two stages. The aim of the first stage is to determine and compare the robustness, imperceptibility and capacity requirements of the DCT based and DWT based methods. The original video is processed with the DCT based and DWT based methods separately and the results of these tests are presented with tables and graphs. In the second stage, the original video is processed with the

proposed hybrid method and the same requirements as those in the first stage are evaluated. We remind that, as implemented in this thesis, the hybrid method embeds a watermark piece into a frame of the test video using one of the DCT based, DWT based and the combined methods randomly. As explained in Section 4.3.3, the watermark data are recovered piece by piece using all three methods from the video frames. A final recovered watermark image is obtained from the recovered watermark pieces using a data fusion approach that is explained in detail in Section 5.2.

In both stages, the tests are performed under 4 different scenarios. The first watermark image is divided into 2 and 4 pieces in the first two scenarios, respectively. And the second watermark image is divided into 2 and 6 pieces in the last two scenarios, respectively.

The details of the attacks and the results obtained with every attack are presented in the following sections. The normalized correlation value between a reconstructed entire watermark and a real entire watermark is computed and given as a measure of watermark detection robustness of the tested method under a given scenario. These correlation values are presented in tables and charts and compared with each other for all scenarios in the related sections.

There is an important point that must be mentioned regarding the test results. The results show the performance of a watermarking algorithm on a digital video with 104 frames under a particular attack. If longer videos were used in the tests, each watermark piece would be embedded into more frames. In this case, more frames would contain the same watermark piece, thus, increasing the probability of recovering the entire watermark data correctly. As a conclusion, we can say that the computed correlation values change depending on the length of test video and size of the watermark image. The longer a test video is used, the higher correlation values are obtained.



## 5.2 Tests for Robustness Requirement

In this section, robustness requirement of the methods are tested after applying some attacks. A video may be distorted in transmission and distribution channel after the watermark is embedded in the video. In this thesis, these distortions or attacks are simulated with software which is written in MATLAB environment.

Several attacks are applied to the watermarked video and the performances of the watermark recovering algorithms are compared with each other and presented in tables and graphs. Frame dropping, frame averaging, noise addition, video compression, image enhancement and median filtering attacks are performed on the watermarked video. The measure used for comparison of the robustness characteristics of the methods is the normalized correlation value between recovered watermark data and real watermark data computed after the entire watermark data are reconstructed. A normalized correlation value is calculated with 'corr2' function in MATLAB. These correlation values between a reconstructed watermark image and corresponding original watermark image are presented in tables. The results of the attacks are explained in detail in the next sections.

Figure 5.3 shows a block diagram of the data fusion algorithm applied after recovering watermark pieces. A possible watermark piece is recovered from a frame and these data are compared with each of the real watermark pieces. Recovered watermark piece, index of most correlated real watermark piece and correlation value between the real watermark piece and recovered watermark piece are the outputs of the recovering function. After all these data are obtained from all frames, data fusion is performed. Firstly, the correlation values obtained from all frames are compared to a threshold value. A recovered watermark piece which has produced a correlation value lower than the threshold is ignored. Then, recovered watermark pieces are grouped according to their piece indexes. The watermark pieces in the same group are compared pixel by pixel and if a pixel has a same value (0 or 1) for a number of frames which is higher than a predefined threshold, the value of this pixel is selected for the same pixel in the reconstructed final watermark, otherwise it is set as '0' as

default. After all pixels in all groups of watermark pieces are processed in this way, a final recovered watermark image is reconstructed.

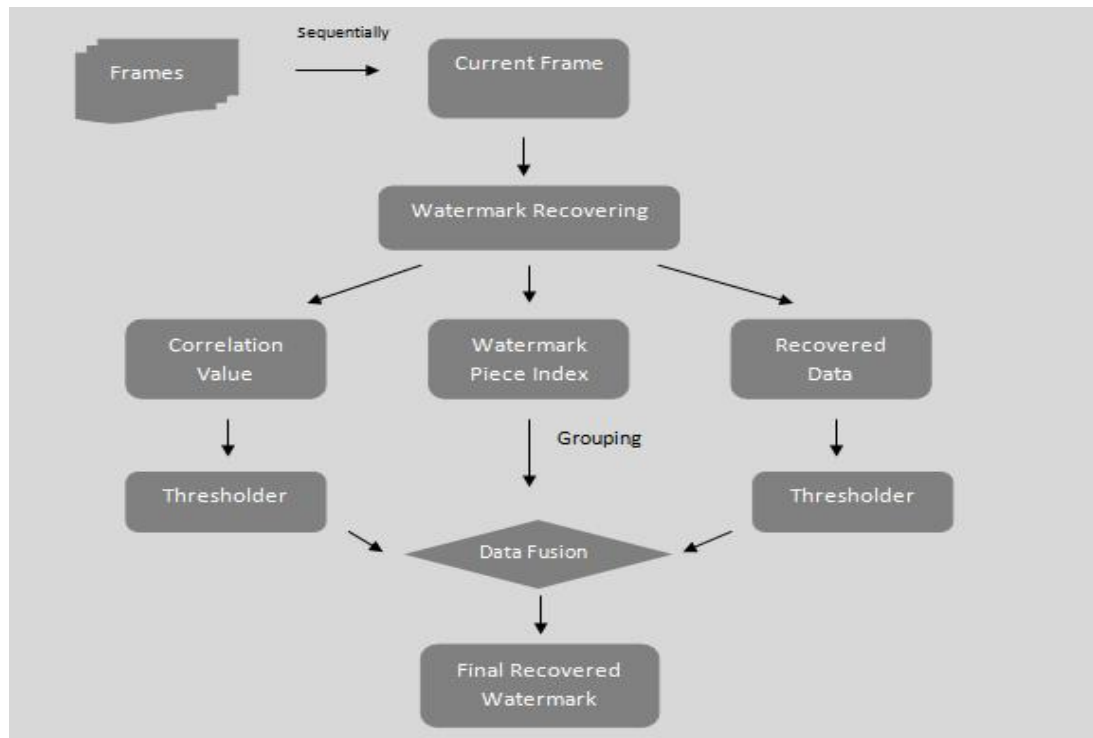


Figure 5.3 Data fusion after recovering watermark pieces

### 5.2.1 Noise Addition Attacks

A watermark data are embedded into the original video and noise addition attacks are performed. DCT based, DWT based and DCT-DWT combined methods are tested one by one. Noise is added into all color bands (i.e., red, green, and blue) of the watermarked video. Noise addition is done using MATLAB function *imnoise* and two types of noise are selected: ‘salt & pepper’ noise and Gaussian noise.

The tests are done for 4 different scenarios. The video is tested with ‘salt & pepper’ noise for 4 different noise densities. Noise density gives the amount of degraded pixels in percentage in each frame of the video. Tests with Gaussian noise are performed using white Gaussian noise of zero mean and normalized variance 0.005. The MATLAB function *imnoise* requires us to input normalized variance

values. The results of the tests are presented in Table 5.1. Also, Figures 5.4 and 5.5 show the results with graphs.

Table 5.1 Correlation results of DCT based and DWT based methods after noise addition attacks

Noise Density (salt & pepper)	DCT				DWT			
	Scenario				Scenario			
	1	2	3	4	1	2	3	4
0.01	0,99	0,99	0,97	0,93	1,00	1,00	1,00	1,00
0.02	0,98	0,98	0,97	0,91	1,00	1,00	1,00	1,00
0.03	0,87	0,81	0,97	0,79	1,00	1,00	1,00	1,00
0.04	0,69	0,74	0,96	0,65	0,99	0,95	1,00	1,00
Gaussian noise	0,97	0,88	0,98	0,87	1,00	1,00	1,00	1,00

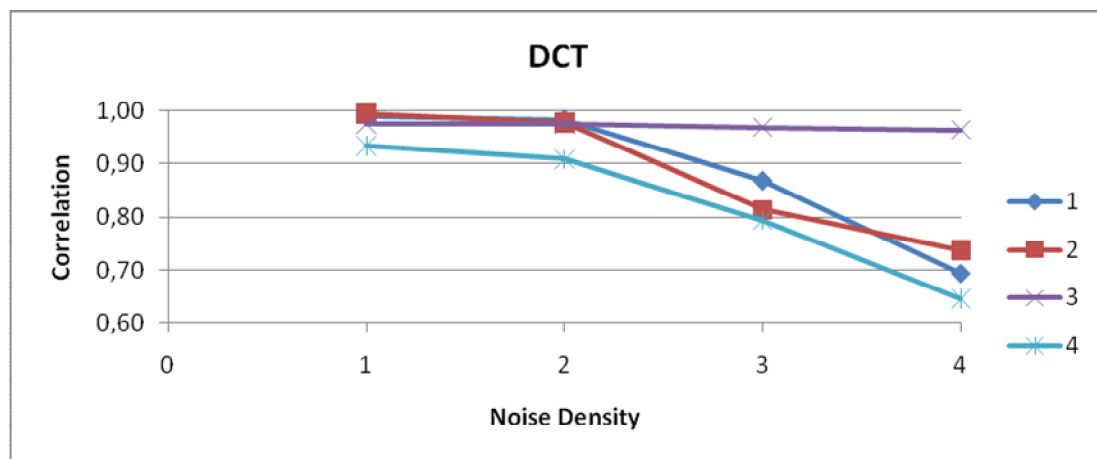


Figure 5.4 Correlation values obtained with DCT based method for noise addition attacks

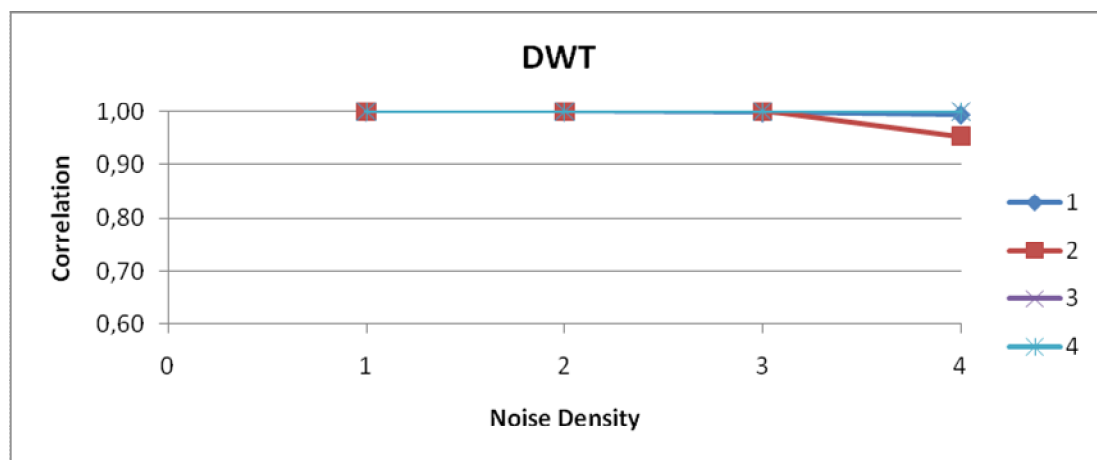


Figure 5.5 Correlation values obtained with DWT based method for noise addition attacks

From the table and graphs given above, it is seen that the robustness of all the methods to noise attacks are good. When the methods are compared, it is seen that the DWT based method is more robust to noise attacks. Even for the highest noise density attack, correlations between the recovered watermarks and the original watermark are high. The noise attack is applied to all regions of a watermarked frame randomly so every pixel can undergo this attack and be set to black or white. If the watermark data are divided into very small pieces so that each embedded piece of watermark data contains too little information, applying severe random noise to a watermarked frame can easily distort majority of the bits in this piece. This makes the recovery of that piece of watermark all over the video data using fusion approach more erroneously. Because the same distorted bits in a frame are more probable to be distorted in the other frames as well when the size of the piece of watermark is too small. The watermark data are divided into 4 and 6 pieces in the 2<sup>nd</sup> and 4<sup>th</sup> scenarios and the embedded data are relatively less compared to that of the other scenarios, thus the embedded data in all frames can be distorted more easily after noise addition.

The first result is that DWT based method is more robust to noise attacks. The second is that when the amount of embedded data per frame is larger, the watermarking methods become more robust.

In the second stage of the test, the original video is processed with the proposed hybrid method and the same noise addition attacks are applied to this video. The results of the tests are presented in Table 5.2 and also in Figure 5.6.

Table 5.2 Correlation results of hybrid method after noise addition attacks

	<b>Hybrid Method</b>			
	<b>Scenario</b>			
Noise Density (salt & pepper)	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
0.01	1,00	1,00	1,00	1,00
0.02	1,00	1,00	1,00	1,00
0.03	1,00	0,98	1,00	1,00
0.04	0,89	0,95	1,00	1,00
Gaussian	1,00	1,00	1,00	1,00

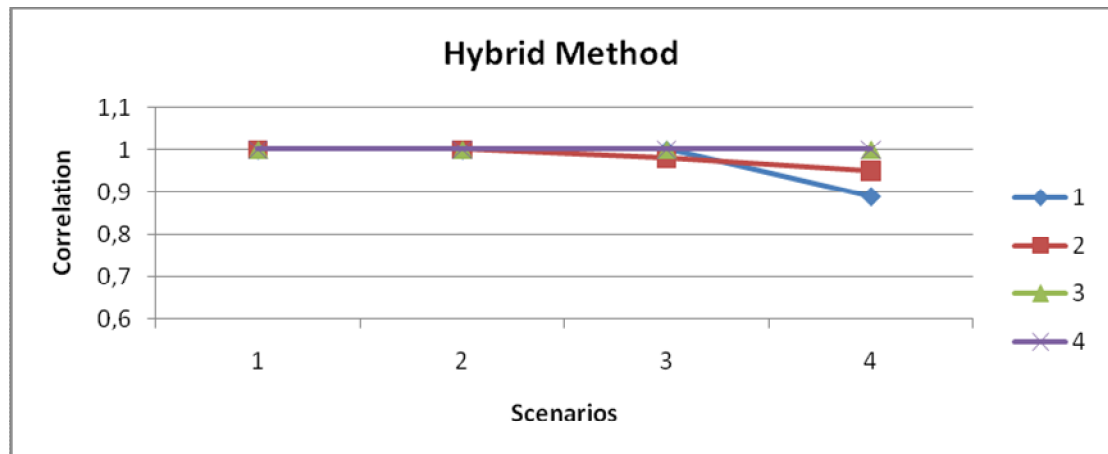


Figure 5.6 Correlation values obtained with the hybrid method for noise addition attacks

From the table and graphs given above, it is seen that the hybrid method is robust to noise attacks as well. Even for the highest noise density attack, correlations between the recovered watermarks and the original watermark are high.

In the literature, there are some other algorithms which use DCT for watermarking. In some of these algorithms, the watermark data are embedded to the same region in every frame of the original video using DCT. This is either one of the corner regions, bottom region, or the central region of the frames. An attacker can guess where the watermark data are in a frame and can only distort this region of the watermarked frame. But, in this thesis, we propose a different algorithm in that sense. Our algorithm embeds watermark data to a scattered region which are determined by a secret key and this region is known by only the content owner.

### 5.2.2 *Frame Dropping Attacks*

A video consists of many frames and these frames can be dropped by some attacks. Because a video contains a large amount of redundancies between frames, frame dropping may be an attractive attack to destroy watermark data. In the tests, the frames of the watermarked videos were dropped by different ratios and the robustness results of the methods are compared to each other. After the frame dropping ratios were determined, frame dropped videos were generated in MATLAB

environment, and then the videos were tested one by one. The results of the tests are presented in Table 5.3 and also in Figures 5.7 and 5.8 below.

Table 5.3 Correlation results of DCT based and DWT based methods after frame dropping attacks

Frame dropping ratio %	DCT				DWT			
	Scenario				Scenario			
	1	2	3	4	1	2	3	4
10	0,99	0,99	0,97	0,98	1,00	1,00	1,00	1,00
20	0,99	0,99	0,98	0,96	1,00	1,00	1,00	1,00
30	0,99	0,99	0,97	0,95	1,00	1,00	1,00	1,00
40	0,98	0,98	0,97	0,94	1,00	1,00	1,00	1,00
50	0,99	0,97	0,96	0,90	1,00	1,00	1,00	1,00
70	0,99	0,98	0,97	0,87	1,00	1,00	1,00	1,00

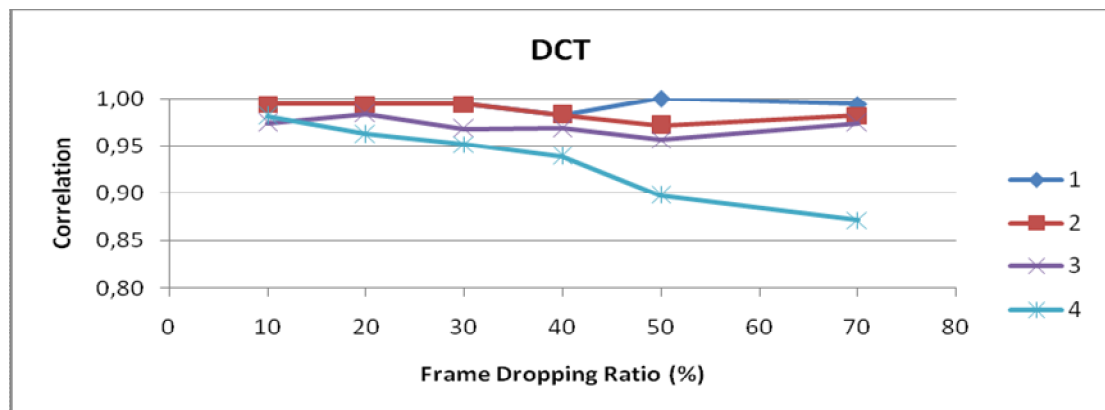


Figure 5.7 Correlation values obtained with the DCT based method for frame dropping attacks

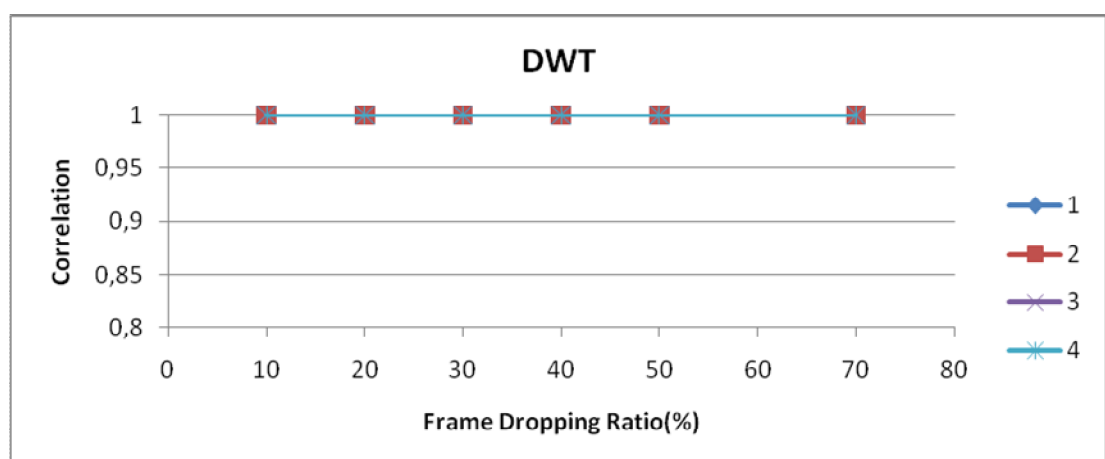


Figure 5.8 Correlation values obtained with the DWT based method for frame dropping attacks

From the results given above, it is seen that the DCT based and the DWT based methods are robust to frame dropping attacks even if the significant number of frames are dropped.

In this thesis, we propose a method in which the watermark data are embedded to original video after dividing into pieces. This scheme achieves better performance. In the literature, there are some methods in which the entire watermark data is embedded to every frame without dividing it. The drawback of these methods is that this same watermark data in every frame is easier to detect by statistically analysis methods to remove from the video. Also, in the literature there are some methods in which the watermark data is divided into pieces and each piece is embedded to different scenes of a video. These methods also have the risk of losing a particular piece of the watermark data by the removal of corresponding scene from the video.

In the second stage of the test, the original video is processed with the proposed hybrid method and same attacks are applied to this video. The results of the tests are presented in Table 5.4 and in Figure 5.9.

Table 5.4 Correlation results of the hybrid method after frame dropping attacks

	<b>Hybrid Method</b>			
	<b>Scenario</b>			
<b>Frame Dropping Ratio %</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
10	1,00	1,00	1,00	1,00
20	1,00	1,00	1,00	1,00
30	1,00	1,00	1,00	1,00
40	1,00	1,00	1,00	1,00
50	1,00	1,00	1,00	1,00
70	1,00	1,00	1,00	1,00

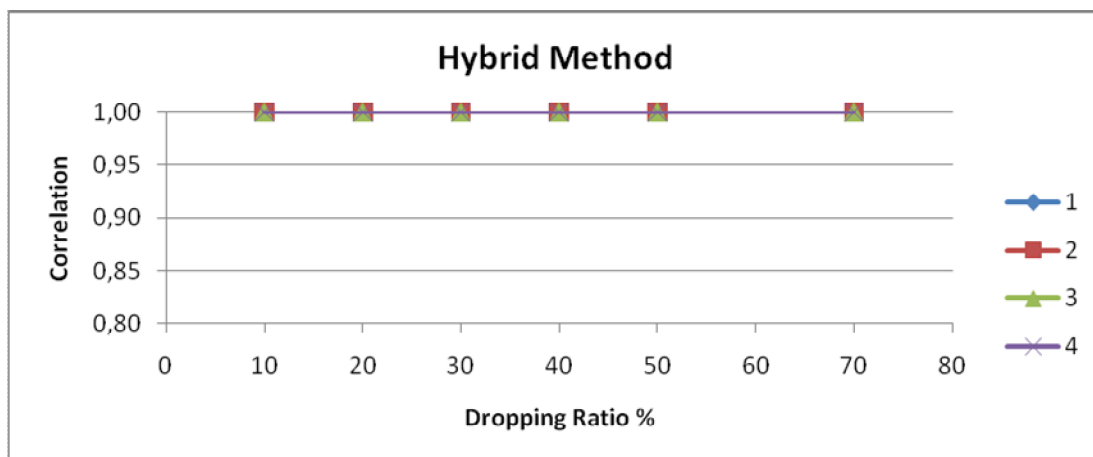


Figure 5.9 Correlation values obtained with the hybrid method for frame dropping attacks

From the table and graphs given above, it is seen that the hybrid method is robust to frame dropping attacks as well. Even for the highest frame dropping ratio attack, correlation with the recovered watermark data and the original data is high. The same watermark piece is embedded in many frames and even after dropping of some frames, entire watermark data can be recovered from the other frames. This scheme achieves as good of a performance as the DWT based method.

### 5.2.3 Frame Averaging Attacks

Frame averaging is one of the significant video watermarking attacks. It removes dynamic composition of the watermarked video. An attacker can collect some successive frames and average them out to generate an output frame. Repeating frame averaging at every frame of watermarked video produces an averaged video in which watermark data may be distorted. The averaged video looks similar to the original video if the averaged frame number is few.

The frame averaging attack was simulated in MATLAB by averaging each frame successively. First test is performed with averaging 2 frames and the second test is performed with averaging 6 frames. The correlation results of the methods are given in Table 5.5 and also Figures 5.10 and 5.11 below.



Table 5.5 Correlation results of DCT based and DWT based methods after frame averaging attacks

	DCT				DWT			
	Scenario				Scenario			
	1	2	3	4	1	2	3	4
2 frames averaged	0,98	0,98	0,97	0,78	1,00	1,00	0,90	0,79
6 frames averaged	0,92	0,81	0,93	0,70	0,86	0,86	0,86	0,58

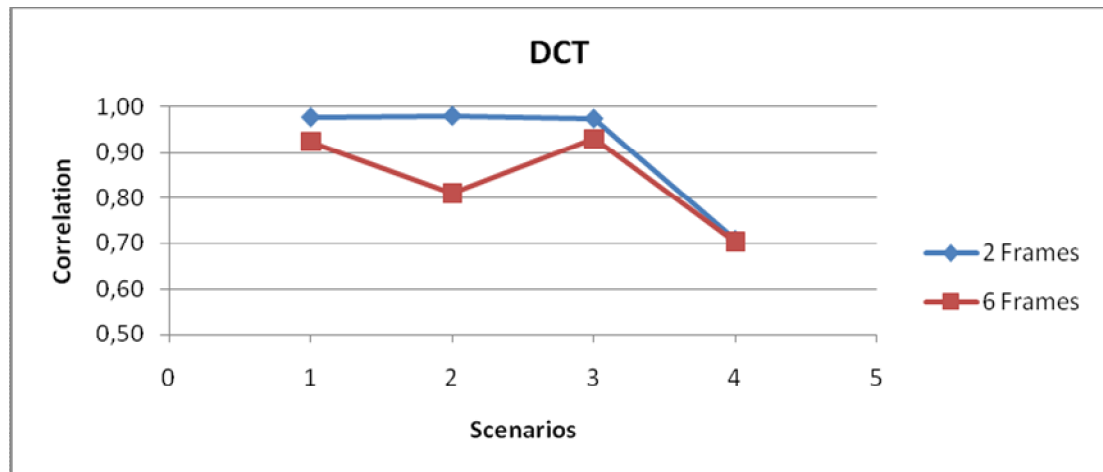


Figure 5.10 Correlation values obtained with the DCT based method for frame averaging attacks

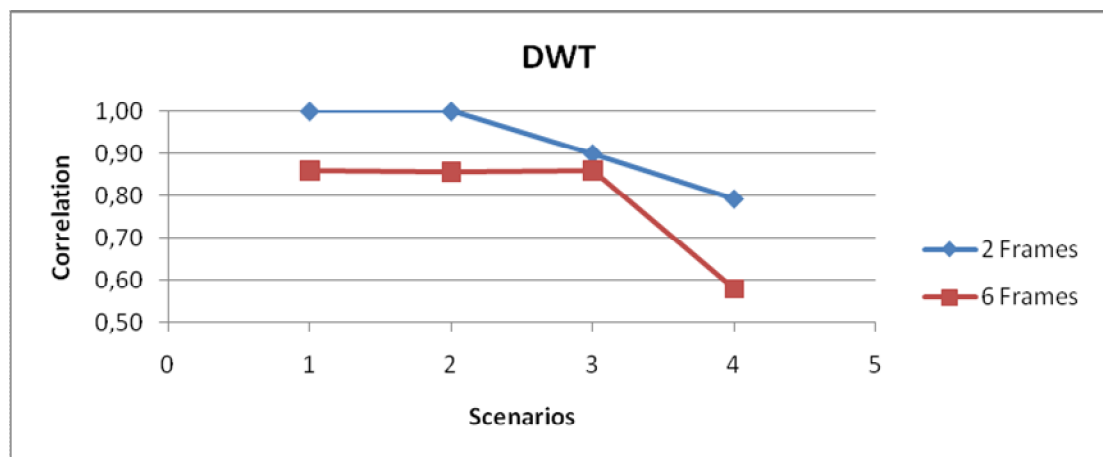


Figure 5.11 Correlation values obtained with the DWT based method for frame averaging attacks

From the tables and graphs given above it is seen that the DCT and DWT based methods are robust against frame averaging.

In the second stage of the test, the original video is processed with the proposed hybrid method and the same frame averaging attacks are applied to this video. The results of the tests are presented in Table 5.7 and also in Figure 5.12.

Table 5.7 Correlation results of the hybrid method after frame averaging attacks

	Hybrid Method			
	Scenario			
	1	2	3	4
2 Frames Averaged	1,00	0,99	1,00	1,00
6 Frames Averaged	1,00	0,99	1,00	0,95

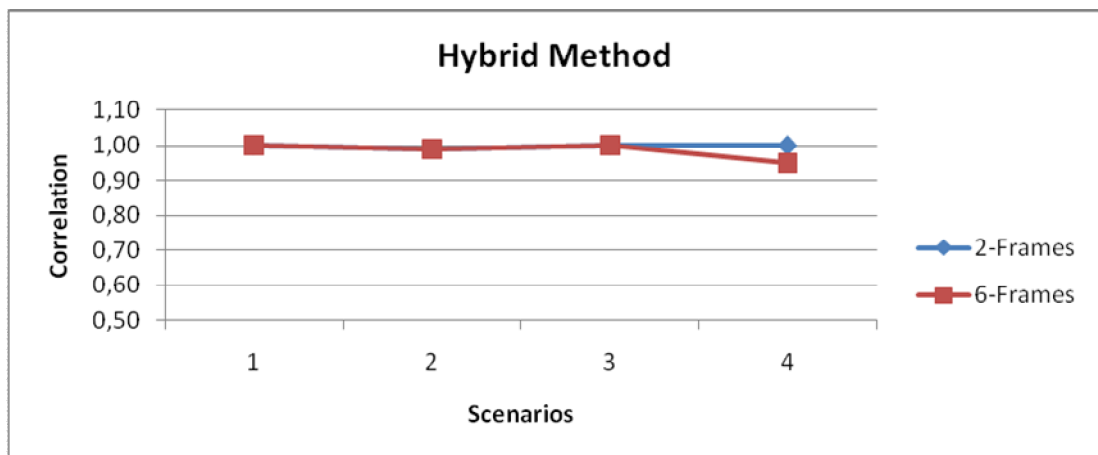


Figure 5.12 Correlation values obtained with the hybrid method for frame averaging attacks

It can be seen from the results above that the hybrid method is more robust to frame averaging attack than both DCT based and DWT based methods. The hybrid method manifests here its power of diversity of watermarking. More accurate reconstruction of watermark bits in the data fusion stage is achieved by the hybrid method.

#### 5.2.4 Video Compression Attacks

The video compression is also one of the common attacks on the watermarked video. The watermarked video may be compressed to distort the watermark as well as to reduce file size of the video. The compression ratio can be adjusted depending on the needs for video. A quality factor is introduced in lossy compression algorithms that are closely related to the compression ratio. With lower quality factors, the video is compressed very much but the visual quality of the video

becomes worse. The watermark is also distorted significantly when the video is compressed with lower quality factors.

In the implemented DCT based watermarking method, watermark is embedded into middle band frequency coefficients to make the method robust to compression attacks. The compression algorithms distort the high frequency band coefficients mostly and middle band coefficients are usually not affected so much. The compression attack is simulated in MATLAB environment and the watermarked video is compressed using two different codecs. These compression algorithms are ‘Cinepak’ and ‘wmv3’. The compressed videos are then used to test the watermarking methods one by one. The performances of the DCT based and DWT based methods against this attack are shown in Table 5.8 and also in Figures 5.13 and 5.14.

Table 5.8 Correlation results of the DCT based and DWT based methods after compression attacks

		DCT				DWT			
		Scenario				Scenario			
Algorithm	Quality Factor	1	2	3	4	1	2	3	4
WMV3	90	0,87	0,70	0,86	0,72	1,00	1,00	1,00	1,00
	100	0,99	0,99	0,97	0,97	1,00	1,00	1,00	1,00
Cinepak	90	0,99	0,98	0,95	0,96	1,00	1,00	1,00	1,00

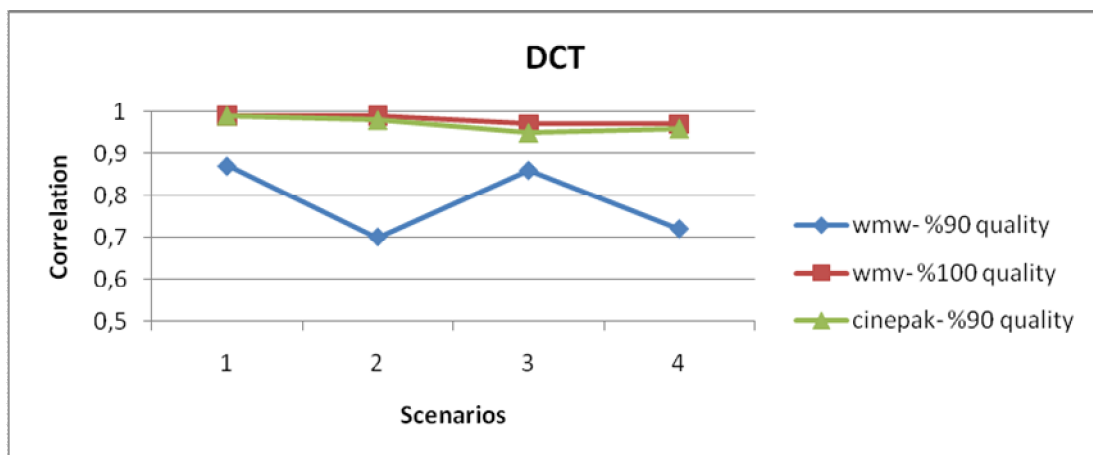


Figure 5.13 Correlation values obtained with the DCT based method for compression attacks

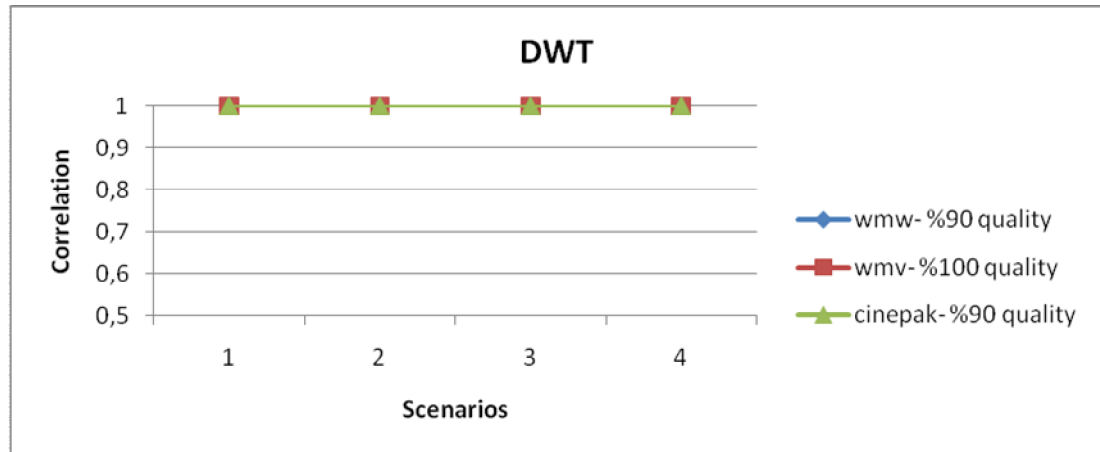


Figure 5.14 Correlation values obtained with the DWT based method for compression attacks

The test results of the proposed hybrid method under video compression attack are presented in Table 5.9 and also in Figure 5.15.

Table 5.9 Correlation results of the hybrid method after compression attacks

		Hybrid Method			
		Scenario			
Algorithm	Quality Factor	1	2	3	4
WMV3	90	1,00	0,99	1,00	1,00
	100	1,00	1,00	1,00	1,00
Cinepak	90	1,00	1,00	1,00	1,00

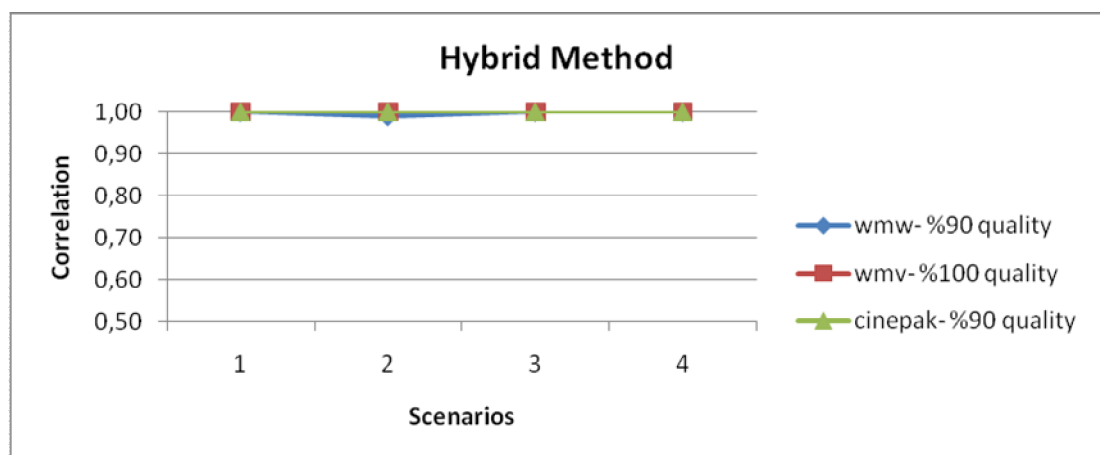


Figure 5.15 Correlation values obtained with the hybrid method for compression attacks

From the results given above, it is seen that the proposed hybrid method is also robust to compression attacks. Its performance is the same as that of the DWT based

method. On the other hand, the DCT based method performs worse because as the quality factor decreases, the DCT middle band coefficients of blocks are also modified by compression attacks and watermark data starts to be distorted.

### 5.2.5 Median Filtering Attacks

Another type of attack to distort watermark in video is to apply filtering operations. Median filtering is a nonlinear operation used in image processing. The aim of this operation is to reduce the noise in images without blurring edges significantly. This property of median filtering makes it favorable for attacking videos. Median filtering the frames of a video may both reduce the noise and distort the watermark data. Therefore, a good watermarking method must be robust to this operation, too. In this thesis, the watermarked video is undergone median filtering operations with a filter size of 3x3. The correlation results obtained by the DCT based and DWT based methods are given in Table 5.10 and Figures 5.16 and 5.17.

Table 5.10 Correlation results of the DCT based and DWT based methods after median filtering attacks

	DCT				DWT			
	Scenario				Scenario			
	1	2	3	4	1	2	3	4
3x3 median filter	0,98	0,93	0,90	0,84	0,00	0,00	0,01	0,20

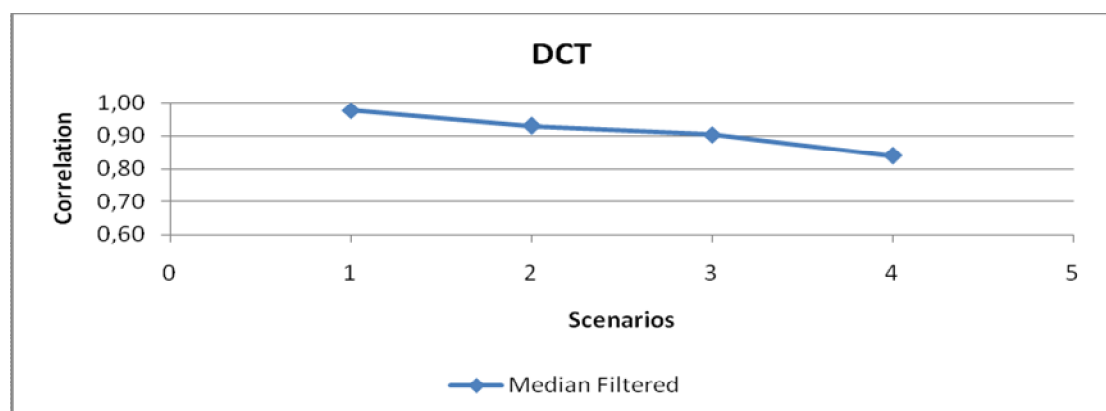


Figure 5.16 Correlation values obtained with the DCT based method for median filtering attacks

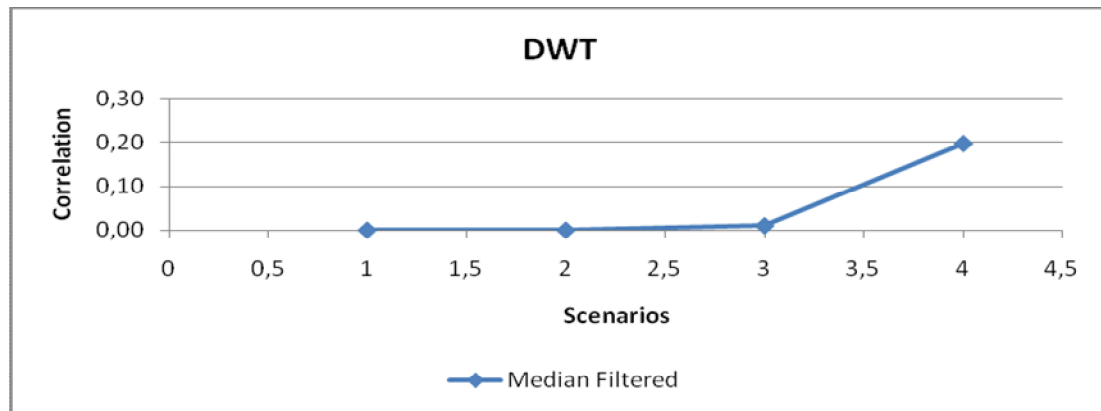


Figure 5.17 Correlation values obtained with the DWT based method for median filtering attacks

In this thesis, the proposed hybrid method contains different transform based algorithms to increase the resistance to the attacks. On frames where DCT is used, watermark data is embedded into middle band frequency coefficients for chosen blocks and, where DWT is applied, the watermark data is embedded into both vertical and horizontal detail bands. The band selection is done by considering the possible attacks and their effects on the frequency bands. Choosing the middle band coefficients for DCT makes the proposed method robust to filtering attacks. Because filtering attacks mainly distort the high frequency band coefficients and middle band coefficients are not affected so much. As to the watermark embedding by DWT, the lower resolution approximation band is not selected for embedding because this band has the most important information about the visual content. Embedding watermark data into this band causes poor imperceptibility. So, horizontal and vertical detail bands can only be selected by the content owner for watermarking. We know that sharp intensity variations such as edges are decomposed into the detail bands. Since the filtering attacks distort the edges in frames, we can expect that coefficients in the detail bands of DWT of an image will be damaged substantially. Thus, the watermark data which are embedded into these regions are also greatly distorted and cannot be recovered completely from frames in which they are embedded by DWT. This explains the poor performance of the DWT based method under the filtering attack.

The test results of the proposed hybrid method under median filtering attack are presented in Table 5.11 and in Figure 5.18.

Table 5.11 Correlation results of the hybrid method after median filter attack

	Hybrid Method			
	Scenario			
	1	2	3	4
3x3 median filter	0,97	0,91	0,97	0,84

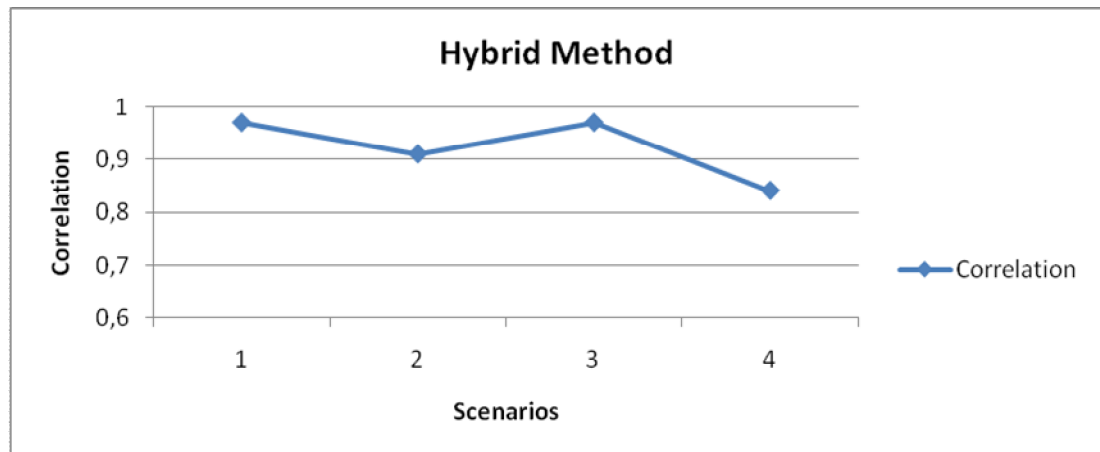


Figure 5.18 Correlation values obtained with the hybrid method for median filter attack

The proposed hybrid method provides good robustness against median filtering attacks. This is obviously due to the support of good recovery results obtained from frames (or half frames) watermarked by the DCT based method. Even any watermark data cannot be recovered from where it is embedded by the DWT based method, there are always copies of them embedded by the DCT based method in the same video. In this sense, filtering may be the best example for a type of attack against which usefulness of the proposed hybrid method is shown convincingly.

### 5.2.6 Image Enhancement Attacks

Attackers can change the appearance of the frames by image enhancement methods. The brightness, intensity, contrast and filtering operations may be applied to a video. These operations may also distort the watermark data. Again, the watermarking method must be robust to these attacks, too.

The watermarked video is undergone intensity and contrast manipulation attacks in the tests. The contrast values of the frames of watermarked video are increased with ‘imadjust’ tool in MATLAB as the first attack. And, as the second attack, image contrasts of all frames are enhanced using histogram equalization with ‘histeq’ tool in MATLAB.

#### 5.2.6.1 Intensity Adjustment Attack

By this attack, the values in intensity image are mapped to new values such that normalized intensity values less than 0.01 and higher than 0.99 are saturated at 0 and 1, respectively. After the intensity adjustment attack the correlation results obtained in the recovering stage are presented in Table 5.12 and also in Figures 5.19 and 5.20.

Table 5.12 Correlation results of the DCT based and DWT based methods after intensity adjustment attack

DCT				DWT			
Scenario				Scenario			
1	2	3	4	1	2	4	5
0,99	0,99	0,99	0,98	1,00	1,00	1,00	1,00

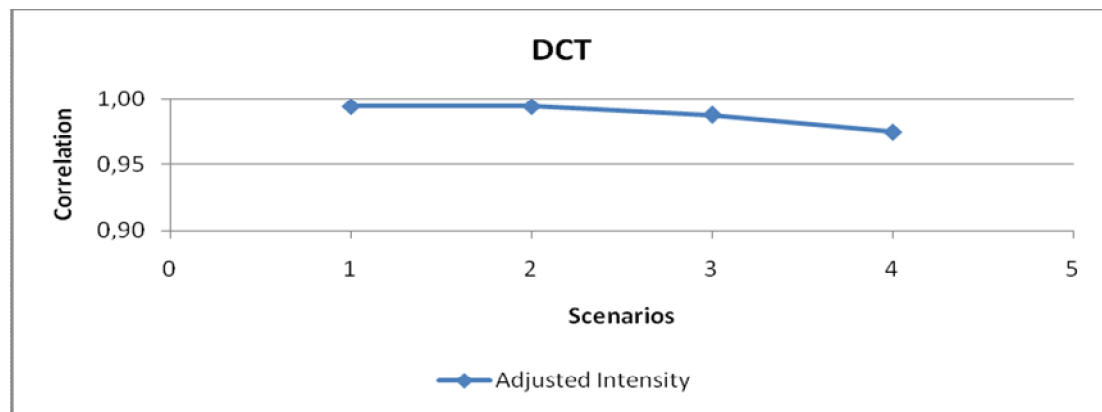


Figure 5.19 Correlation values obtained with the DCT based method for intensity adjustment attack



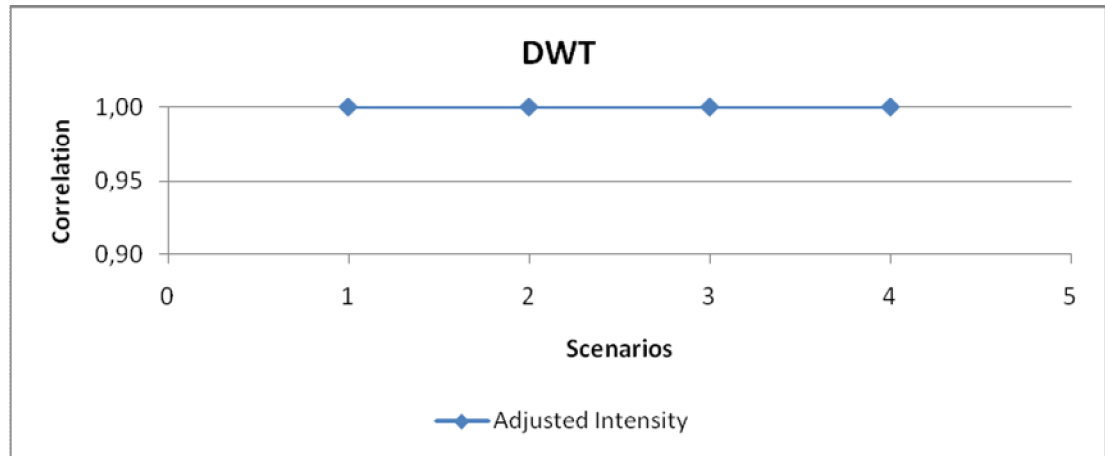


Figure 5.20 Correlation values obtained with the DWT based method for intensity adjustment attack

The robustness of the DCT based and DWT based methods against intensity adjustment attack can be observed from the results given above. Shifting the intensity values of the pixels in frames does not have serious effects on the results of correlations performed to detect watermark data in the recovering stage. This attack causes almost no distortion on the watermark data that is embedded with the DWT based method.

The test results of the proposed hybrid method under intensity adjustment attack are presented in Table 5.13 and also in Figure 5.21.

Table 5.13 Correlation results of the hybrid method after intensity adjustment attack

Hybrid Method			
Scenario			
1	2	3	4
1,00	1,00	1,00	1,00

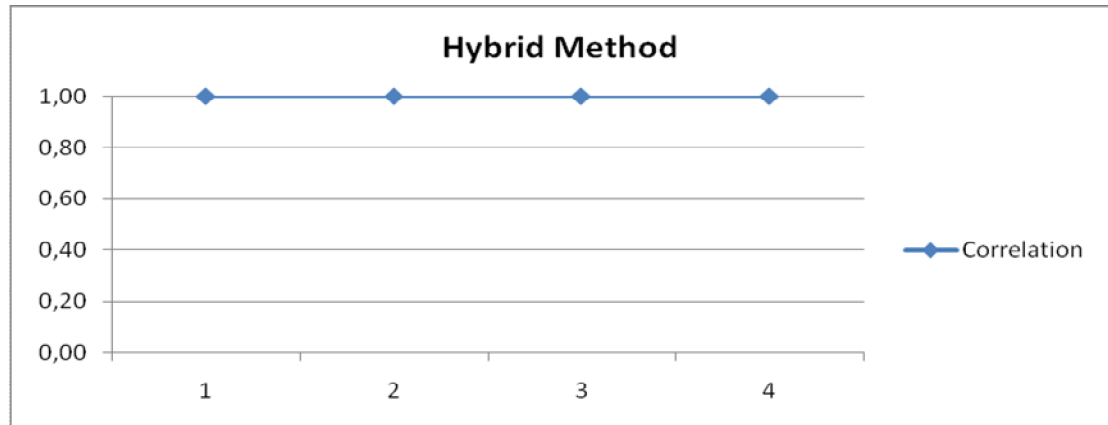


Figure 5.21 Correlation values obtained with the hybrid method for intensity adjustment attack

The robustness of the hybrid method against intensity adjustment attack can be observed from the results given above. This attack causes no distortion on the watermark data embedded by the hybrid method into the test video.

#### 5.2.6.2 Contrast Enhancement Attack

By this attack, frames are mapped to 64 discrete gray levels during histogram equalization for contrast enhancement. A roughly equal number of pixels are mapped to each of the 64 levels in attacked frames. After the contrast enhancement attack the correlation results obtained in the recovering stage are presented in Table 5.14 and also in Figure 5.22 and Figure 5.23 below.

Table 5.14 Correlation results of the DCT based and DWT based methods after contrast enhancement attack

DCT				DWT			
Scenario				Scenario			
1	2	3	4	1	2	3	4
0,99	0,99	0,98	0,98	1,00	1,00	1,00	1,00

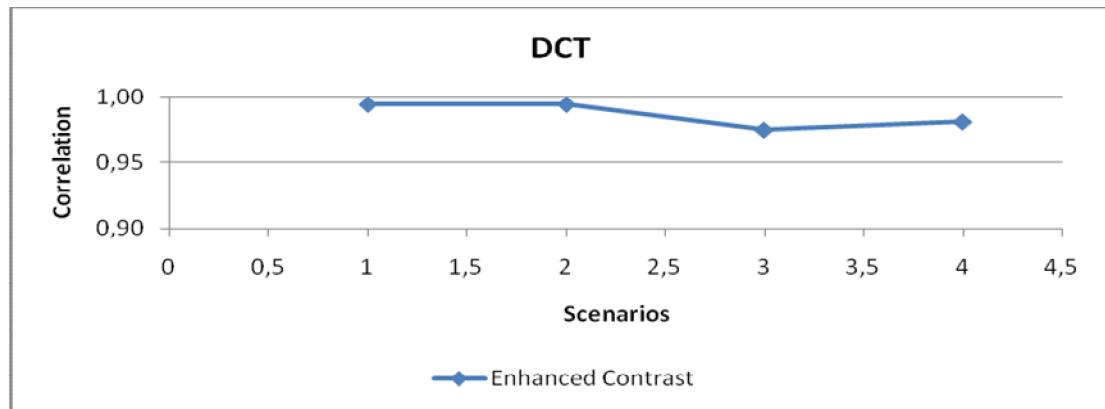


Figure 5.22 Correlation values obtained with the DCT based method for contrast enhancement attack

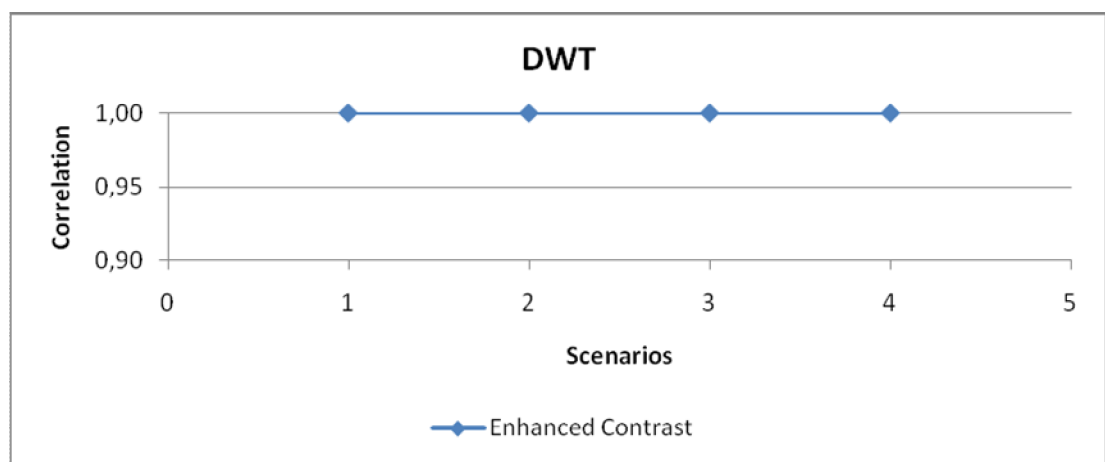


Figure 5.23 Correlation values obtained with the DWT based method for contrast enhancement attack

The effect of this attack on the correlation results is nearly the same as that of the intensity adjustment attack. Enhancing the contrast of the frames in the watermarked video have little effect on the results of correlations performed to detect watermark data in the recovering stage. The robustness of the DCT and DWT based methods against contrast enhancement attack can be observed from the results presented above. This attack causes almost no distortion on the watermark data that are embedded with the DWT based method.

The proposed hybrid method is also tested under the same contrast enhancement attack and Table 5.15 and Figure 5.24 show the results of the tests.

Table 5.15 Correlation results of the hybrid method after contrast enhancement attack

Hybrid Method			
Scenario			
1	2	3	4
1,00	1,00	1,00	1,00

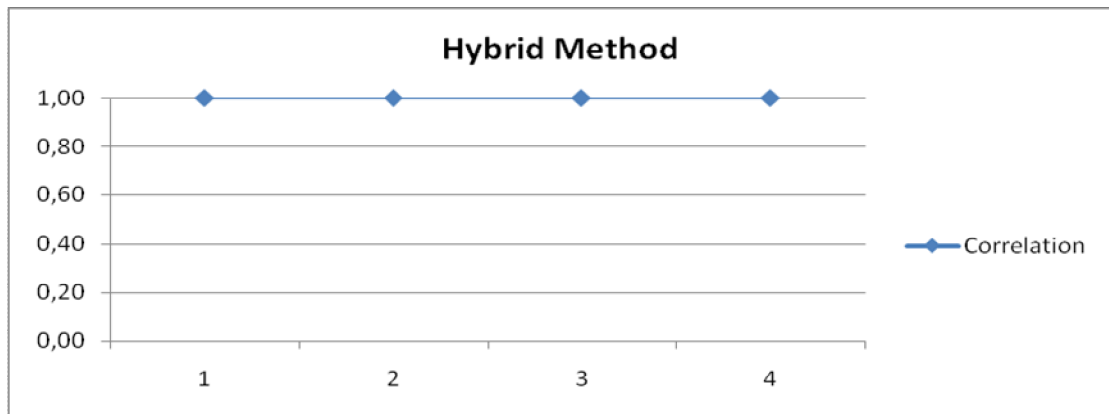


Figure 5.24 Correlation values obtained with the hybrid method for contrast enhancement attack

The robustness of the hybrid method against contrast enhancement attack can also be observed from the results presented above. This attack causes no distortion on the watermark data embedded by the hybrid method into the test video.

### 5.3 Tests for Imperceptibility Requirement

Imperceptibility indicates how invisible the watermark is. In other words, it means the invisibility of watermark being embedded in image or video without degrading the perceptual quality of watermarking. This requirement has a trade off relation with other requirements such as robustness. The more imperceptible method means that the watermarking method is less robust to attacks.

The imperceptibility of the watermarking method can be examined with a parameter which is called Peak Signal-to-Noise ratio (PSNR). The watermarked frames and the original frames are the inputs and this ratio is computed by a software written in MATLAB. The equation of the PSNR formula is given by

$$PSNR = 10 \log(255^2 / MSE)$$

$$MSE = \frac{1}{M \cdot N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |X(i, j) - X^W(i, j)|^2 \quad 5.1$$

where  $X(i, j)$  and  $X^W(i, j)$  are the intensity values of the original video frame and the watermarked video frame, respectively.  $M$  and  $N$  stands for the height and the width of image respectively. Thus the invisibility is measured by calculating the average mean square error (MSE) and the average PSNR. The higher the PSNR, the better the visual quality of video is. In general for digital images or frames, noise with PSNR higher than 30 dB is hardly noticeable.

In watermarking algorithms, the watermark data are embedded to original data by either modifying the pixel values directly in the spatial domain or causing them to change indirectly following an inverse transform from frequency domain in which some frequency band coefficients are modified. In both cases, the watermarked video is different from the original content on the pixel by pixel basis. But the most desired requirement is that embedding watermark data should cause imperceptible changes on video. The imperceptibility of the watermark data is measured using PSNR.

The watermarked videos are tested in MATLAB environment and the PSNR values of each method are given in Table 5.16. The results in the table present the maximum and minimum PSNR values which are obtained from all frames. As the PSNR values show, the quantitative imperceptibilities of all methods are extremely high. Thus, existence of any watermark cannot be visually detected by looking at any frame into which some watermark data was embedded by any of the three methods. In addition, the DCT based frames give better PSNR values than the DWT based frames.

Table 5.16 Minimum and maximum PSNR values of frames in video watermarked by all methods

Method	Scenario							
	1		2		3		4	
	Min	Max	Min	Max	Min	Max	Min	Max
DCT	127,1	128,0	134,0	134,3	123,0	123,0	133,5	134,3
DWT	82,6	84,2	87,9	91,2	85,8	86,5	91,9	Inf
Hybrid	82,6	127,2	87,8	134,3	85,8	123,0	91,9	Inf

The imperceptibility level of the frames watermarked by the DWT in the proposed hybrid method can be increased in our implementation by choosing the detail band in which watermark is to be embedded. The results below were obtained by using both vertical and horizontal detail bands. If the content owner chooses only one of these bands, the imperceptibility increases. But in this case, the robustness of the DWT method becomes worse. There is a tradeoff relation between the requirements of a watermarking algorithm. The more imperceptibility means less robustness.

Table 5.17 gives the imperceptibility measurements of the hybrid method in PSNR value with respect to the chosen detail band in the DWT for embedding watermark. The second and third lines in Table 5.17 are added to visualize the imperceptibility results when a different detail band selection is preferred. In this thesis, all tests were performed by using both horizontal and vertical detail bands.

Table 5.17 Minimum and maximum PSNR values of frames in video watermarked by the hybrid method with respect to selected detail band in DWT

Detail band	Hybrid Method							
	Scenario							
	1		2		3		4	
	Min	Max	Min	Max	Min	Max	Min	Max
horiz. & vert. band	82,6	127,2	87,8	134,3	85,8	123,0	91,9	Inf
horizontal band	89,39	127,22	94,67	134,34	92,68	123,02	98,68	Inf
vertical band	89,39	127,22	94,67	134,34	92,68	123,02	98,68	Inf

The strength constant parameter determines the robustness and imperceptibility requirements of watermarking and these requirements have a tradeoff relation between them. In this thesis, strength constants are chosen as different for the DCT based and DWT based methods. By trial and error, selection of the two strength

constants was made so as to obtain comparable robustness results from these two methods. So, this test technique eventually yielded different imperceptibility results for the methods. Another test technique that could be chosen is to set the imperceptibility values of the methods as equal as possible by tuning the two strength constants and then measure the robustness of the methods against attacks.

When the results are examined, it is seen that minimum PSNR values increase for methods which uses one of the detail bands only. This means that using only one detail band of the DWT makes the watermark data more imperceptible. But the more imperceptibility means less robustness and the content owner has options here for the band(s) to be used by the proposed method. The content owner must determine which watermarking requirement is more important to him/her by considering the purpose of production of video.

In Tables 5.16 and 5.17, there are cells whose values are written as 'Inf'. This is due to the embedding algorithm used in the DWT based method. In this algorithm, only '0' watermark bits are embedded. So, a watermark piece which completely consists of '1' bits causes infinite PSNR value, because the pseudo watermarked frame and original frame is the same since no data is embedded to an original frame matched to such a watermark piece.

The proposed hybrid method has an advantage over the DCT based and DWT based methods when the human visual system based imperceptibility of watermarking is concerned. Table 5.16 gives a measure of static imperceptibility for the methods since video frames are regarded as still images in the computation of PSNR values. The human visual system includes a temporal low pass filter that smoothes out fast changing imagery such as high speed motion and temporal noise. Temporal smoothing effect of the human visual system diminishes the perception of any distortion in watermarked video when a distortion pattern appears less frequently. This is obviously the case in the video watermarked by the hybrid method that produces 3 different distortion patterns (of DCT, DWT, and combined method) for every piece of watermark, appearing in a random order. The same distortion

pattern appears with a longer average period compared to those of the DCT based and DWT based methods that produce one distortion pattern for every piece of watermark. A dynamic imperceptibility compatible to the human visual system is an improvement over the static imperceptibility and favors the hybrid method.

#### 5.4 Capacity Properties

Capacity is the amount of data that can be embedded in a digital data. The digital data may not have a theoretical limit of size, but the amount of watermark data embedded affects the other requirements of the method. Increasing the amount of watermark data embedded in video decreases the visual quality of the video by increasing the distortion in each frame. Therefore, watermarking methods prefer to keep the size of embedded watermark data small in a frame or image.

In this thesis, for frames which are based on DWT, the watermark data are embedded by adding pseudo random sequences cumulatively to the frequency coefficients which are obtained after DWT of original frames. So, more watermark data embedded means less imperceptibility. The PSNR values of these frames decrease if much data is embedded.

For a given video, capacity of the DCT based method can be calculated by the following formula

$$capacity = nMN/B^2 \quad 5.2$$

where  $n$  is the number of frames in video.  $M$  and  $N$  denote the height and the width of frames, respectively.  $B$  stands for the size of a block (usually 8) in which one bit of watermark data is embedded.

The content owner determines the total number of pieces of the watermark data. For a decision, the size and the number of frames in video, and size of the watermark data must be considered. For the video used in the experiments the DCT based capacity per frame is computed as given in Table 5.18.



Table 5.18 DCT based capacities per frame for the test video

	Capacity/Frame
DCT Method (full frame)	4800 Bit
Combined DCT-DWT Method (half frame)	2400 Bit

Note that combined DCT-DWT based capacity of the related frames in hybrid method is half the DCT based full frame capacity per frame because only half (lower) part of those frames can be used to embed a watermark data by DCT based method.

If too much data are embedded to original content, imperceptibility of the watermark decreases. The visual quality of the watermark video is also decreased. The content owner should consider the tradeoff between capacity and imperceptibility requirements.

## CHAPTER SIX

### CONCLUSION AND FUTURE WORK

With the rapid growth of the Internet, digital multimedia can be easily distributed via Internet. Also, digital video is becoming popular due to the widespread use of video-based applications. This also brings some problems beside its advantages which are called as unauthorized copying and distribution of digital video. In recent years, a new term is becoming famous and offered a solution to copyright protection problems. This term is *digital video watermarking*. Theoretically, the basics of the proposed digital video watermarking methods are almost the same; secret information is embedded to original video and this data proves the ownership of the video.

Assuming that aim of using watermarking is to ensure the copyright protection; we can say that the robustness of a watermarking method is the most important concern of the content owner. Therefore, designing and testing a digital video watermarking method with improved robustness to the most probable types of attacks was the main motivation for this study. In this thesis, a hybrid digital video watermarking method is proposed. This hybrid method contains two frequency domain watermarking methods because of their advantages: DCT based and DWT based methods. Thus, the advantages of the both methods are utilized for the proposed method. In addition, some security, robustness and imperceptibility improvement algorithms are included in the proposed method. The new proposed watermarking method is tested to demonstrate that it is robust to attacks. The attacks against which the method is tested are frame dropping, frame averaging, noise addition, compression, median filtering, and image enhancement.

The proposed hybrid method has better robustness compared to the individual methods it merges. This is mainly due to the diversity of different ways of watermarking that allows efficient and more accurate fusion of recovered watermark data from all over the attacked video. The size of a piece of watermark to be

embedded into a frame must not be too small. Otherwise, recovery of such small pieces from an attacked video will be more erroneously reducing the robustness of the method. Improved robustness of the method does not bring objectionable reductions in the capacity and imperceptibility requirements. It is experimentally shown that the hybrid method can resist to all attacks applied successfully.

The proposed method has some advantages over the traditional DCT based and DWT based methods;

- Random block selection algorithm improves the security of the watermark embedded by the DCT based method. The watermark data cannot be recovered without knowing the position and order of the watermarked blocks. This is important for applications that require hiding the watermark from the unauthorized people.
- Detail band selection flexibility introduced for watermarking by the DWT in the hybrid method gives chances to content owner to determine which requirement is the most important for him, either better robustness or better imperceptibility. The watermarked band information is also needed in the recovering stage.
- The hybrid method embeds a piece of watermark in a frame using one of the three methods selected randomly. Each frame is processed with one of the DCT based and DWT based methods or both of them. If some frames processed with one of the methods cannot resist to some attacks, other frames processed with the other methods can be useful in recovering the watermark data. If frames watermarked by both DCT based and DWT based methods are distorted, then frames watermarked by the combined method can provide support in recovering stage.
- Temporal smoothing effect of the human visual system is in favor of the hybrid method. Thus, this method gives better dynamic imperceptibility that is more relevant to video in stream than static imperceptibility that is easy to measure.

During the course of our study, we speculated that the proposed method can be further expanded by adding audio watermarking. The watermark data can be

embedded into audio and video together. Thus, more secure and robust watermarking methods can be designed. This also improves the imperceptibility of the watermark data since less data is required to embed into video frames.

Finally, it is the truth that there is no watermarking method which is resistant to all attacks. But it is also recognized that, by determined research on new watermarking methods, improved robustness against many types of attacks can be achieved.

## REFERENCES

- Bartolini F., Barni, M., Cappellini V., & Piva A. (1998). Mask building for perceptually hiding frequency embedded watermarks. *Proc. Int. Conf. on Image Processing, I*, 450-454.
- Bruyndonckx, O., Quisquater, J.J., & Macq, B. (1995). Spatial method for copyright labeling of digital images. *Proc. IEEE Workshop Nonlinear Signal and Image Processing*, Halkidiki, Greece, June.
- Busch, C., Funk, W., & Wolthusen, S. (1999). Digital watermarking: From concepts to real-time video applications. *IEEE Computer Graphics and Applications*, 19 (1), 25-35.
- Chan Pik-Wah, (2004). Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery, The Chinese University of Hong Kong.
- Chetan K.R, & Raghavendra K. (2010). DWT based blind digital video watermarking scheme for video authentication. *International Journal of Computer Applications*, 4 (10).
- Cox, I., Kilian, J., Leighton, F., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6 (12), 1673-1687.
- Delaigle J., De Vleeschouwer C., & Macq B. (1998). Psychovisual approach to digital picture watermarking. *Journal of Electronic Imaging*, 7 (3), 628-640.
- Fridrich, J. (1998). Applications of data hiding in digital images. *Tutorial of the ISPACS '98 Conference*, Melbourne, Australia.

- Hartung, F., Girod, B. (1999). Watermarking of uncompressed and compressed video. *Signal Processing*, 283–301.
- J. J. K. Q Ruanaidh and T. Pun (1997). Rotation, scale and translation invariant digital image watermarking, *IEEE International Conference on Image Processing, I*, 536-539.
- Joo Lee and Sung-Hwan Jung(2001), A survey of watermarking techniques applied to multimedia. Proceedings, *IEEE International Symposium on Industrial Electronics (ISIE2001)*, 1, 272 -277
- Kundur et al. ( 1997), "A robust digital image watermarking method using wavelet-based fusion," *Int. Conf. on Image Proc.*, 544-547.
- Langelaar, G., & Lagendijk, R. (2001). Optimal differential energy watermarking of dct encoded images and video. *IEEE Transactions on Image Processing*, 148–158.
- M. Kutter and F. Hartung (2000), "Introduction to Watermarking Techniques", in: S. Katzenbeisser, F. Petitcolas (Eds.), *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House.
- Schyndel, R., Tirkel, A., & Osborne, C. (1994). A Digital Watermark. *Proc. IEEE Int. Conf. on Image Processing, II*, 86-90.
- T.Jayamalar and V.Radha(2010), Survey on Digital Video Watermarking Techniques and Attacks on Watermarks., *International Journal of Engineering Science and Technology*, 2(12), 6963-6967
- Wong, P.W. (1998). A public key watermark for image verification and authentication. *Proceedings of the International Conference on Image Processing*.

Xia, X., Boncelet, C., and Arce, G. (1997). A multiresolution watermark for digital images. *Proc. IEEE Int. Conf. on Image Processing, I*, 548-551.

Y. Meng and E. Chang (2003), Image Copy Detection Using DPF", *IS&T/SPIE International Conference on Storage and Retrieval for Media Databases*, San Jose, 176-186.