ROBUST BLIND AND NONBLIND DETECTION FOR DIGITAL WATERMARKING

by

ÇAĞATAY KARABAT

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabanci University

August 2007

ROBUST BLIND AND NON-BLIND DETECTION FOR DIGITAL WATERMARKING

APPROVED BY:

Asst. Prof. Dr. Mehmet KESKİNÖZ …….
(Thesis Advisor)

Dr. A. Murat APOHAN …….

Asst. Prof. Dr. Ayhan BOZKURT …….

Assoc. Prof. Dr. A. Berrin YANIKOĞLU ..…….

Asst. Prof. Dr. Hakan ERDOĞAN …….

DATE OF APPROVAL: 13/08/2007

ROBUST BLIND AND NONBLIND DETECTION FOR DIGITAL WATERMARKING

Çağatay KARABAT

EECS, MS Thesis, 2007

Thesis Supervisor: Mehmet KESKİNÖZ

Keywords: Watermarking, Detection, Robust

ABSTRACT

Rapid development of Internet has greatly increased the need for creation, storage and distribution of digital multimedia products. This raises, however, security concerns due to digital multimedia products high vulnerability to the illegal copying, distribution, manipulation, and other attacks. To remedy these security issues, in literature, the Digital Watermarking has been developed where the information to be hidden is carried by the watermark signal that is transmitted over the host signal.

The capacity of a watermarking system is suffered from much degradation such as channel distortion, filtering, JPEG compression, cropping etc. In addition to those degradations, the host signal interference may even limit the capacity of some systems called blind watermarking systems where host signal is not available to the end-users.

To mitigate these sources of errors and increase the capacity of the system, in this thesis, we develop robust detection methods. For this purpose, we devise block normalization based methods for blind watermarking system in Discrete Cosine Transform domain. We also propose the channel reliability estimation based detector for both blind quantization based watermarking system in Discrete Wavelet Transform domain and non-blind watermarking system in Discrete Cosine Transform domain. Simulation results demonstrate that the developed detection methods improve the capacity, bit error rate performance and the robustness of the systems as compared to existing methods against various distortions and attacks.

SAYISAL DAMGALAMA İÇİN DAYANIKLI GÖZÜ KAPALI VE GÖZÜ KAPALI OLMAYAN SEZİMLEME

Çağatay KARABAT

EECS, Yüksek Lisans Tezi, 2007

Tez Danışmanı: Mehmet KESKİNÖZ

Anahtar Kelimeler: Damgalama, Sezimleme, Dayanıklı

ÖZET

İnternetin hızla gelişmesi, sayısal çoğul ortam ürünlerinin üretilmesi, saklanması ve dağıtılmasına olan ihtiyacı büyük ölçüde arttırmıştır. Bunun yanı sıra, bu artış sayısal çoğul ortam ürünlerinin yasal olmayan kopyalamaya, dağıtım, değiştirme ve diğer saldırılardan etkilenmesi sebebiyle güvenlik sorunlarını da artırmıştır. Literatürde, bu güvenlik sorunlarını çözmek için, saklanacak olan bilginin damga işareti vasıtasıyla taşıyıcı işaret üzerinden gönderildiği Sayısal Damgalama geliştirilmiştir.

Damgalama sisteminin kapasitesi kanal bozunumu, süzgeçleme, JPEG sıkıştırması ve kırpma gibi birçok bozulumdan etkilenmektedir. Bu bozulumlara ek olarak, taşıyıcı işaret girişimi, taşıyıcı işaretin son kullanıcıda mevcut olmadığı gözü kapalı damgalama sistemleri adı verilen sistemlerde kapasiteyi sınırlayabilir.

Bu tezde, bu tip hata kaynaklarını önlemek ve sistemin kapasitesini arttırmak için gürbüz sezimleme yöntemleri geliştirdik. Bu amaçla, ayrık kosünüs dönüşümü alanında gözü kapalı damgalama sistemleri için blok normalize etme yöntemine dayalı yöntemler geliştirdik. Ayrıca, hem ayrık dalgacık dönüşümü alanında nicemleme tabanlı gözü kapalı damgalama sistemi için hem de ayrık kosünüs dönüşümü alanında gözü kapalı olmayan damgalama sistemi için kanal güvenirliği kestirimlerine dayalı sezici önerdik. Benzetim sonuçları, geliştirilen sezimleme yöntemlerinin, çeşitli bozunumlar ve saldırılar altında varolan yöntemlerle karşılaştırıldığında kapasiteyi, bit hata oranı başarımlarını ve gürbüzlüğü arttırdığını göstermektedir.

ACKNOWLEDGEMENTS

I would like to sincerely thank my supervisor, Asst. Prof. Dr. Mehmet Keskinöz for his continuous guidance during my graduate study and for his valuable discussions and detailed reviews during the development of this thesis. My research skills are improved with his advices and challenging questions. I am grateful to my family for encouraging me during my graduate study. In addition, I would like to thank Sabancı University for supporting me with full scholarship.

I wish to also acknowledge the members of my Ms. Thesis committees, Dr. A.Murat Apohan, Asst. Prof. Dr. Hakan Erdoğan, Assoc. Prof. Dr. A.Berrin Yanıkoğlu, Asst. Prof. Dr. Ayhan Bozkurt, for reviewing my thesis and their useful remarks.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AWGN	Additive White Gaussian Noise
BCMLD	Block Coefficient Based Maximum Likelihood Detector
BMLD	Block Maximum Likelihood Detector
BNMLD	Block Normalization Based Maximum Likelihood Detector
BNCRD	Block Normalization Based Correlation Detector
BNCVD	Block Normalization Based Covariance Detector
CRD	Correlation Detector
CVD	Covariance Detector
CRED	Channel Reliability Estimation Based Watermark Detector
DACD	Diversity and Attack Characterization Based Watermark Detector
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
MRD	Majority Rule Based Watermark Detector
MMSE	Minimum Mean Square Error
PSNR	Peak Signal to Noise Ratio
SNR	Signal to Noise Ratio
WDR	Watermark to Document Ratio

TABLE OF CONTENTS

1. INTRODUCTION

The developments in digital technology during the recent years resulted in explosion in the use of digital media products (image, audio and video). Parallel to the deployment of the digital infrastucture and the growth of the internet, the producers are making investments to deliver digital audio, image and video information to its consumers [1]. The audio, image and video industries are distributing their products in digital form. This trend will further be increased with the increasing availability of various advanced multimedia broadcasting services such as pay-per-view, video-on-demand, tele-marketing, electronic commerce, electronic newspapers, digital libraries and web magazines [2]. The problem arises at the same time that the media stored in digital form are vulnerable in a number of ways. First, digital media may be simply copied and redistributed, either legally or illegally, at low cost and with no loss of information. In addition, today's fast computers allow digital media to be easily manipulated, so it is possible to incorporate portions of a digital signal into someone's work without regard for copyright restrictions placed upon the work. For these reasons, the researchers have started looking for techniques that could be used for copy control, proof of ownership, fingerprinting of digital media content and enable copyright enforcement.

Cryptographic techniques are used to overcome these security problems. The cryptography can be defined as the processing of information into an unintelligible (encrypted) form for the purposes of secure transmission. However, these techniques are not sufficient for secure transmission, since the data is not protected as soon as it is used after decryption [3]. While cryptography is about protecting the content of messages, steganography is about concealing their existence. Steganography is a term derived from the Greek words steganos, which means covered, and graphia, which means writing [4]. It is the science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. Examples include

sending a message to a spy by marking certain letters in a newspaper using invisible ink, and adding sub-perceptible echo at certain places in an audio recording. As the purpose of steganography is having a covert communication between two parties whose existence is unknown to a possible attacker, a successful attack consists in detecting the existence of this communication. Watermarking, as opposed to steganography, the existing of the data can be known by the attacker, even in visible watermarking application the embedded watermark can be seen by anyone. In addition, the embedded data is related to the host signal in the watermarking systems; however, the embedded data may not be related to the host signal in the steganography applications. The other difference is that the steganography incorporates with the cryptography. The digital watermarking addresses the growing concerns of the security problems with advanced signal processing strategies. Actually, a digital watermark is an imperceptible, robust, secure message embedded into the multimedia content. The watermark identifies at least one of the media owners, the distributor of the media, the recipient of the media, the origin or status of the data or the transaction dates [5]. It is hidden in the host media in such a way that it is not noticed. The imperceptibility constraint can be achieved by taking into account the properties of the human visual system (HVS) or human audio system (HAS) which makes the system more robust against most types of attacks.

The idea of watermarking has been arised to remedy these concerns. The digital image watermarking is a relatively new discipline, the term only becoming widely known in the early nineties, having first been coined in Komatsu and Tominaga's 1988 paper [6]. During the early nineties, research output was as little as five to ten papers per year, until 1995 when interest in the area increased greatly. Since then, research papers have approximately doubled in number each year [7]. The International Society for Optical Engineering (SPIE) began devoting a specific conference to “Security and Watermarking of Digital Contents” in 1999.

The commercial exploitation of digital watermarking has started with few notable commercial applications until the formation of Digimarc Corporation in 1995. Digimarc has released its first digital image watermarking product in 1996, and now has revenues in excess of ninety million dollars per year and is backed by large industry players such as Adobe, NEC and Sony [8]. Digimarc currently provides watermarking solutions for use in the copyright protection models of many large stock photography firms.

1.1. Digital Watermarking Systems

The watermarking process can be modelled as a secure communication system as shown in Figure 1.1, in which the watermark information is transmitted over the watermark channels within the host signal. These systems are designed for the applications where security of the transmitted information is an additional requirement along with very low bit error probability. The secure communication systems use a pair of secret keys (encryption key and decryption key) at channel encoder to encrypt the transmitted sequence and to decrypt received sequence at the channel decoder respectively. These keys are also used in the watermarking system in the watermark generation and embedding stages that the watermark signal is generated and embedded into the host image. These stages resemble the encoding and modulation stages in the secure communication channel model. In addition, the watermark extraction stage is similar to the demodulation and decoding process, in which the upon reception of a noisy signal the detector forms an estimate of the transmitted data.

An important issue concerning with the digital watermarking systems is the detection techniques. The detectors requiring the original image for watermark detection, such as used in [2], are called non-blind detectors. The other types of watermark detectors are called blind detectors, i.e. used in [9] - [11] which can detect the watermark bits without exploit the original image features. Especially, in case of attacks or strong channel distortions such as filtering, lossy compression, rotation, scaling, cropping etc., or the host signal interference in the spread spectrum watermarking systems, the performance of the detection schemes is very critical for the digital watermarking system for properly recovering the hiding information. In this thesis, we aim at designing watermark detection methods to make the digital watermarking system more robust against pre-mentioned channel distortions and attacks.

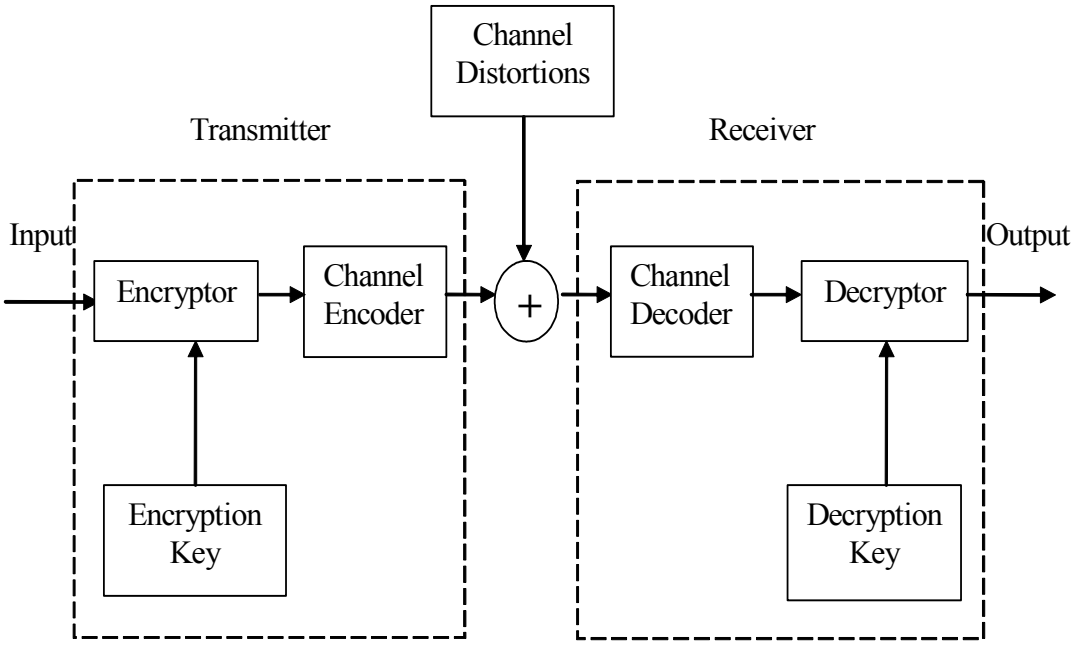

Figure 1.1: Secure Communication Channel Model

In rest of this section, the main processes of a digital watermarking system such as embedding and extraction processes are presented, in an attempt to capture the various systems and configurations that have been presented in the literature. The Figure 1.2 shows a block diagram of a typical watermark embedding system. In its simplest form, such a system has two inputs, the host signal and the watermark data, and a single output, the watermarked version of the signal. This process may be represented by two blocks: an encoder and an embedding function. In the former, watermark data is converted into a form suitable to embed into the host signal. Generally, the watermark signal is converted to the sequence of bits from the set {1,-1} or {0,1}. In the latter, the encoded watermark is embedded into the host signal by using various methods such as additive, additive-multiplicative, and quantization method etc. The Figure 1.3 illustrates a block diagram of a typical watermark extraction process. It is clear from the illustration that the extraction procedure is almost an inverse of the embedding process. Depending on the intended application, two additional stages may be performed during the embedding and extraction process such as perceptual analysis and key generation. These stages are used in the spread spectrum based watermarking system which is

detailly explained in Chapter 2. In addition, note that the host signal is an optional input to the extraction system. The presence or absence of this signal indicates the difference between a non-blind or blind watermarking system respectively. In this thesis, we employ blind watermarking system in Chapter 2 and 3, and non-blind watermarking system in Chapter 4. In the following chapters, the watermark embedding and extraction processes are described in greater detail. The watermarking systems can be named according their properties such as blind, non-blind, imperceptible, etc. as we mentioned in this section. Actually, the classification of watermarking systems is very important. In the next section, we describe criterions used to classify the various watermarking systems.

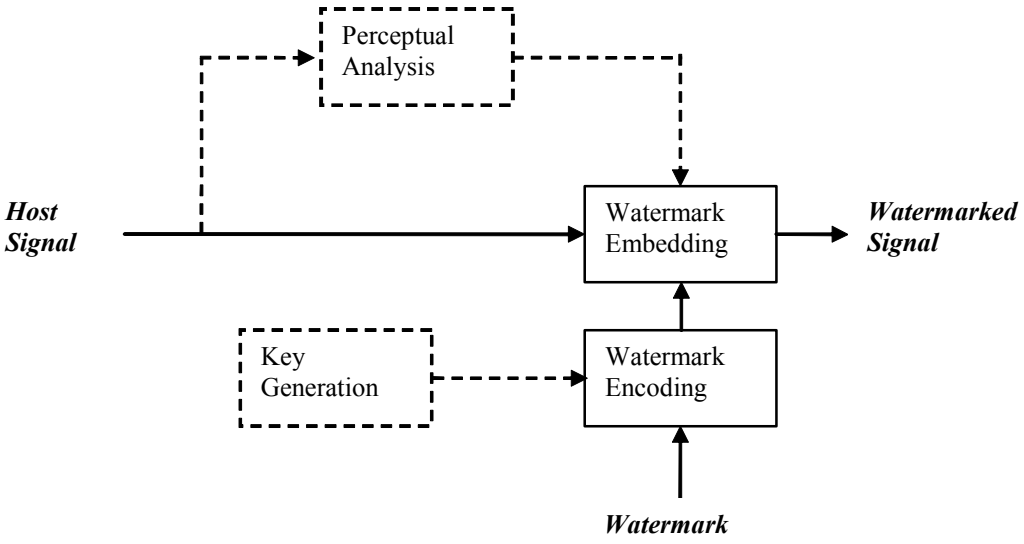

Figure 1.2: Typical Digital Watermark Embedding System. Dashed Lines Indicates Optional Blocks.

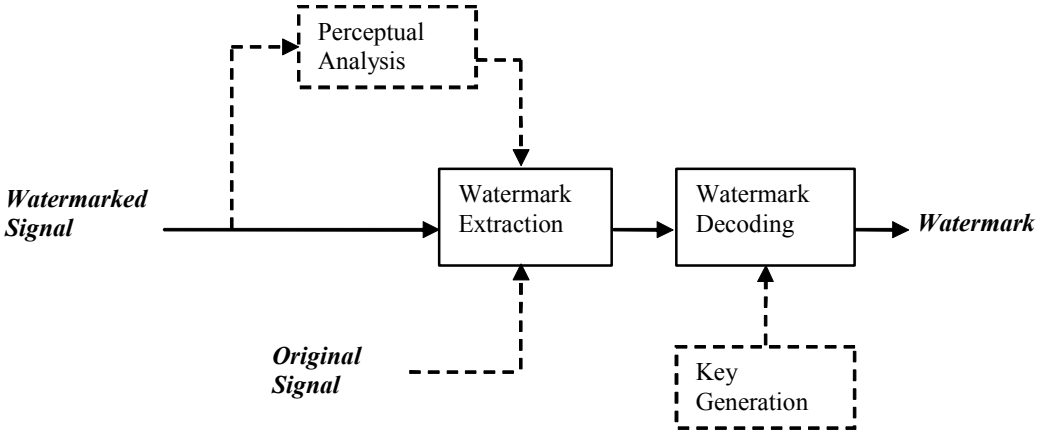

Figure 1.3: Typical Digital Watermark Extraction System. Dashed Lines Indicates Optional Blocks.

1.2. Classification of Digital Watermarking Techniques

This section provides a general classification of existing digital watermarking systems, as shown in the Figure 1.4, based on the following five criteria:

1) Host Signal Type (images, video, audio, and text),
2) Based on Applications (robust, fragile, and semi-fragile),
3) Perceptibility (visible and invisible),
4) Embedding Domain (spatial and transform),
5) Availability of Host Signal at the Receiver (non-blind and blind).

1.2.1. Classification Based on Host Media Type

The most of the digital watermarking research is focused on digital images compared with the other host media types i.e. video, audio, image and text. This is due to the fact that the performance evaluation of a digital watermarking system for digital images is relatively easier than digital audio and video; because the performance

evaluation of a watermark embedding scheme for audio or video generally requires subjective testing. Digital watermarking techniques based on host signal type can be divided into four sub-groups [1]-[12]:

1. Digital Watermarking in Images
2. Digital Watermarking in Video
3. Digital Watermarking in Audio
4. Digital Watermarking in Text

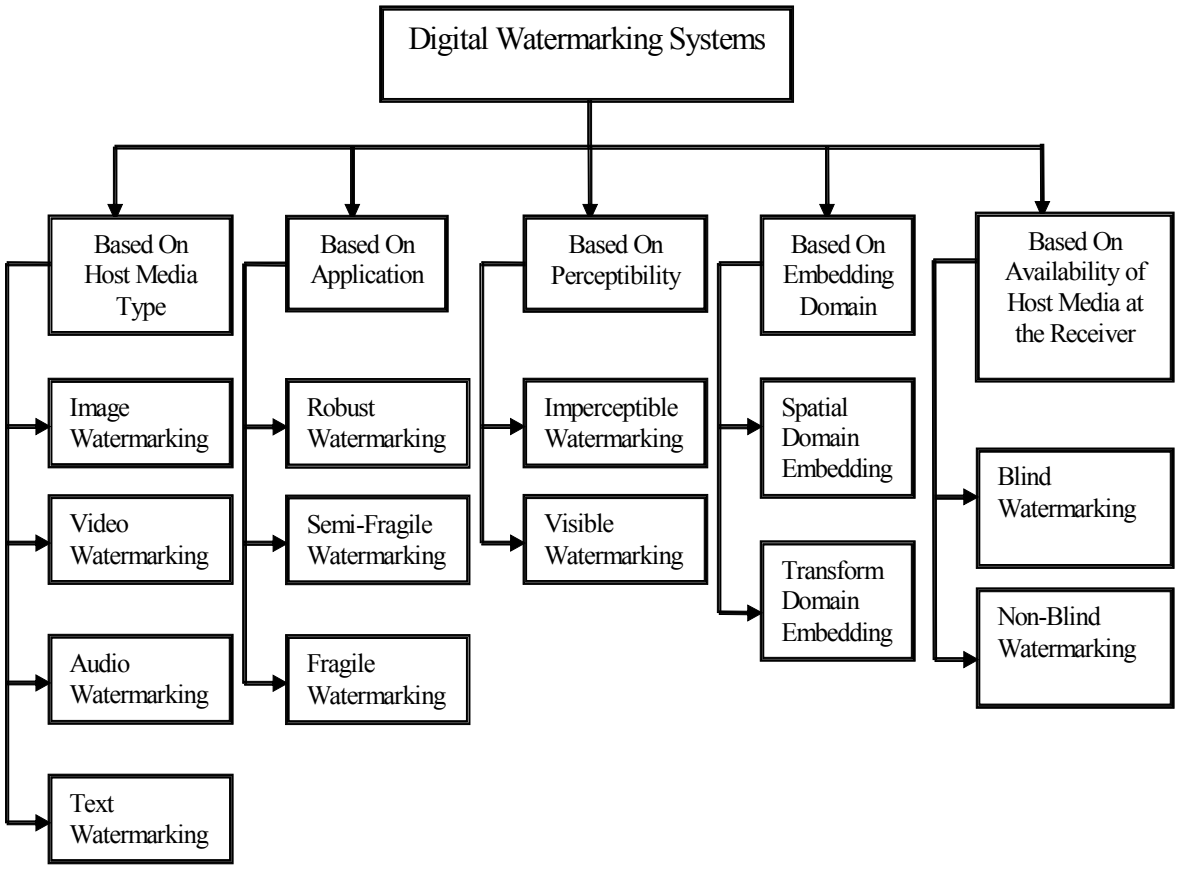

Figure 1.4 : General Classification of Digital Watermarking Systems

1.2.2. Classification Based on Digital Watermarking Applications

The performance based on robustness, capacity and fidelity of a digital watermarking systems depend on the application of interest. For example, copyrights protection applications require a robust watermarking [14], [15], where as content verification applications need a fragile watermarking [7]. Similarly, fingerprinting needs a semi-fragile watermarking [16] and [17]. Therefore, existing digital watermarking systems can be classified into three sub-groups based on the application of interest:

1. Robust Digital Watermarking
2. Fragile Digital Watermarking
3. Semi-Fragile Digital Watermarking

1.2.3. Classification Based on Perceptibility

Existing digital watermarking systems can be divided into two main categories based on the perceptibility (fidelity) of embedded watermark [7] and [18] that is,

1. Imperceptible Watermark Embedding
2. Visible Watermark Embedding

Imperceptible watermark embedding implies that embedded watermark is invisible (in case of image, video, and text host media) and inaudible (for audio host media). Imperceptible watermark embedding schemes are more common than the visible watermark embedding schemes [19]. Imperceptible watermark embedding schemes exploit the Human Visual System (HVS) and Human Audio System (HAS) characteristics to ensure imperceptibility of the embedded watermark. Visible watermark embedding schemes are generally used to imprint visible logo in digital images or video.

1.2.4. Classification Based on Watermark Embedding Domain

Existing digital watermarking sytems can be classified into two major categories based on embedding domain of the watermark, that is,

1. Digital Watermarking in Spatial/Time Domain
2. Digital Watermarking in Transform Domain

Least significant bit (LSB) and most significant bit (MSB) encoding are the most common digital watermarking techniques of spatial domain digital watermarking schemes [1]. The spatial domain digital watermarking systems were very popular among the data hiding community. However, transform domain techniques, especially DWT domain techniques, are more commonly used digital watermarking systems nowadays due to their robustness of various channel distortions and attacks. Discrete cosine transform (DCT), discrete wavelet transform (DWT), and discrete fourier transform (DFT) are the most commonly used transforms for data embedding process. The most of the DCT-based image digital watermarking systems commonly use *8x8* DCT block of image for host data transformation. Then, watermark is embedded by modifying DCT-coefficients according to human visual system. In DWT-based digital watermarking algorithms, the host data is first decomposed into subbands using DWT, then for data embedding discrete wavelet coefficients in the selected subbands are modified based on human perceptual model. DFT-based algorithms are also common for audio digital watermarking schemes. The robust digital watermarking systems should be robust against the common channel distortions such as AWGN, lossy compression or attacks such cropping, rotation, mean and median filtering etc.

1.2.5. Classification Based on Availability of Host Signal at the Receiver

The digital watermarking systems based on the host signal availability at receiver side can be classified in following categories,

1. Non-Blind (Private) Digital Watermarking System
2. Blind Digital (Public) Watermarking System

The digital watermarking systems, which have non-blind watermark detection scheme, require that the original signal be present at the receiver side in order to extract watermark information. In contrast, a digital watermarking system which employs blind watermark detector, does not require access to the original signal in order to decode the watermark. A blind system, for example, would typically be used to send watermarks to the end-users of a host signal, whereas a non-blind watermarking system would intuitively be more secure [20]. The non-blind watermarking may not be practical for applications where a large number or volume of host signals are generated, or for applications where watermark data is intended for a large number of end-users to decode. Examples of such applications are high definition digital television (HDTV) or broadcast digital radio. In these cases, it is not feasible to transmit both the original and watermarked versions of the host signal. However, non-blind watermarking may be suitable for other applications, such as on-line stock photography shops, where a non-blind library of digital media is maintained by the business, and watermarked versions sold to consumers. In addition, these systems are suitable for used in the digital watermarking applications like content authentication, ownership verification, etc. The blind and non-blind watermarking applications are explained in the following section in greater detail.

1.3. Applications of Digital Watermarking

Watermarking can be used in a wide variety of applications. The application area is another criterion to categorize the digital watermarking systems. In this section, we examine six actual digital watermarking applications. The general watermarking applications include ownership protection, content authentication and tamper detection, fingerprinting or labelling, copy & access control, hidden annotation and broadcast monitoring as explained in the following sub-sections detailly.

1.3.1. Ownership Protection

The robust digital watermarking systems can be used for ownership protection of the multimedia data. Digital watermarking systems used for ownership protection is expected to be robust against strong attacks and channel distortions. In case of dispute over ownership of the host data, embedded information can be used as a proof to identify the true owner of the host data. The digital watermarking systems intended for ownership protection required to have low probability of error and false alarm rate. In general, digital watermarking systems are used for ownership protection requires relatively lower embedding capacity [7].

1.3.2. Content Authentication and Tampering Detection

In content authentication and tamper detection applications, robustness and undetectability are not the main concerns. In general, fragile digital watermarking systems can be used for such applications. A set of secondary data (watermark) is embedded into the host data beforehand, and later is used to determine whether the host data is tampered or not. The robustness against removing the watermark or making it undetectable is not a concern [7], [21] . However, forging a valid authentication watermark in an unauthorized or tampered data source must be prevented. In practical applications, it is also desirable to locate the tampering and to distinguish some changes, such as the non-content change is made by lossy compression, from some other changes such as content tampering. The embedding capacity has to be high in general to accommodate these needs. The detection should be performed without the original unwatermarked copy because either this original data is unavailable or its integrity has not been established yet. Hence, the blind watermark detection schemes are used in these systems generally.

1.3.3. Fingerprinting or Labeling

The owner or distributor of multimedia contents uses fingerprinting or labelling to trace the illegal copies. The watermark in this application is used to trace the originator or recipients of a particular copy of multimedia source. For such applications, content owner or distributor embed a unique bit sequence such as fingerprint, label, or serial number in each copy of the distributed data before distributing to each customer. Even if a copy is made illegally, the source can be easily tracked since each original copy had a unique bit sequence embedded into it. Although these systems do not require high embedding capacity in general, they should be robust against intentional and unintentional attacks, more specifically collusion attacks where colluders combine several copies with the same content but different fingerprints to remove or attenuate the original fingerprints [16], [17]. Also, it does require robustness against active adversary attacks. Actually, in these applications, digital watermarking systems should be semi-fragile.

1.3.4. Copy Control & Access Control

Embedded watermark in the host multimedia data can be used to control the copying device for unauthorized copy prevention [7], or can be used in access control applications. For this purpose, a watermark detector is generally integrated in the recording or playback system, such as, DVD copy control scheme proposed in [24]. For such applications, watermarking systems should be robust against all channel distortions and attacks especailly removal type attacks. Moreover, digital watermarking systems designed for copy control intend should use a blind watermark detection scheme and generally requires low data embedding capacity.

1.3.5. Hidden Annotation

The embedded watermark in this application is expected to convey as many bits as possible without the use of original unmarked copy in detection. Therefore, in these

applications, the digital watermarking system should use blind watermark detection scheme [7] . While the robustness against intentional attack is not required, a certain degree of robustness against common processing like lossy compression may be desired. For example; the names of the patients can be printed on the X-ray reports and MRI scans using the techniques of visible digital watermarking systems. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster.

1.3.6. Broadcast Monitoring

A watermark is embedded into data, for example, commercials or copyrighted materials [25], to allow automatic monitoring of the data in the broadcasting channels. For example, a commercial advertisement may be watermarked by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring systems can then receive broadcasts and check for these watermarks, identifying when and where each clip appears. This proves very helpful for the advertisers as they actually pay for only the number of times the advertisement was actually relayed. For such applications digital watermarking system should be robust against channel distortions and attacks and requires a blind detection scheme. Furthermore, such applications require low watermark embedding capacity.

1.4. Requirements for Digital Watermarking Systems

It is important to define the requirements of a digital watermarking system because they can be used to compare different systems. The importance of each property depends on the requirements of the application. However, importance of each property depends on the type of the application and the role of data embedding in the application. For example, if we are evaluating the performance of an audio watermarking system for copy control application, we may need to check the robustness of short time energy ratio that adversary might use for attack. However, such robustness might be irrelevant for broadcast monitoring applications. Therefore, the performance

of any watermarking system should be evaluated based on the underlying application. The most three important requirements of the digital watermarking systems are robustness, imperceptibility and the hiding capacity. These properties are detailly explained in the following sub-sections.

1.4.1. Robustness

The one of the important requirements for the digital watermarking systems is the robustness. Once the watermark is embedded into a host signal, distortions and attacks degradate watermarked signal before, during, and after distribution across the communication channel. In general, a digital watermarking system is supposed to be robust against common data manipulations, such as lossy compression, digital-to-analog conversion, rescaling, requantization, resampling, low-pass filtering, median filtering and data format conversion etc. It is also suppose to robust against active adversary attacks, such as noise and collusion attacks etc. The robustness measures the ability of embedded watermark to withstand against intentional and unintentional attacks. Unintentional attacks generally include common data processing operations i.e. compression, digital-to-analog conversion, resampling, requantization etc, where as, intentional attacks cover a broad range of degradations [21]-[23], for example, noise addition, scaling, rotation (for image and video watermarking schemes), cropping, low-pass filtering, high-pass filtering, mean and median filtering etc.

1.4.2. Imperceptibility

The imperceptibility is another important property of all perceptual based digital watermarking systems [7]. To meet this constraint, the perceptual distortion introduced by the watermark is kept below the threshold of human visual system (HVS) for video and image watermarking systems and human auditory system (HAS) for audio watermarking systems. This means that the perceived “quality” of the host signal should not be distorted by the presence of the watermark. Ideally, a typical user should not be able to differentiate between watermarked and unwatermarked signals. There are two

reasons why it is important to ensure that the watermarked signal is imperceptible. First of all, the presence or absence of a watermark should not detract from the primary purpose of the host signal, that of conveying high-quality audio or visual information. In addition, perceptible distortion may indicate the presence of a watermark, and perhaps its precise location within a host signal. This knowledge may be used by a malicious party to distort, replace, or remove the watermark data.

1.4.3. Hiding Capacity

The hiding capacity refers to the amount of information that a watermarking system can successfully embed without introducing perceptual distortion. The need for this property is application dependent, for example, a watermarking system designed for copyright protection or copy control application does not require high data embedding capacity because only a few bits of information are sufficient for this application. Whereas, a data embedding scheme for broadcast monitoring applications requires to embed relatively large amount of data.

1.5. Thesis Contributions

In this thesis, we try to develop robust watermark detection schemes for various digital image watermarking systems. First, we address the blind detection methods that are used in the spread spectrum based watermarking systems. They have the host image interference problem. In the literature, the existing blind detectors for these systems regard the host signal interference as a noise and employ statistical characterization of the host image. These systems reduce the interference by developing optimal or sub-optimal detectors in the maximum likelihood (ML) sense and by using long pseudo random sequences. However, their performance is not satisfactory even in the absence of the channel distortion and attack due to the interference. We propose the block normalization method to reduce the host image interference. Then, we employ this method in various types of watermark detectors such as correlation, covariance and ML detectors based on Bayes tests with certain underlying distributions. Hence, we decrease

the bit error rate (BER) of the recovered watermark by employing the proposed block normalization method. For example, we approximately decrease the BER from 10^{-1} to 10^{-3} for the covariance detector by applying the proposed method when the insertion strength is set to 0.4 and the watermark length is 256. In addition, the proposed method approximately decreases the BER from 10^{-2} to 10^{-4} for the ML estimation based detectors when the insertion strength is set to 0.4 and the watermark length is 256. Moreover, we approximately 4 times increase the hiding capacity of the system, which is very critical in most of the applications.

Then, we focus on the developing a new detection scheme for quantization based watermarking system in DWT domain. The existing diversity and attack characterization based detector (DACD) , simultaneously, uses the reference watermarks to characterize the watermark channel, and the information watermarks to transmit the hidden information. However, they assume that all the watermark estimates are reliable. Hence, they do not eliminate the unreliable estimates deteriorating performance of the system against severe degradations. We propose a new blind detection method that is called channel reliability estimation based detector (CRED). In the proposed scheme, first, the reliabilities of the watermark channels are estimated. Then, channel parameters are found by using the first and second order statistics of the reliabilities and reliable watermark channels are determined by the proposed threshold method. Finally, the information watermark is recovered by using estimated information watermarks from the reliable watermark channels. The use of communication theory principles such as coefficient diversity, reference patterns and threshold broadens the class of distortions for which the watermark is robust. The proposed CRED detector can attain the target correlation coefficient at low SNRs. For example; when we set the target correlation coefficient to 0,8 , the proposed CRED detector achieves 3 dB SNR gain in comparison to the DACD detector. On the other hand, it achieves 9 dB SNR gain in comparison to the MRD detector. Furthermore, if the receiver employs the proposed detector, the transmitter can more aggressively compress the watermarked signal with lower JPEG quality factor. Thus, it increases the amount of information to be hided. For example, when we set the target correlation coefficient to 0.8; the proposed detector decreases the JPEG quality factor from 56 to 46 in comparison to the DACD detector. On the other hand, it decreases the quality factor from 91 to 46 in comparison to the MRD detector.

Finally, we employ the detectors, which are used in the quantization based watermarking system, in the non-blind watermarking system in DCT domain. Our goal is to both characterize the channel distortions and attacks by employing the proposed channel reliability estimation based detector and compensate the effects of them by using image restoration algorithms. The proposed channel reliability estimation based detector decreases BER and increases correlation coefficient of the recovered watermark. Hence, the proposed detector shows superior performance and demonstrates robustness to broad class of pre-mentioned channel distortions and attacks. For example; when we set the target correlation coefficient to 0,9 , the proposed CRED detector achieves 3 dB SNR gain in comparison to the DACD detector. On the other hand, it achieves 5 dB SNR gain in comparison to the MRD detector. In addition, when we set the target correlation coefficient to 0.9; the proposed detector decreases the JPEG quality factor from 17 to 14 in comparison to the DACD detector. On the other hand, it decreases the quality factor from 22 to 14 in comparison to the MRD detector. Furthermore, we apply the image restoration algorithms to the degradated watermarked image in order to decrease the defects of the degradations and increase the detection performance. We first apply Wiener filtering for restoring the image. In this case, when we set the target BER to 10^{-4}, the proposed detector achieves 4 dB SNR gain in comparison to the DACD detector. On the other hand, it achieves 7 dB SNR gain in comparison to the MRD detector. Then, we apply LR algorithm. . In that case, when we set the target BER to 10^{-4}, the proposed detector achieves 3 dB SNR gain in comparison to the DACD detector. It also achieves 6 dB SNR gain in comparison to the MRD detector. Finally, we employ regularized filter. To evaluate the performance, we set the target BER to 10^{-4}, the proposed detector achieves 3 dB SNR gain in comparison to the DACD detector. In addition, it achieves 7 dB SNR gain in comparison to the MRD detector. We can conclude from the simulation results that the proposed CRED detector achieves the maximum performance improvement.

1.6. Thesis Organization

The rest of the thesis is organized as follows: The Chapter 2 starts with the introduction to the spread spectrum based watermarking systems in DCT domain. It

presents the existing watermark detectors and the proposed block normalization method for blind detection schemes for these systems. Finally, it presents the simulation results and the conclusions. Chapter 3 explains the quantization based watermarking system in DWT domain and addresses the basic detection problems of this system against various degradations. Next, the existing detection methods and the proposed detection method are explained. Finally, the performance of the detectors are tested and compared with the simulation results at the last section of this chapter. The Chapter 4, first, explains the non-blind digital watermarking system in DCT domain. We employ the watermark detection methods explained in Chapter 3 and evaluate their performances in this non-blind watermarking system against severe channel distortions and attacks. Finally, we conclude our work in Chapter 5 with remarks and suggestion for possible research directions.

2. ROBUST BLIND DETECTION FOR DCT DOMAIN SPREAD SPECTRUM WATERMARKING SYSTEM

In this chapter, first, we present the spread spectrum based digital watermarking system in *8x8* block DCT domain in Section 2.1. We address the basic interference problems of the blind detectors in these systems in Section 2.2. Then, we introduce the watermark detection method used in these systems and the proposed detection methods in Sections 2.3 and 2.4 respectively. Finally, we test and compare the performance of the detectors with the simulation results and give conclusions in Sections 2.5 and 2.6 respectively.

2.1. Spread Spectrum Watermarking for Still Images

This section introduces the spread spectrum watermarking system in *8x8* block DCT domain for still images. It covers the generic processes of the watermarking system such as watermark embedding and extraction processes.

2.1.1. Watermark Embedding Process

In all the subsequent analysis, $X[i, j]$ and $Y[i, j]$ denote host and watermarked image in spatial domain respectively. Also, $x[u, v]$ and $y[u, v]$ denote host and watermarked image in DCT domain respectively.

For embedding process which are shown in detail in Figure 2.1 , we first compute *8x8* block DCT of host image $X[i, j]$. Then, binary antipodal message

sequence $\vec{\mathbf{b}} = \left[b_1, b_2, ..., b_{T_b} \right]$ of length T_b, whose elements are from the set $\{\pm 1\}$, is randomly generated. Each message bit is repeated *M* times to obtain repetition-coded message vector $\vec{\mathbf{b}}_c$ of length $T_c = T_b \times M$. In the spread-spectrum modulation stage, we randomly generate a spread-spectrum sequence $\vec{\mathbf{p}}_c$ whose elements are from the set $\{\pm 1\}$ and length is T_c using the security key K_1. Then, we multiply repetition coded bit sequence $\vec{\mathbf{b}}_c$ with the pseudo-random sequence $\vec{\mathbf{p}}_c$ to obtain the watermark sequence $\vec{\mathbf{w}}_c$. To achieve a trade-off between perceptual transparency and robustness, we select and mark only 16 band-pass coefficients for each *8x8* DCT block, as illustrated in Figure 2.2 . We use key K_2 to distribute $\vec{\mathbf{w}}_c$ randomly over the all band-pass coefficients obtained in the block DCT transformed image in order to increase the confidentiality. The unmarked coefficients are filled with zeros, and consequently the watermark mask $w[u,v]$ of size *N*x*N* is generated in the DCT domain. During the watermark embedding stage, we shape the watermarked coefficients according to the human visual system (HVS) using the perceptual mask $m[u,v]$ which is derived and explained in [5], [27]-[29]. We also introduce the perceptual mask in detail in Section 2.1.2. Finally, we embed the watermark in DCT domain as follow:

$$y[u,v] = x[u,v]\left(1 + \phi[u,v]w[u,v]\right) \tag{2.1}$$

where $\phi[u,v] = \gamma m[u,v]$ is the insertion strength matrix, $m[u,v]$ denotes the perceptual mask, and γ denotes the insertion coefficient. Hence, we adapt the watermark embedding process adaptively according to the HVS by employing a different insertion strength coefficient to each of the DCT coefficient to be marked.

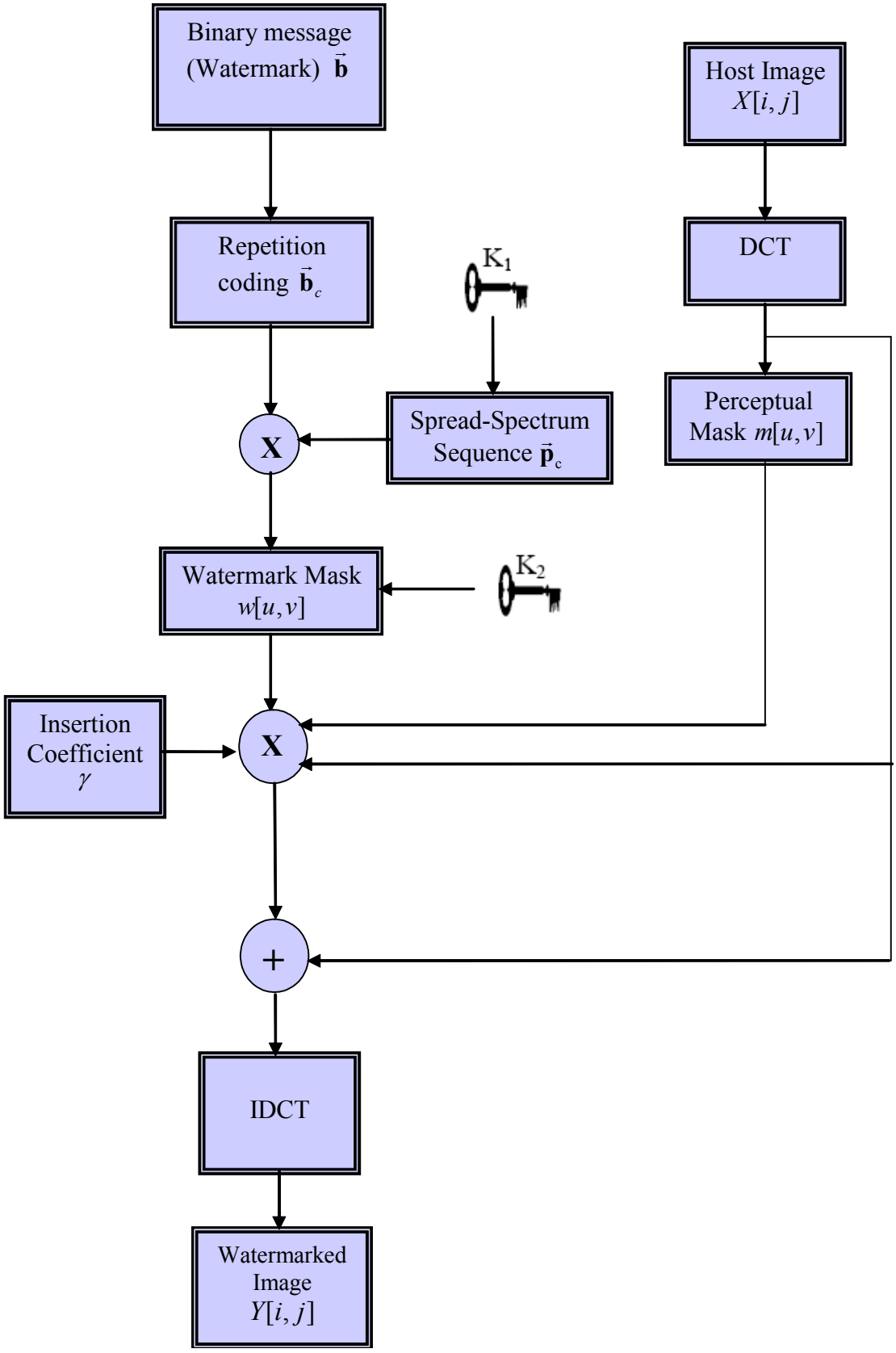

Figure 2.1: Watermark Embedding Process

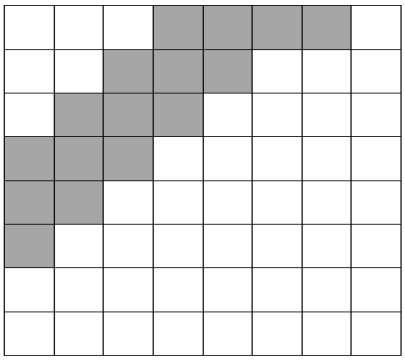

Figure 2.2: Watermarked Image Coefficients in *8x8* DCT Block

2.1.2. Perceptual Mask

We can embed a stronger watermark if we amplify the mark in the areas where it is well hidden (such as textures in the images) and attenuate it in the areas where it is perceptible (such as plain regions in the images). This process is referred as the perceptual shaping. During the watermark embedding process, we shape the watermark by employing the perceptual mask $m[u,v]$ which is based on Watson's Model [29]. The model uses the *8x8* block DCT transform. The goal is to guarantee the invisibility of the alterations introduced by the watermark. We employ the Watson's DCT-based visual model as proposed in [5]. First, we estimate the visibility threshold T [i,j] for every [i,j] where i = 1,2,..,8 and j = 1,2,…,8 , the DCT coefficients of each *8x8* block which can be approximated in logarithmic units by the following function.

$$\log T[i,j] = \log\left(\frac{T_{\min}\left(f_{i,0}^2 + f_{0,j}^2\right)^2}{\left(f_{i,0}^2 + f_{0,j}^2\right)^2 - 4(1-r) f_{i,0}^2 f_{0,j}^2}\right) + K\left(\log\sqrt{f_{i,0}^2 + f_{0,j}^2} - \log f_{\min}\right)^2 \tag{2.2}$$

where $f_{i,0}$ and $f_{0,j}$ are the vertical and horizontal spatial frequencies of the DCT basis functions respectively (in cycles/degree), T_{min} is the minimum value of $T[i,j]$ associated with f_{min} , K is constant value that determines the degree of the perceptual mask. Also, r is a constant between 0 and 1 and may be different for each frequency coefficient. Watson uses a value $r = 0.7$ for all i and j. Then, we obtain $T[i,j]$ values

of size *8x8* as shown in Table 2.1. Since this model is valid for only AC frequencies, $T[i,j]$ is re-arranged for every block by using:

$$T'[i,j] = T[i,j]\left(\frac{X_{0,0}}{\bar{X}_{0,0}}\right)^{\alpha_T} \tag{2.3}$$

Where α_T is a constant exponent controlling the degree of luminance masking, $X_{0,0}$ is the DC coefficient for each block, $\bar{X}_{0,0}$ is the average of the DC coefficients in *8x8* DCT blocks. Equation (2.2) and (2.3) contains parameters which are set to $T_{\min} = 1.01$, $K = 1.728$, $f_{\min} = 3.68$ cycles/degree, $\alpha_T = 0.649$ and $\bar{X}_{0,0} = 1024$ as suggested in [5]. Finally, the perceptual mask is obtained as follows:

$$m[u,v] = 4\left(1+\left(\sqrt{2}-1\right)\delta[l_1]\right)\left(1+\left(\sqrt{2}-1\right)\delta[l_1]\right)\chi T'[l_1,l_2] \tag{2.4}$$

where $l_1 = n_1 \bmod 8$, $l_2 = n_2 \bmod 8$, $\delta[.]$ is the Kronocker function and $\chi < 1$ is the scaling factor.

This mask ensures that the watermark will remain imperceptible to the human eye; however, at the same time it will alter the pixel values as much as possible in order to achieve maximum robustness. The small values in DCT sensitivity table shown in Table 2.1 indicate that human eye is more sensitive to the changes in those coefficients. Thus, we embed the watermark bits in those coefficients with power.

1,40	1,01	1,16	1,66	2,40	3,43	4,79	6,56
1,01	1,45	1,32	1,52	2,00	2,71	3,67	4,93
1,16	1,32	2,24	2,59	2,98	3,64	4,60	5,88
1,66	1,52	2,59	3,77	4,55	8,71	6,28	7,60
2,40	2,00	2,98	4,55	6,15	7,46	8,71	10,17
3,43	2,71	3,64	5,30	7,46	9,62	11,58	13,51
4,79	3,67	4,60	6,28	8,71	11,58	14,50	17,29
6,56	4,93	5,88	7,60	10,17	13,51	17,29	21,15

Table 2.1 : *8x8* DCT Sensitivity Table

2.1.3. Watermark Extraction Process

In the watermark extraction process, as shown in Figure 2.3, we compute *8x8* block DCT of the watermarked image. Since the host image is not available in the watermark extraction process, we construct the perceptual mask, $m[u,v]$, by using watermarked image assuming that its perceptual analysis result is similar with that of host image. Then, we extract the watermarked coefficients corresponding to each watermark bit by using distribution key K_2. The watermarked coefficients corresponding to the i^{th} bit of the message sequence constitutes a vector $\vec{\mathbf{y}}_i = \left[\vec{\mathbf{y}}_i(1), \vec{\mathbf{y}}_i(2), ..., \vec{\mathbf{y}}_i(M)\right]$ where $i = 1, 2, ..., T_b$. Therefore, all watermarked coefficients can be put into a vector $\vec{\mathbf{y}} = \left[\vec{\mathbf{y}}_1, \vec{\mathbf{y}}_2, ..., \vec{\mathbf{y}}_{T_b}\right]$. At the repetition decoding stage, security key K_1 is used to re-generate the spread-spectrum sequence $\vec{\mathbf{p}}_c$ of length T_c. Then, the spread-spectrum sequence $\vec{\mathbf{p}}_c$ is divided into T_b consecutive M-length $\vec{\mathbf{p}}_{c,i}$ sequences corresponding to each coded bit. The embedded binary message bits are recovered with the selected watermark detection scheme using $\vec{\mathbf{y}}_i$ and $\vec{\mathbf{p}}_{c,i}$.

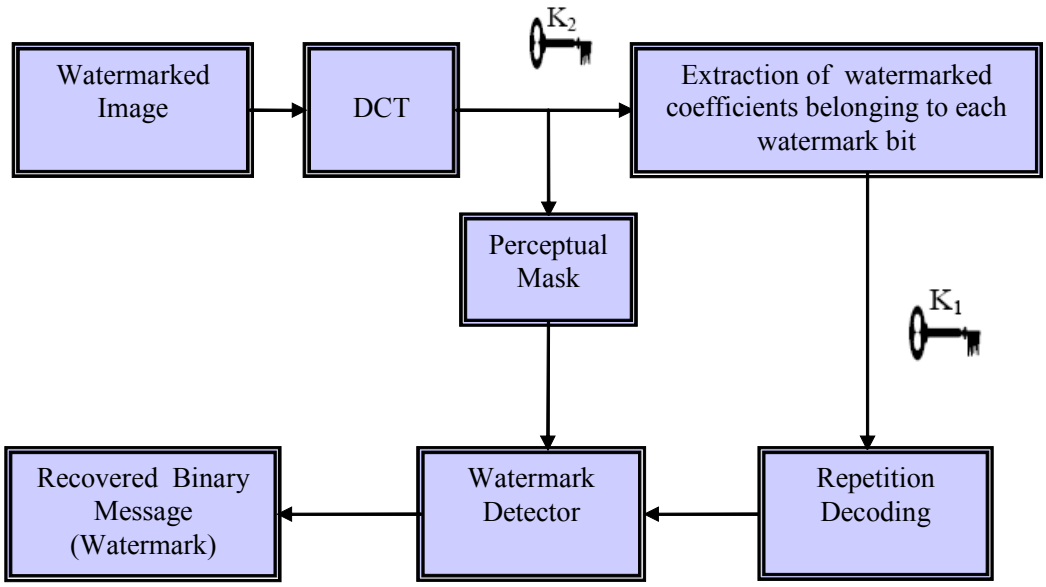

Figure 2.3: Watermark Extraction Process

2.2. The Problem Statement

The existing blind detection methods used in the spread spectrum based watermarking systems perform poorly, particularly in terms of decoding error probability due to the presence of the host signal interference at the receiver side. The interference at the detector limits the detection performance of the spread spectrum watermarking systems even in the absence of channel distortion and attack. In this case, we can improve performance of the detectors for these systems by either rejecting or minimizing the host signal interference. For complete rejection of the host signal interference we should use a non-blind detection mechanism which is, however, not feasible for many data hiding applications such as copy control, device control, etc. Thus, we can think of minimizing the host signal interference and one possible way to do this by applying pre-processing to the watermarked image which is the main idea of our work. The main motivation of this chapter has been to design blind detection schemes for spread spectrum based watermarking systems, which are capable of cancelling host signal interference at the receiver side. Hence, we can improve decoding as well as detection performance. These detectors are based on the proposed block

normalization method. This method reduces host signal interference by using the local statistics of each *8x8* discrete cosine transform (DCT) block of the watermarked signal. We employ the proposed method in different types of existing watermark detectors such as correlation; covariance and maximum likelihood (ML) based detectors with certain underlying distributions. The simulation results demonstrate that the proposed block normalization method considerably reduces the bit error rate of the existing correlation, covariance and ML estimation based watermark detectors.

2.3. Existing Watermark Detection Mechanisms Used in Spread Spectrum Watermarking Systems

The correlation based watermark detector is one of the oldest blind detection methods in literature [5]. However, this method performs poorly since the watermarked coefficients do not obey Gaussian statistics. Even if they were Gaussian, channel distortions & host signal interference would make them non-Gaussian. We can easily verify whether the totally 65536 watermarked DCT coefficients deviate from the Gaussian distribution, by comparing its histogram as shown in Figure 2.4 with the normal the probability-probability (P-P) plot as shown in Figure 2.5. The P-P plot is employed to see whether a given set of data follows some specified distribution. The "+" marks denote the empirical probability versus the data value for each point in the sample. We use the 65536 watermarked coefficients as the data for the P-P plot. Since the data deviates from the straight line, we can conclude that the watermarked DCT coefficients do not follow Gaussian distribution and they are heavy-tailed. In order to improve the correlation based detectors, the other methods are presented which takes the statistical characteristics of the transform coefficients into account. The watermark detection schemes for spread spectrum based watermarking systems employ statistical characterization of the host signal to develop an optimal or near-optimal watermark detector in the maximum likelihood (ML) sense [5], [10]. However, they can not reach non-zero decoding error probability due to the host signal interference at the watermark decoder even in the absence of attack and channel distortion.

In remaining part of this section, we introduce the existing watermark detection schemes such as correlation, and covariance and ML based detectors used in the spread

spectrum watermarking systems. Then, we address the limitations of these watermark detectors due to the host image interference.

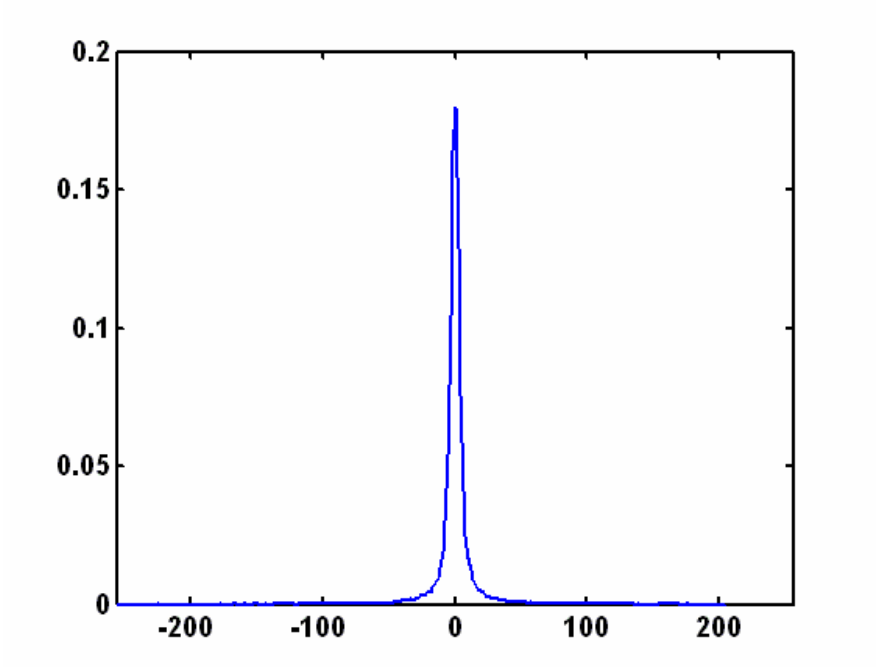

Figure 2.4: Histogram of the Watermarked Coefficients in DCT Domain

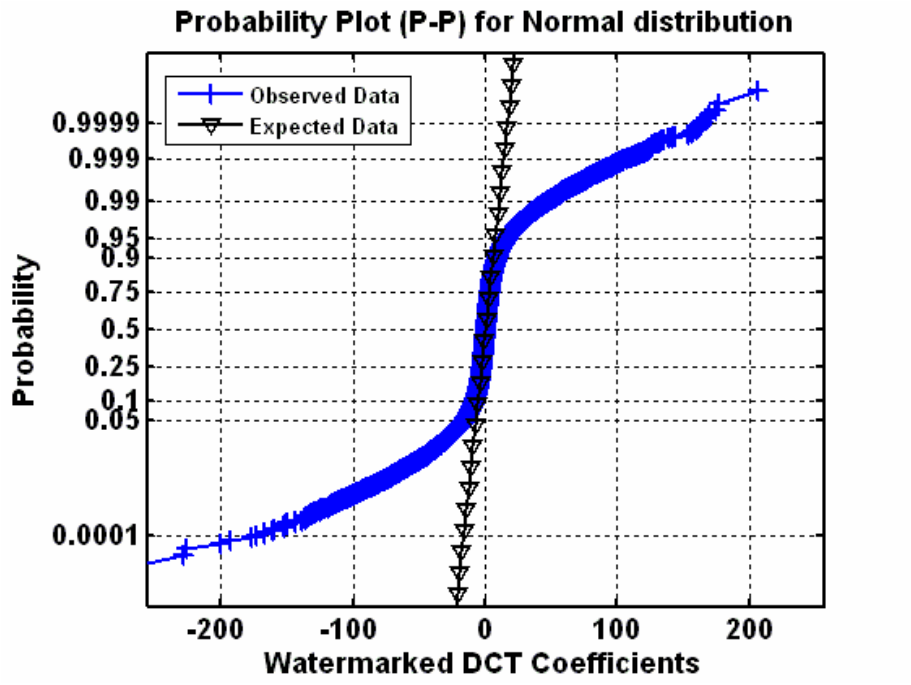

Figure 2.5 : Normal Probability (P-P) Plot for the Watermarked Coefficients of Lena Image

2.3.1. Correlation Detector (CRD)

In the spread spectrum watermarking system, the watermarked coefficient vector corresponding to the i^{th} bit of the message sequence can be expressed as follows:

$$\vec{\mathbf{y}}_i = \vec{\mathbf{x}}_i \odot \left(\vec{\mathbf{U}} + \vec{\phi}_i \odot \vec{\mathbf{w}}_{c,i} \right) \tag{2.5}$$

where $\odot$ denotes the element-wise multiplication of two vectors, $\vec{\phi}_i = \gamma \vec{m}_i$ denotes the insertion strength vector, $\vec{\mathbf{U}}$ is a vector of size *1xM* whose elements are all ones, $\vec{\mathbf{w}}_{c,i} = \vec{\mathbf{b}}(i)\vec{\mathbf{p}}_{c,i}$ is watermark sequence and $\vec{\mathbf{p}}_{c,i}$ is the spread-spectrum sequence. Hence, the correlation detector has the form:

$$\left\{ \begin{array}{ll} \vec{\mathbf{b}}(i) = 1, & \text{if } \left\langle |\vec{\mathbf{y}}_i|, \vec{\mathbf{p}}_{c,i} \right\rangle \geq 0 \\ \vec{\mathbf{b}}(i) = -1, & \text{if } \left\langle |\vec{\mathbf{y}}_i|, \vec{\mathbf{p}}_{c,i} \right\rangle < 0 \end{array} \right\} \tag{2.6}$$

where "<,>" is the inner product operation.

$$|\vec{\mathbf{y}}_i| = \left| \vec{\mathbf{x}}_i \odot \left(\vec{\mathbf{U}} + \vec{\phi}_i \odot \vec{\mathbf{w}}_{c,i} \right) \right| = |\vec{\mathbf{x}}_i| \odot \left(\vec{\mathbf{U}} + \vec{\phi}_i \odot \vec{\mathbf{w}}_{c,i} \right) \tag{2.7}$$

since, $0 < \vec{\phi}_i(k) < 1$ for $\forall k$.

$$|\vec{\mathbf{y}}_i| \odot \vec{\mathbf{p}}_{c,i} = |\vec{\mathbf{x}}_i| \odot \vec{\mathbf{p}}_{c,i} + \vec{\phi}_i \odot |\vec{\mathbf{x}}_i| \odot \left(\vec{\mathbf{p}}_{c,i} \odot \vec{\mathbf{w}}_{c,i} \right) \tag{2.8}$$

$$|\vec{\mathbf{y}}_i| \odot \vec{\mathbf{p}}_{c,i} = |\vec{\mathbf{x}}_i| \odot \vec{\mathbf{p}}_{c,i} + \left(\vec{\phi}_i \odot |\vec{\mathbf{x}}_i| \odot |\vec{\mathbf{p}}_{c,i}|^2 \right) \vec{\mathbf{b}}(i) \tag{2.9}$$

$$\left|\vec{\mathbf{y}}_i\right| \odot \vec{\mathbf{p}}_{c,i} = \left|\vec{\mathbf{x}}_i\right| \odot \vec{\mathbf{p}}_{c,i} + \left(\vec{\phi}_i \odot \left|\vec{\mathbf{x}}_i\right| \odot \vec{\mathbf{U}} \right) \vec{\mathbf{b}}(i) \tag{2.10}$$

Therefore, the correlation based watermark detector determines the i^{th} bit of the embedded message as follows:

$$\left\langle \left|\vec{\mathbf{y}}_i\right|, \vec{\mathbf{p}}_{c,i} \right\rangle = \sum_{k=1}^{M} \left|\vec{\mathbf{y}}_i(k)\right| \vec{\mathbf{p}}_{c,i}(k)$$

$$= \sum_{k=1}^{M} \left|\vec{\mathbf{x}}_i(k)\right| \vec{\mathbf{p}}_{c,i}(k) + \left(\sum_{k=1}^{M} \vec{\phi}_i(k) \left|\vec{\mathbf{x}}_i(k)\right| \vec{\mathbf{U}}(k) \right) \vec{\mathbf{b}}(i) = I_i + \zeta_i \vec{\mathbf{b}}(i) \tag{2.11}$$

where ζ_i is a positive power strength and I_i is a constant value denoting the host image interference for $\vec{\mathbf{b}}(i)$.

2.3.2. Covariance Detector (CVD)

Due to the interference of the host image, spread-spectrum sequence $\vec{\mathbf{p}}_c$ and watermarked image $y[u,v]$ in DCT domain are not uncorrelated; a better solution is to subtract the mean of $\vec{\mathbf{y}}_i$ and $\vec{\mathbf{p}}_{c,i}$ before correlation. The detection rule for each of the binary message bit $\vec{\mathbf{b}}(i)$, $i = 1, 2, ..., T_b$, has the form:

$$\left\{ \begin{array}{lll} \vec{\mathbf{b}}(i) = 1, & \text{if} & \left\langle \left(\left|\vec{\mathbf{y}}_i\right| - \mu_{\left|\vec{\mathbf{y}}_i\right|} \right), \left(\vec{\mathbf{p}}_{c,i} - \mu_{\vec{\mathbf{p}}_{c,i}} \right) \right\rangle \geq 0 \\ \vec{\mathbf{b}}(i) = -1, & \text{if} & \left\langle \left(\left|\vec{\mathbf{y}}_i\right| - \mu_{\left|\vec{\mathbf{y}}_i\right|} \right), \left(\vec{\mathbf{p}}_{c,i} - \mu_{\vec{\mathbf{p}}_{c,i}} \right) \right\rangle < 0 \end{array} \right\} \tag{2.12}$$

where $\mu_{|\vec{\mathbf{y}}_i|}$ denotes sample mean of the vector $|\vec{\mathbf{y}}_i|$, $\mu_{\vec{\mathbf{p}}_{c,i}}$ denotes sample mean of the vector $\vec{\mathbf{p}}_{c,i}$.

2.3.3. Block Coefficient Based Maximum Likelihood Detector (BCMLD)

The distribution of DCT coefficients of the watermarked image can be modelled by using zero-mean Generalized Gaussian distribution as defined in [5] as follows;

$$f_X(x) = A\exp\left(-|\alpha x|^{\beta}\right) \tag{2.13}$$

where A and α are the functions of β and the standard deviation σ as follows,

$$\alpha = \frac{1}{\sigma_x}\left(\frac{\Gamma(3/\beta)}{\Gamma(1/\beta)}\right)^{1/2} \tag{2.14}$$

where $\Gamma(\bullet)$ denotes the Gamma function and calculated by $\Gamma(x) = \int_0^{\infty} t^{x-1}e^{-t}dt$ and

$$A = \frac{\alpha\beta/2}{\Gamma(1/\beta)} \tag{2.15}$$

We can write two hypotheses for the i^{th} bit of the embedded message sequence associated with a bit '-1' and '1' respectively:

$$H_0 : \vec{\mathbf{y}}_i(k) = \vec{\mathbf{x}}_i(k)\left(1 - \vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)\right) \tag{2.16}$$

$$H_1 : \vec{\mathbf{y}}_i(k) = \vec{\mathbf{x}}_i(k)\left(1 + \vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)\right) \tag{2.17}$$

where $k = 1,2,...M$ and M denotes the number of the watermarked coefficients to embed the i^{th} bit of the message sequence.

By assuming that a priori probabilities for both hypotheses are equal, i.e., $p(H_0) = p(H_1)$, Bayes test becomes;

$$\Lambda\left(\vec{\mathbf{y}}_i(k)\right) = \frac{p\left(\vec{\mathbf{y}}_i(k) \mid H_1\right)}{p\left(\vec{\mathbf{y}}_i(k) \mid H_0\right)} \underset{H_0}{\overset{H_1}{\gtrless}} T \tag{2.18}$$

$$f_Y(\vec{\mathbf{y}}_i(k) \mid H_0) = \frac{A}{1-\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)} \exp\left(-\left| \frac{\alpha(k)\vec{\mathbf{y}}_i(k)}{1-\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)} \right|^{\beta(k)} \right) \tag{2.19}$$

$$f_Y(\vec{\mathbf{y}}_i(k) \mid H_1) = \frac{A}{1+\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)} \exp\left(-\left| \frac{\alpha(k)\vec{\mathbf{y}}_i(k)}{1+\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)} \right|^{\beta(k)} \right) \tag{2.20}$$

where $f_Y(\vec{\mathbf{y}}_i(k) \mid H_1)$ and $f_Y(\vec{\mathbf{y}}_i(k) \mid H_0)$ are the probability density function of $\vec{\mathbf{y}}_i(k)$ under the hypotheses H_1 and H_0 respectively and T is threshold as given in Equations 2.19 and 2.20.

In this detection scheme, the estimation of β and σ parameters are separately done on each of the watermarked 16 coefficients in *8x8* DCT block. That is, there are $N_b = N^2/64$ blocks in the watermarked image of size *NxN*, so for each block coefficient we have N_b DCT samples. Therefore, 16 different (σ, β) values are obtained after estimation since we mark 16 coefficients in each *8x8* DCT block. By using the obtained (σ, β) sets, we can calculate α and A. In fact, there is no need to calculate A since it is irrelevant to the likelihood ratio. Therefore, the standard deviation can be found as follows:

$$\sigma_{i,j} = \sqrt{\frac{1}{N_b}\sum_{k=1}^{N_b}\left(\mathbf{y}_{i,j}(k)\right)^2 - \left(\frac{1}{N_b}\sum_{k=1}^{N_b}\mathbf{y}_{i,j}(k)\right)^2} \tag{2.21}$$

where $\sigma_{i,j}$ is the standard deviation corresponding to the DCT coefficients of the watermarked image in the i^{th} row and the j^{th} column of $8x8$ DCT blocks which is denoted by $\mathbf{y}_{i,j}$. Estimates of $\beta_{i,j}$ parameters are obtained by matching the sample mean absolute value and the sample variance of DCT coefficients to those of Generalized Gaussian distribution as proposed in [30] and by solving maximum likelihood equation as follows;

$$\frac{E\left\{\left|\mathbf{y}_{i,j}\right|\right\}}{\sigma_{i,j}} = \frac{\Gamma\left(2/\beta_{i,j}\right)}{\sqrt{\Gamma\left(1/\beta_{i,j}\right)\Gamma\left(3/\beta_{i,j}\right)}} \tag{2.22}$$

where $E\{.\}$ denotes the expected value function, actually in our case it denotes the sample mean.

Since an open solution for $\beta_{i,j}$ does not exist, one can instead sample the solution space by computing the right hand side of the Equation (2.22) for several values of $\beta_{i,j}$ and find the best match. We construct an ensemble between $0.3 < \beta < 2$ in steps of 0,01 to estimate the best approximation of $\beta_{i,j}$ parameters. Once $\left(\sigma_{i,j}, \beta_{i,j}\right)$ parameters are estimated for each of the 16 coefficient sets, we can start decoding each bit of the embedded watermark independently. Therefore, we obtain decision test as follows:

$$\Lambda(|\vec{\mathbf{y}}_i|) = \frac{\prod_{k=1}^{M}\frac{1}{1+\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)}\exp\left(-\left|\frac{\alpha(k)|\vec{\mathbf{y}}_i(k)|}{1+\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)}\right|^{\beta(k)}\right)}{\prod_{k=1}^{M}\frac{1}{1-\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)}\exp\left(-\left|\frac{\alpha(k)|\vec{\mathbf{y}}_i(k)|}{1-\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)}\right|^{\beta(k)}\right)} \tag{2.23}$$

where $k=1,2,...M$ and β and α are the vectors of size $1xM$ whose elements belong to one of the 16 parameter set $\left(\sigma_{i,j},\beta_{i,j}\right)$ depending on which set $\vec{\mathbf{y}}_i(k)$ belongs to. We use the log-likelihood ratio to determine the value of $\vec{\mathbf{b}}(i)$,

$$S\left(\left|\vec{\mathbf{y}}_i\right|\right)=\sum_{k=1}^{M}\ln\left(1-\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)\right)+\sum_{k=1}^{M}\left(-\left|\frac{\alpha(k)\left|\vec{\mathbf{y}}_i(k)\right|}{1-\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)}\right|^{\beta(k)}\right)$$

$$-\sum_{k=1}^{M}\ln\left(1+\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)\right)+\sum_{k=1}^{M}\left(-\left|\frac{\alpha(k)\left|\vec{\mathbf{y}}_i(k)\right|}{1+\vec{\phi}_i(k)\vec{\mathbf{p}}_{c,i}(k)}\right|^{\beta(k)}\right) \tag{2.24}$$

where $S(|\vec{\mathbf{y}}_i|)\underset{H_0}{\overset{H_1}{\gtrless}}0$ and $\beta(k)$ and $\alpha(k)$ denotes the parameter set in which $\vec{\mathbf{y}}_i(k)$ belongs to.

2.4. The Proposed Block Normalization Based Watermark Detectors

In this section, we present the proposed block normalization method and the watermark detectors using that method. The proposed method is used to reduce the host signal interference at the receiver side. It is applied to the new and existing detection schemes as stated in [31].

2.4.1. Block Normalization based Correlation Detector (BNCRD)

In this watermark detection scheme, we aim at to reduce the host image interference in the correlation detector. We therefore employ the proposed block normalization method. Firstly, we transform the absolute value of the 16 watermarked

coefficients in each *8x8* DCT block by using the proposed block normalization method in DCT domain as follows:

$$\vec{\mathbf{z}}^{\,j}(n) = \frac{\left|\vec{\mathbf{y}}^{\,j}(n)\right| - \mu_{\left|\vec{\mathbf{y}}^{\,j}\right|}}{\sigma_{\left|\vec{\mathbf{y}}^{\,j}\right|}} \tag{2.25}$$

where $n=1,2,..,16$, $j = 1,....,N^2/64$ and $N^2/64$ denotes the block number of watermarked coefficients for image of size *NxN*, $\vec{\mathbf{y}}^{\,j}$ and $\vec{\mathbf{z}}^{\,j}$ denotes watermarked and transformed coefficient vector respectively for the j^{th} DCT block. Also, $\mu_{\left|\vec{\mathbf{y}}^{\,j}\right|}$ and $\sigma_{\left|\vec{\mathbf{y}}^{\,j}\right|}$ denotes the sample mean and the standard deviation of the absolute value of the j^{th} DCT block's watermarked coefficients. The watermarked coefficient vector corresponding to the i^{th} bit of the embedded binary message can be transformed as shown in the following formula:

$$\vec{\mathbf{z}}_i(k) = \frac{\left|\vec{\mathbf{y}}_i(k)\right| - \vec{\mu}_{\left|\vec{\mathbf{y}}^{\,j}\right|}(k)}{\vec{\sigma}_{\left|\vec{\mathbf{y}}^{\,j}\right|}(k)} \tag{2.26}$$

where $k=1,2,..,M$, M denotes the number of watermarked coefficients to embed i^{th} bit of the watermark sequence, $\vec{\mu}_{\left|\vec{\mathbf{y}}^{\,j}\right|}(k)$ and $\vec{\sigma}_{\left|\vec{\mathbf{y}}^{\,j}\right|}(k)$ denotes the sample mean and the standard deviation of the absolute value of watermarked coefficients of the DCT block in which $\left|\vec{\mathbf{y}}_i(k)\right|$ belongs to and is calculated as follows:

$$\vec{\mu}_{\left|\vec{\mathbf{y}}^{\,j}\right|}(k) = \frac{1}{16}\sum_{n=1}^{16}\left|\vec{\mathbf{y}}^{\,j}(n)\right| \tag{2.27}$$

and

$$\vec{\sigma}_{\left|\vec{\mathbf{y}}^{\,j}\right|}(k) = \sqrt{\frac{1}{16}\sum_{n=1}^{16}\left|\vec{\mathbf{y}}^{\,j}(n)\right|^2 - \frac{1}{16}\sum_{n=1}^{16}\left|\vec{\mathbf{y}}^{\,j}(n)\right|} \tag{2.28}$$

Then, we calculate the inner product of the vector $\vec{\mathbf{z}}_i$, which belongs to the watermarked coefficients, and $\vec{\mathbf{p}}_{c,i}$, which belongs to the spread-spectrum sequence, in order to determine the value of i^{th} bit of the watermark $\vec{\mathbf{b}}(i)$ as follows;

$$\left\langle \vec{\mathbf{z}}_i, \vec{\mathbf{p}}_{c,i} \right\rangle = \sum_{k=1}^{M} \vec{\mathbf{z}}_i(k) \vec{\mathbf{p}}_{c,i}(k)$$

$$= \sum_{k=1}^{M} \frac{\left|\vec{\mathbf{x}}_i(k)\right|}{\vec{\sigma}_{\left|\vec{\mathbf{y}}^j\right|}(k)} \vec{\mathbf{p}}_{c,i}(k) - \sum_{k=1}^{M} \frac{\vec{\mu}_{\left|\vec{\mathbf{y}}^j\right|}(k)}{\vec{\sigma}_{\left|\vec{\mathbf{y}}^j\right|}(k)} \vec{\mathbf{p}}_{c,i}(k) + \left(\sum_{k=1}^{M} \frac{\left(\vec{\phi}_i(k)\left|\vec{\mathbf{x}}_i(k)\right|\right)}{\vec{\sigma}_{\left|\vec{\mathbf{y}}^j\right|}(k)} \right) \vec{\mathbf{b}}(i) = I_i' + \zeta_i' \vec{\mathbf{b}}(i) \qquad (2.29)$$

where ζ_i' denotes the positive power strength for i^{th} bit of the watermark sequence and I_i' denotes the constant value denoting the reduced host image interference for $\vec{\mathbf{b}}(i)$.

Finally, we conclude to the i^{th} bit of the embedded binary message $\vec{\mathbf{b}}(i)$ as follows:

$$\left\{ \begin{array}{ll} \vec{\mathbf{b}}(i) = 1, & \text{if } \left\langle \vec{\mathbf{z}}_i, \vec{\mathbf{p}}_{c,i} \right\rangle \geq 0 \\ \vec{\mathbf{b}}(i) = -1, & \text{if } \left\langle \vec{\mathbf{z}}_i, \vec{\mathbf{p}}_{c,i} \right\rangle < 0 \end{array} \right\} \qquad (2.30)$$

2.4.2. Block Normalization Based Covariance Detector (BNCVD)

In this detection method, we employ the proposed block normalization method in the *8x8* DCT domain in order to increase the detection performance of the covariance detector. Hence, we calculate the vector $\vec{\mathbf{z}}_i$, where $i = 1, 2, ..., T_b$, in order to recover the i^{th} bit of the embedded watermark. Finally, we recover the embedded watermark by using the formula below:

$$\left\{\begin{array}{lll}\vec{\mathbf{b}}(i)=1, & \text{if} & \left\langle\left(\vec{\mathbf{z}}_i-\mu_{|\vec{\mathbf{z}}_i|}\right),\left(\vec{\mathbf{p}}_{c,i}-\mu_{\vec{\mathbf{p}}_{c,i}}\right)\right\rangle \geq 0 \\ \vec{\mathbf{b}}(i)=-1, & \text{if} & \left\langle\left(\vec{\mathbf{z}}_i-\mu_{|\vec{\mathbf{z}}_i|}\right),\left(\vec{\mathbf{p}}_{c,i}-\mu_{\vec{\mathbf{p}}_{c,i}}\right)\right\rangle < 0\end{array}\right\} \tag{2.31}$$

where $\mu_{|\vec{\mathbf{z}}_i|}$ and and $\mu_{\vec{\mathbf{p}}_{c,i}}$ denote the sample mean of the vectors $\vec{\mathbf{z}}_i$ and $\vec{\mathbf{p}}_{c,i}$ respectively.

2.4.3. Block Based Maximum Likelihood Detector (BMLD)

In this watermark detection scheme, we model the distribution of the j^{th} *8x8* DCT block belonging to the watermarked image according to the Generalized Gaussian model in Equation (2.13). We find the $\left(\sigma_j,\beta_j\right)$ parameter set, where $j=1,....,N^2/64$ and $N^2/64$ denotes the block number of watermarked coefficients for the image of size *NxN*, for each of the j^{th} DCT block as found in BCMLD detector by using the following formulas;

$$\sigma_{i,j} = \sqrt{\frac{1}{16}\sum_{n=1}^{16}\left(\vec{\mathbf{y}}^{\,j}(n)\right)^2-\left(\frac{1}{16}\sum_{n=1}^{16}\vec{\mathbf{y}}^{\,j}(n)\right)^2} \tag{2.32}$$

and

$$\frac{E\left\{\left|\vec{\mathbf{y}}^{\,j}\right|\right\}}{\sigma_j} = \frac{\Gamma\left(2/\beta_j\right)}{\sqrt{\Gamma\left(1/\beta_j\right)\Gamma\left(1/\beta_j\right)}} \tag{2.33}$$

where $E\{.\}$ denotes the expected value function actually in our case it takes the sample mean of the input vector $\left|\vec{\mathbf{y}}^{\,j}\right|$. Also, $\vec{\mathbf{y}}^{\,j}$ denotes vector which contains watermarked coefficients of the j^{th} DCT block, $j=1,....,N^2/64$ and $N^2/64$ denote the block number of the watermarked coefficients for the image of size *NxN*.

Then, we take the average of all the $\left(\sigma_j,\beta_j\right)$ parameter sets, to obtain $\left(\sigma,\beta\right)$ parameter set which is used to model all the watermarked coefficients. Finally, we

decode each bit of the embedded watermark sequence by using (σ, β) parameter set and Equation (2.24).

2.4.4. Block Normalization Based Maximum Likelihood Detector (BNMLD)

In this watermark detection method, our aim is to improve the detection performance of the BMLD detector. To achieve this aim, firstly, we employ the block normalization method in each of the *8x8* DCT blocks. Therefore, we obtain the vector $\vec{\mathbf{z}}^{j}$, where $j = 1, ..., N^2/64$ and $N^2/64$ denotes the block number of watermarked coefficients for the image of size *NxN*, for the j^{th} DCT block by using the Equation (2.25). Then, with the normalized watermarked coefficients and the process used in the BMLD detector, we can recover the embedded binary message bits.

2.5. Simulation Results and Discussions

In all experiments, we examined the performances of the watermark detection schemes by using the test image "Lena" of size *512x512* as a host image. We calculate the peak signal to noise ratio (PSNR) and watermark to document ratio (WDR) to evaluate the perceptual quality of the watermarked image. The PSNR is a measure of the degradation in the original image introduced by the watermark as well as by the other factors. It also a rough measure of the image fidelity and calculated as follows,

$$PSNR = 10 \log \frac{X_{peak}^2}{\frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} \left(X[i,j] - Y[i,j] \right)^2} \tag{2.34}$$

where $X[i,j]$ and $Y[i,j]$ denotes the host and the watermarked image respectively, N denotes the size of the image along both dimensions, and X_{peak}^2 is the maximum pixel luminance value in the host image.

On the other hand, WDR is the measure of the ratio of watermark energy to the host image energy calculated as:

$$\mathrm{WDR} = 10\log\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}\left(X[i,j]-Y[i,j]\right)^2}{\sum_{i=1}^{N}\sum_{j=1}^{N}X^2[i,j]} \tag{2.35}$$

The bit error rate (BER) is the probability that an information bit is decoded erroneously during the watermark extraction process. It is the ratio of the number of bits received in error to the total number of received bits. As in every communications system, the watermarking systems also depend on the transmitted signal energy since BER decreases when signal energy increases. The simulation results shown in Figure 2.11 – Figure 2.13 demonstrate that the watermark energy increases linearly as we increase the insertion coefficient γ from 0.02 to 0.06. Therefore, we obtain lower BERs and the performance of the watermark detectors increases. However, there is a trade-off between robustness and perceptual quality in these simulations. As we increase the insertion coefficient γ to achieve more robust and reliable digital watermarking system, we decrease the perceptual quality of the watermarked image**.** In order to achieve a low bit error rate and high channel capacity while maintaining an acceptable image quality; one has to compromise between the WDR and PSNR as shown in Table 2.2. The insertion strength should be chosen so that the watermark power is maximized, while the PSNR is kept above the minimum acceptable level of 38 dB [32]. In addition, we can subjectively evaluate the perceptual quality of the watermarked images with the various insertion strengths shown in Figure 2.6 - Figure 2.10. In these figures, as the insertion increases, the images lose the perceptual quality.

Insertion Coefficient	PSNR [dB]	WDR [dB]
0.01	55.6277	-50.3188
0.02	49.6071	-44.2982
0.03	46.0853	-40.7764
0.04	43.5865	-38.2776
0.05	41.6483	-36.3394
0.06	40.0647	-34.7558
0.07	38.7257	-33.4169
0.08	37.5659	-32.2570
0.09	36.5428	-31.2340
0.1	35.6277	-30.3188

Table 2.2 : PSNR and WDR Results of the Watermarked Lena Image as a Function of Insertion Coefficient γ

Figure 2.6 : Original Lena Image used as Host Signal

Figure 2.7: Watermarked Lena Image with Insertion Coefficient $\gamma = 0.1$

Figure 2.8: Watermarked Lena Image with Insertion Coefficient $\gamma = 0.07$

Figure 2.9 : Watermarked Lena Image with Insertion Coefficient $\gamma = 0.04$

Figure 2.10 : Watermarked Lena Image with Insertion Coefficient $\gamma = 0.01$

Research of relation between watermarking capacity and reliability will help us to find how to transmit more watermark information while keep an acceptable watermark detection bit error rate. In watermarking schemes, image can be considered as a communication channel to transmit messages. However, watermarking have some properties different from traditional communication because of the requirements of robustness and invisibility. We totally embed 65536 watermark bits into the host image in each simulation as shown in Figure 2.11 – Figure 2.14. As we decrease the watermark length, the number of repetition of watermark increases as well. However, the total watermark power does not depend on the number of embedded watermarks since the total number of embedded watermark bits is equal in each experiment. In these simulations, we embed the watermarks of length 256, 512 and 1024 bit respectively by changing the number of repetitions.

The simulations shown in Figure 2.11 – Figure 2.13, an increase in the length of watermark, results in a decrease in the number of embedded watermark repetitions and the bit per energy at a constant insertion coefficient γ. Low bit energy in turn, produces a higher bit error rate. This severely limits the amount of information that the watermark can carry. Hence, the dependence of the bit error rate on the insertion coefficient γ, can be seen in these figures. Furthermore, the detectors using the proposed block normalization method reduce the BER and increase the capacity at a constant insertion coefficient in these simulations.

Generally, the recovered watermarks have high BERs because the watermark bits are embedded with low powers not to lose the perceptual quality of the watermarked image. Figure 2.13 illustrates how the BER rate of the extracted watermark increases as the length of watermark increases. Since the number of pixels per bit decreases, the energy per bit hence decreases. In this simulation, the value of insertion strength γ is set to 0.04 fulfilling the pre-mentioned requirements. We can also evaluate the perceptual quality of this watermarked image by looking at the Figure 2.9. Furthermore, if we evaluate the system at a constant BER, we can conclude that the proposed detectors approximately increase the capacity of the system four fold. Hence, the

proposed BNMLD detector can especially be chosen in most of the watermarking applications since hiding capacity is one of the most important requirements.

When we set the watermark length to 256 bit in simulation shown in Figure 2.14, the proposed block normalization method approximately reduces the BER of the covariance detector from 10^{-1} to 10^{-2}. In addition, the proposed method approximately reduces the BER from 10^{-2} to 10^{-4} in the ML based detection schemes. In this simulation, the insertion coefficient is set to 0.04.

The proposed detection methods reduce the computational complexity of the watermarking system. For example, the existing BCMLD detector has higher BER than the BNCVD detector, however, the proposed BNCVD has the lower computational complexity since it does not model the distribution of the coefficients and does not employ ML estimation method. Thus, the BNCVD can be employed as sub-optimal detection method in most of the watermarking applications.

In all experiments in this chapter, the proposed BNMLD watermark detector has the lowest BER among all watermark detectors. The main reason is that the BNMLD detector models and normalizes the watermarked coefficients in a block-wise manner. The other detectors do not use the block-wise manner both to model and normalize watermarked coefficients.

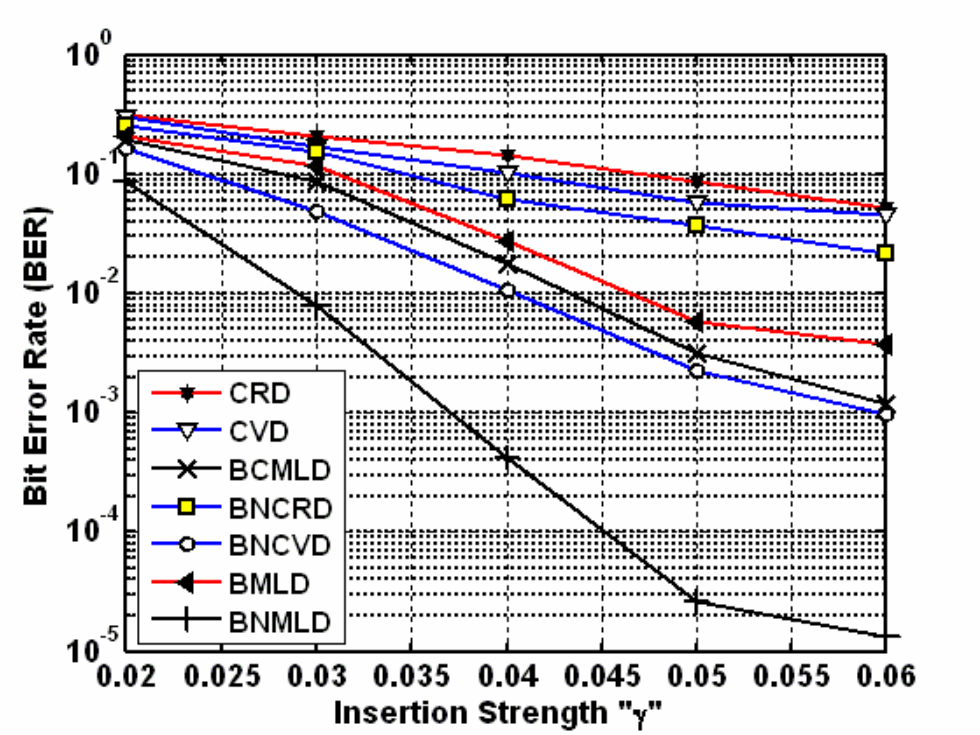

Figure 2.11: BER of Detectors as a Function of Insertion Coefficient γ when Embedding 256 bit Watermarks

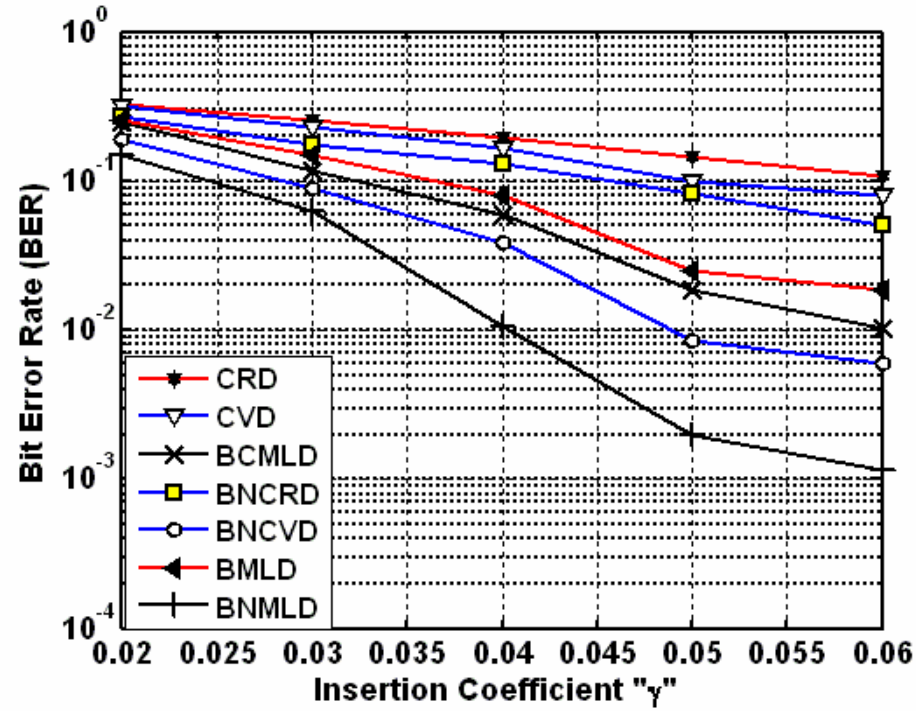

Figure 2.12: BER of Detectors as a Function of Insertion Coefficient γ when Embedding 512 bit Watermarks

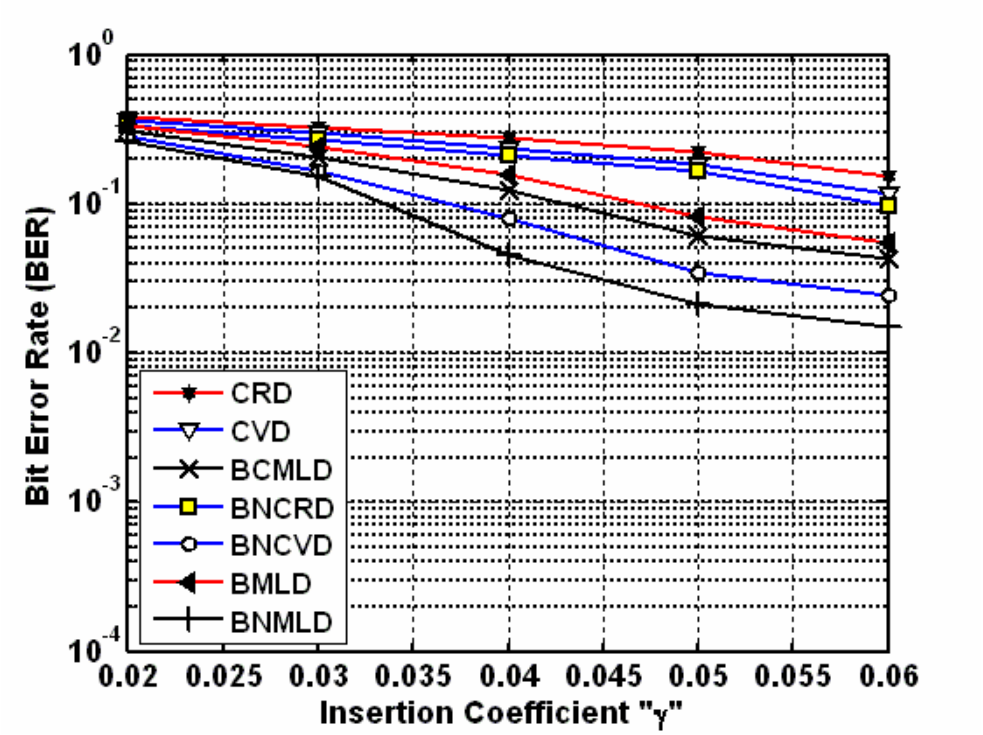

Figure 2.13 : BER of Detectors as a Function of Insertion Coefficient γ when Embedding 1024 Bit Watermarks

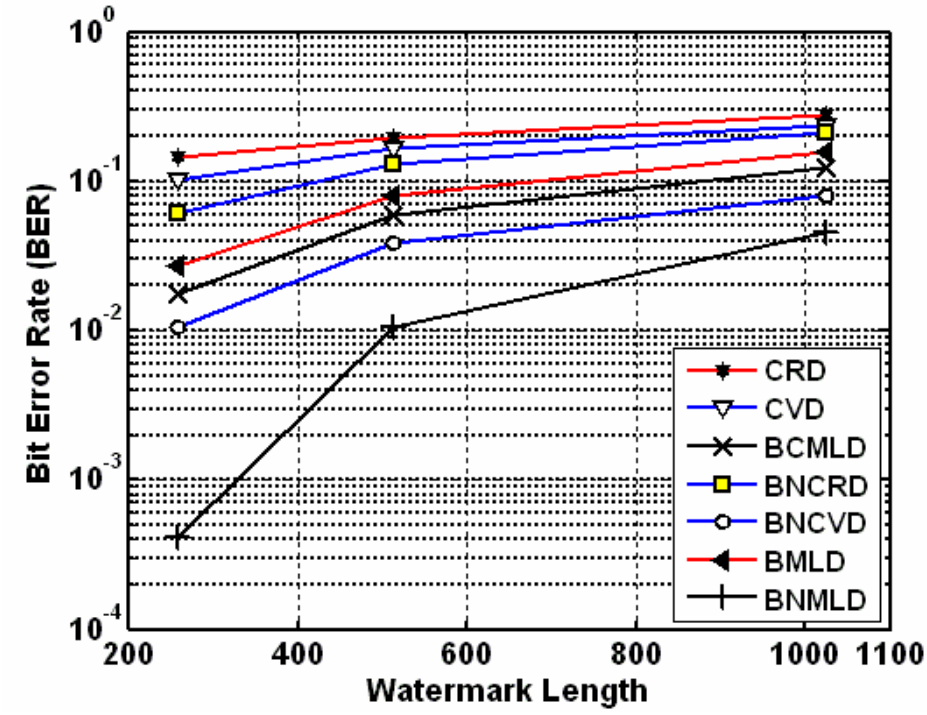

Figure 2.14: BER of the Detectors with Various Watermark Lengths

2.6. Conclusions

In this chapter, we address the host signal interference problem of spread spectrum watermarking systems employing blind detection schemes. The interference both limits the capacity of the system and increases the BER of the recovered watermark even if there is no channel distortion and attack. We develop blind detection schemes based on the host signal interference cancellation method at the receiver side [31]. These schemes reduce the interference by employing the proposed block normalization method. Hence, they approximately 4 times increase the capacity of the system at the same insertion strength level. Since the capacity plays very critical role in many watermarking applications, it provides very important gains to the system. In addition, the block normalization method improves the BER performances of the detectors. For example, when the insertion strength is set to 0.06 and 256-bit watermarks are embedded, the proposed method approximately reduces BER of the recovered watermark from 10^{-2} to 10^{-5} in ML estimation based detection method. In addition, BER of the recovered watermark is reduced from 10^{-1} to 10^{-3} in covariance detector by the proposed method, when the insertion strength is set to 0.06 and 256-bit watermarks are embedded. Furthermore, we utilize Watson's HVS model in the watermark embedding process. Hence, we shape the watermark before embed it into the host image according to the HVS. The simulations results demonstrate that both modeling the watermarked DCT coefficients and reducing the interference in a block-wise manner increases the blind detection performance of the spread spectrum watermarking system.

3. ROBUST BLIND DETECTION FOR DWT DOMAIN QUANTIZATION BASED WATERMARKING SYSTEM

In this chapter, we introduce the quantization based watermarking system in DWT domain in Section 3.1, which is proposed in [33] and [34]. We address the detection problem of this system against channel distortions and attacks in Section 3.2. Then, we briefly describe the detectors used in this system and the proposed detection scheme in Section 3.3 and Section 3.4 respectively. Finally, we evaluate the performance of the detectors with simulation results and give conclusions in Sections 3.5 and 3.6 respectively.

3.1. Quantization Based Digital Watermarking System

In this section, we introduce the quantization based digital watermarking system that is used in [33] and [34] for embedding and extracting the watermark bits. This system, simultaneously, uses the reference watermarks to characterize the channel distortions and degradations, and the information watermarks to transmit the hidden information. The information and reference (optional) watermarks are embedded into the host image at the transmitter. Then, information and reference watermarks are extracted according to the quantization based algorithm at the receiver side from the watermarked image, which is exposed channel distortions and attacks in the transmitting channel, as show in the Figure 3.1. There is no need to know the host image, so, this digital watermarking system employs blind watermark detection schemes. Also, in this digital watermarking system, we randomly generate binary watermark sequences $w(i) \in \{\pm 1\}$ and $r(i) \in \{\pm 1\}$, where $1 \le i \le N$ for information and reference watermarks respectively.

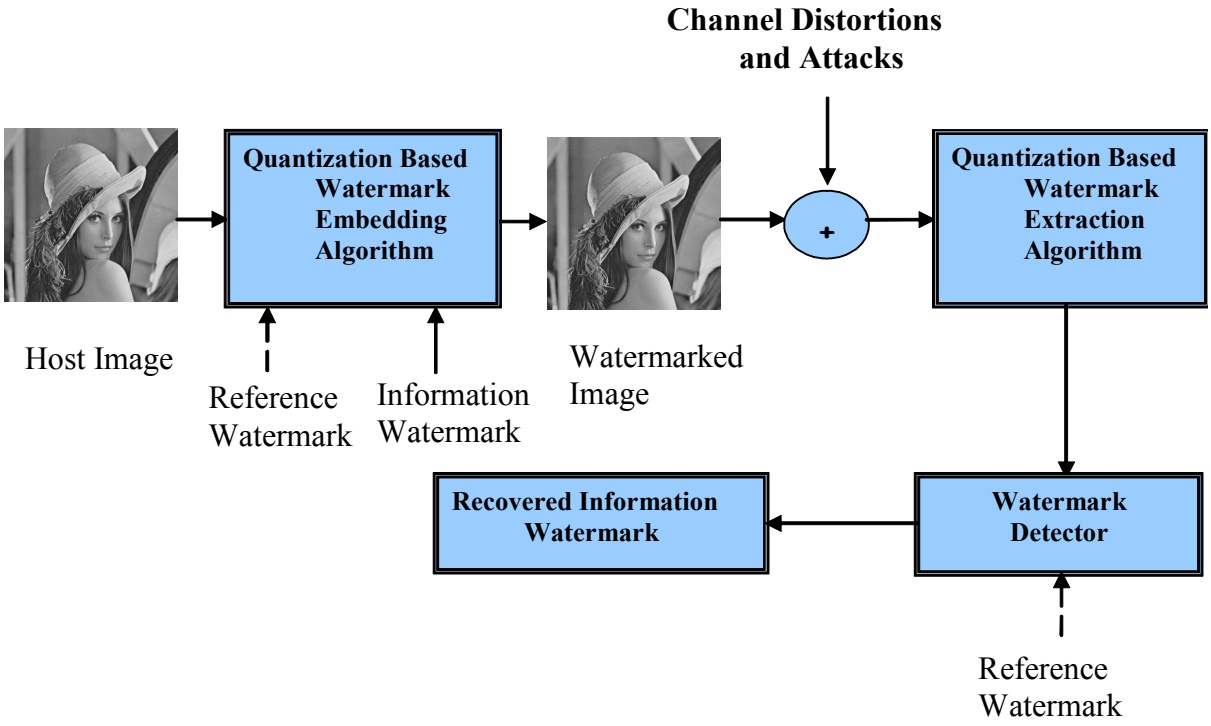

Figure 3.1: Quantization Based Digital Watermarking System

3.1.1. Watermark Embedding Process

In subsequent analysis, $\mathbf{x}[m,n]$ and $\mathbf{y}[m,n]$ denotes the host image and watermarked image in spatial domain respectively. Also, $\mathbf{X}_{o,l}[u,v]$ and $\mathbf{Y}_{o,l}[u,v]$ denotes the o^{th} frequency orientation at the l^{th} resolution level of the host image and the watermarked image in DWT domain respectively. In this notation, $o \in \{h,v,d\}$ expresses the horizontal, vertical and diagonal image details respectively, $l \in \{1,2,...,L\}$ is the resolution level and $[u,v]$ is the particular spatial location index at the resolution level l as shown in Figure 3.2.

In the embedding process, firstly, the host image $\mathbf{x}[m,n]$ is transformed into the DWT domain by performing the L-level DWT decomposition. So, we obtain $3L$ detail images and an approximation image at the coarsest level. Then, we sort the detail image

coefficients at the spatial location $[u,v]$ and at the resolution level l in an ascending order such that;

$$\mathbf{X}_{o1,l}[u,v] \le \mathbf{X}_{o2,l}[u,v] \le \mathbf{X}_{o3,l}[u,v] \tag{3.1}$$

where $o1, o2, o3 \in \{h, v, d\}$ and $o1 \neq o2, o2 \neq o3, o1 \neq o3$. We divide the range of values between the minimum and the maximum detail coefficient into the bins of width Δ by using the below formula;

$$\Delta = \frac{\mathbf{X}_{o3,l}[u,v] - \mathbf{X}_{o1,l}[u,v]}{2Q-1} \tag{3.2}$$

In order to embed the watermark bit, we quantize the median value of the detail image coefficients at the l^{th} resolution level as shown in Figure 3.3. The value of the quantization parameter Q is a trade-off between perceptual transparency and robustness, i.e. if we set smaller value for Q, we may lose the perceptual transparency but the system will be more robust and reliable against channel distortions and attacks. Finally, we compute the L-level inverse DWT and construct watermarked image $\mathbf{y}[m,n]$ in the spatial domain.

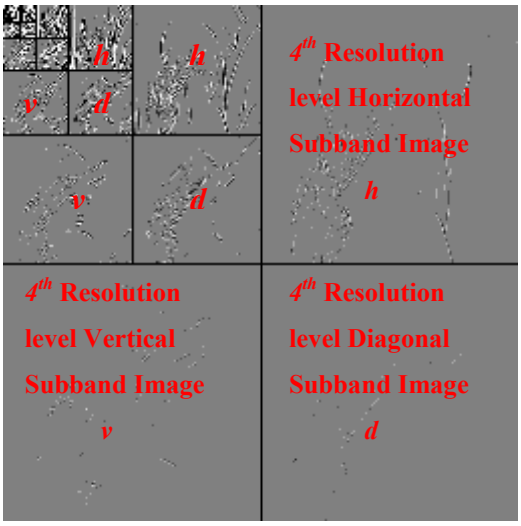

Figure 3.2 : 4 level DWT of the Lena Image

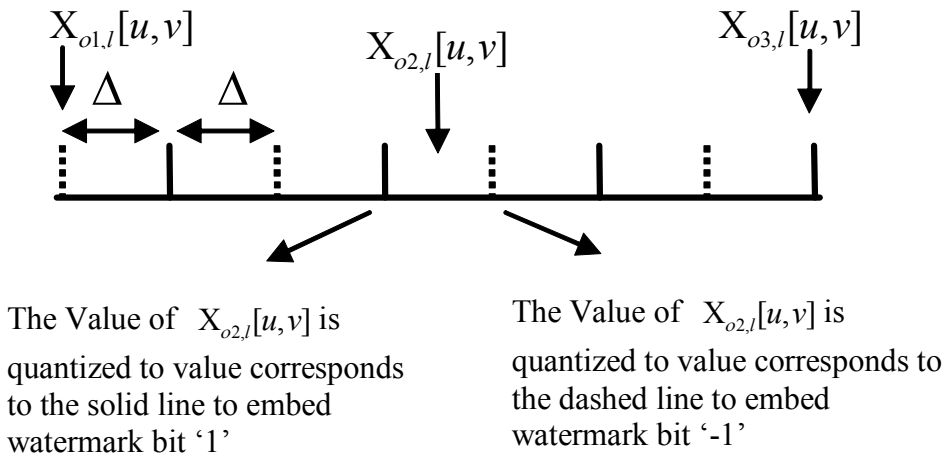

Figure 3.3: Watermark Embedding Scheme

3.1.2. Watermark Extraction Process

The watermarked image, $\mathbf{y}[m,n]$, is transformed into the DWT domain by performing the *L*-level DWT decomposition at the receiver side. Since quantization based watermarking system employs blind watermark detection scheme, the original image is not needed for the watermark extraction process. Then, we sort the detail coefficients in an ascending order as follows,

$$\mathbf{Y}_{o1,l}[u,v] \le \mathbf{Y}_{o2,l}[u,v] \le \mathbf{Y}_{o3,l}[u,v] \tag{3.3}$$

where $o1, o2, o3 \in \{h, v, d\}$ and $o1 \neq o2, o2 \neq o3, o1 \neq o3$. The value of the embedded watermark bit is determined from the relative position of $\mathbf{Y}_{o2,l}[u,v]$ by using the same value of Q used in embedding scheme. Once, we find the closest quantized value to, $\mathbf{Y}_{o2,l}[u,v]$, it is converted into its associated binary value as shown in Figure 3.4.

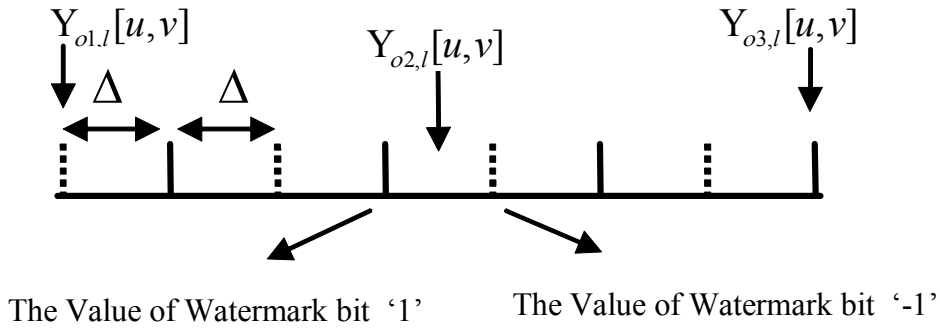

Figure 3.4: Watermark Extraction Scheme

3.2. Existing Watermark Detection Methods Used in Quantization Based Digital Watermarking System

In this section, we introduce the majority rule based watermark detector and diversity and attack characterization based watermark detector. These detectors are developed for the quantization based watermarking system in DWT domain [33], [34].

3.2.1. Majority Rule Based Watermark Detector (MRD)

The quantization based watermarking system using the majority rule based detection scheme to estimate the recovered watermark, is presented in [33]. In this watermark detection method, Kundur and Hatzinakos do not use reference watermarks in order to characterize the attacks. They embed the information watermarks into the host signal multiple times, i.e. M times, at the transmitter and then M watermark estimates are extracted at the receiver. The most common bit value among the i^{th} bits of the M watermark estimates is assigned as the i^{th} bit of the recovered information watermark by the majority rule based detector. Therefore, all the bits of the embedded information watermark are estimated.

3.2.2. Diversity and Attack Characterization Based Watermark Detector (DACD)

Kundur and Hatzinakos proposed the diversity and attack characterization based watermark detector in the quantization based watermarking system in [34]. In this detection scheme, firstly, they define the localized regions. In these localized regions, each of the information and reference watermark bits are alternatively embedded. Hence, they assume that if the information and reference watermarks are in the same localized region, they are effected from the channel distortions and attacks statistically similarly. At the transmitter side, M repetitions of the information watermark w_k and reference watermark r_k were embedded into the host image. Then, these each M repetition of information and reference watermark are extracted according to the quantization based algorithm at the receiver. Kundur and Hatzinakos modelled the region that one information watermark sequence and one reference watermark sequence have embedded as a binary symmetric channel (BSC) as shown in Figure 3.5 . A BSC is a common communications channel model used in communication theory and information theory. In this model, a transmitter wishes to send a bit, and the receiver receives a bit. It is assumed that the bit is usually transmitted correctly, but occasionally the receiver gets the wrong bit. Thus, the bit error probability of each channel is calculated as follows;

$$p_{Ek} = \frac{1}{N}\sum_{i=1}^{N} r_k(i) \oplus \hat{r}_k(i) \tag{3.4}$$

where $\hat{r}_k$ denotes the reference watermark associated with the k^{th} binary symmetric channel or localized region and N denotes the reference watermark length. Finally, all extracted information watermark repetitions are linearly weighed and added in order to recover the information watermark at the receiver side as follows;

$$\hat{w}(i) = \mathrm{sgn}\left[\sum_{k=1}^{M} \alpha_k \hat{w}_k(i)\right] \tag{3.5}$$

where $i = 1, 2, ..., N$, sgn(.) denotes the sign function and α_k denotes the linear combination coefficients for the k^{th} BSC, that are calculated as follows;

$$\alpha_k = \frac{\log\left(\frac{1-p_{Ek}}{p_{Ek}}\right)}{\sum_{j=1}^{M}\log\left(\frac{1-p_{Ej}}{p_{Ej}}\right)} \tag{3.6}$$

Since the watermark bits come from the set $\{\pm 1\}$ rather than the set {0, 1} as in [34], in order to recover the watermark bits we use sgn (.) function instead of round (.) function.

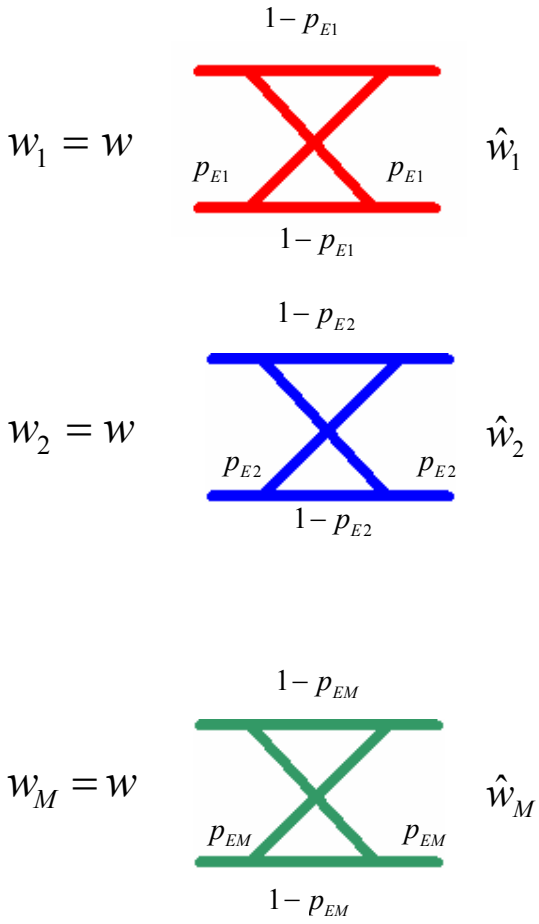

Figure 3.5: Binary Symmetric Channel Model

3.3. The Proposed Channel Reliability Estimation Based Watermark Detector (CRED)

In this section, we propose a new detection method to improve the detection performance in the quantization based watermarking system. The detector is named as the channel reliability estimation based detector [36]. In literature, Kundur and Hatzinakos propose the diversity and attack characterization based blind watermark detection method [34]. They assume that all the watermark estimates are reliable. Hence, they do not eliminate the unreliable estimates deteriorating performance of the system against severe degradations.

In this detection scheme, we, first, define the region that an information watermark sequence and a reference watermark sequence have embedded alternatively as a watermark channel. Then, we employ reference watermarks to estimate the reliabilities of each watermark channel. Hence, the watermark channel parameters are calculated by using the first and second order channel reliabilities and the proposed threshold scheme. Finally, information watermark is recovered one by one.

In the proposed watermark detection method, instead of determining the bit error probability within each watermark channel, we estimate reliability of the each watermark channel by using the below formula,

$$R_k = \frac{1}{N}\sum_{i=1}^{N} S_k(i) \tag{3.7}$$

where R_k denotes the reliability of k^{th} watermark channel, $k = 1, 2, ..., M$, M denotes the number of embedded reference watermarks, N denotes the reference watermark length, $i = 1, 2, ..., N$, and S_k is determined by using the below equation;

$$S_k(i) = \begin{cases} 1, & \text{if } \; r(i) = \hat{r}_k(i) \\ 0, & \text{otherwise} \end{cases} \tag{3.8}$$

where r denotes the reference watermark and $\hat{r}_k$ denotes the reference watermark estimate of the k^{th} watermark channel.

The reliabilities of watermark channels; R_k, can vary according to the channel distortion and attack type and also the embedding region in the DWT domain. The channel parameter of each watermark channel is calculated by using the first and the second order statistics of the channel reliabilities as follows;

$$\beta_k = \frac{R_k - \mu_R}{\sigma_R} \tag{3.9}$$

where β_k denotes the channel parameter of the k^{th} watermark channel and also μ_R and σ_R denotes the sample mean and the standard deviation of the watermark channel reliabilities and calculated by using the below formulas;

$$\mu_R = \frac{1}{M}\sum_{k=1}^{M} R_k \tag{3.10}$$

and

$$\sigma_R = \sqrt{\frac{1}{M}\sum_{k=1}^{M} R_k^2 - \frac{1}{M}\sum_{k=1}^{M} R_k} \tag{3.11}$$

The watermark channel parameters gives information about the watermark channel and the reliabilities of the watermarks extracted from these channels. The channel parameter defined in Equation (3.9) results in large values for high reliability probabilities and negative values for the reliability probabilities that are smaller than μ_R.

As in the all estimation problems, some channel reliability estimates might be unreliable. In our method, we called the channels, whose channel parameters are above the sample mean of the channel reliabilities, as reliable channels experimentally. Since, unreliable estimates increase the bit error rate, we do not use the watermarks extracted

from the unreliable channels in the watermark recovering process. To eliminate these unreliable estimates, we propose a threshold scheme as follows;

$$\lambda_k = \begin{cases} \beta_k, & \text{if } R_k > \mu_R \\ 1, & R_k = \mu_R \\ 0, & \text{otherwise} \end{cases} \tag{3.12}$$

where λ_k denotes the channel parameter of the k^{th} watermark channel after the thresholding scheme.

Due to the nature of the DWT domain, the reliabilities of the watermark channels are equal when there is no channel distortion and attack. In this case, we set the channel parameter to one since all the channel reliabilities equals to the sample mean of the reliabilities. Finally, we recover the i^{th} bit of the information watermark by using the watermark channel parameters λ_k and i^{th} bits of the information watermark estimates $\hat{w}_k$ as follows:

$$\hat{w}(i) = \text{sgn}\left[\sum_{k=1}^{M} \lambda_k \hat{w}_k(i)\right] \tag{3.13}$$

where *i=1,2,..,N* and sgn(.) is the sign function. Hence, the embedded information watermark bits are recovered.

3.4. Simulation Results and Discussions

This section provides simulation results to test and compare the performance of the proposed detection method. In all experiments, randomly generated information and reference watermarks of size 256 bit from the set {-1, 1} are embedded into the test image "Lena" of size *512x512*. To test the performance of the detectors in each simulation, 5000 experiments are done. In the quantization based digital watermarking system, DWT has been performed with the number of resolution level $L = 4$ and 10-

point Daubechies filter. We, first, evaluate and compare the robustness of the detectors against various channel distortions such as mean and median filtering, additive white Gaussian noise (AWGN) and lossy compression by using the normalized correlation coefficient is given by,

$$c(w,\hat{w}) = \frac{\sum_{i=1}^{N} w(i)\hat{w}(i)}{\sqrt{\sum_{i=1}^{N} w^2(i)}\sqrt{\sum_{n=1}^{N} \hat{w}^2(i)}} \tag{3.14}$$

where w denotes the original watermark and $\hat{w}$ denotes the recovered watermark.

The quantization parameter (Q) has to be chosen so that the watermark power is maximized, while the perceptual quality is kept above the minimum acceptable level. We can also subjectively evaluate the perceptual quality of the watermarked image as shown in Figure 3.6 - Figure 3.9 . The simulations shown in the Figure 3.10 - Figure 3.17, we set the quantization parameter Q = 4 and the corresponding PSNR value is 42.33 dB. This PSNR value is quite acceptable for the image quality as shown in the Figure 3.8. The Figure 3.6 shows the original Lena image and the Figure 3.7, Figure 3.8 and Figure 3.9 shows watermarked Lena image with quantization parameter 1, 4 and 6 respectively. The proposed CRED detector shows superior performance in comparison to the other detectors against common channel distortions such as filtering, adding of white noise and JPEG compression that are shown in the Figure 3.10 – Figure 3.13 in terms of the correlation coefficient between the embedded and the recovered watermark. We also use WDR which is a measure of the ratio of watermark energy to the host image energy and calculated as in Equation (2.35). It is used to evaluate the performance of the digital watermarking system against severe channel distortions and attacks.

In practical applications, the watermarked image may be exposed to some channel degradations and attacks. In that case, the performance of the watermark detector is very critical for the watermarking system. The simulations shown in Figure 3.10 and Figure 3.11, mean and median filtering is applied to the watermarked image with varying filter sizes respectively. The aim is to destroy the watermark detection capability. The

performance of the proposed CRED detector is compared with the MRD and DACD detector in terms of the correlation coefficient defined in Equation (3.14). The simulation results demonstrate that the proposed CRED detector is more robust against filtering attacks than the both MRD detector and DACD detector at the same filter size.

We also study the influence of AWGN on the performance of the detectors. The watermarked image is degraded by applying additive white Gaussian noise. The simulation shown in Figure 3.12 presents the corresponding correlation coefficient between the embedded and the recovered watermarks at different SNRs. The watermark correlation coefficient is still high enough to be detected at low SNR value if the proposed detection method is employed. The watermark correlation coefficient should be minimum 0.4 so that the receiver can properly detect it [35]. Hence, if we set the target correlation coefficient to 0.4; the proposed CRED detector achieves 2 dB SNR gain in comparison to the DACD detector. It also achieves 9 dB SNR gain in comparison to the MRD detector as given detailly in the Appendix A. In addition, we conclude that the proposed CRED detector is more robust against AWGN than the MRD detector and CRED detector at the same SNR.

The effects of lossy compression on watermark detection are shown in Figure 3.13. The watermarked image is exposed to the JPEG compression with varying quality factors in this simulation. If we evaluate the performances at the same JPEG quality factor, we can claim that the proposed CRED detector is more robust against JPEG compression than the other detectors used in the quantization based watermarking system. In addition, the performance of the proposed CRED detector is increased with the increasing JPEG quality factor. For example; when we set the target correlation coefficient to 0.4; the proposed CRED detector decreases the JPEG quality factor from 29 to 25 in comparison to the DACD detector. It also decreases the JPEG quality factor from 71 to 25 in comparison to the MRD detector as given detailly in the Appendix A. In other words, if the receiver employs the proposed detector, the transmitter can more aggressively compress the watermarked signal. Hence, it increases the amount of information to be sent.

We also investigate the effects of Low-Pass Filtering on the BER of the recovered watermark in the simulations shown in Figure 3.14- Figure 3.17. The formula of the low-pass filter is shown below:

$$h(m,n) = \frac{\mu_f^{\sqrt{m^2+n^2}}}{K} \tag{3.15}$$

where $K = \sum_{m=1}^{M}\sum_{n=1}^{N} h(m,n)$, μ_f denotes the filter parameter. In these experiments, the watermarked image is exposed to the low-pass filtering attack at various filter sizes and with various filter parameters. As the value of the filter parameter increases, the performances of the detectors decrease. In addition, filter size affects the watermark correlation coefficient. The proposed CRED detector is more robust than the other detectors at the same filter size. It also increases the correlation coefficient at the same filter parameter.

The BER is used as another performance metric to compare the performance of the proposed CRED detector with the MRD detector and DACD detector. The experiment shown in the Figure 3.18 – Figure 3.27, we change the quantization parameter (Q) from 1 to 6 and obtain WDR values in the -41dB to -20 dB range associated with these quantization parameters. The watermarked image is exposed to mean filtering, median filtering, and Gaussian low-pass filtering attack in the simulations shown in the Figure 3.18 – Figure 3.22 respectively. For example, the watermarked image is exposed to *3x3* mean filtering attack in simulation shown in Figure 3.19, if we set the target BER to 10^{-4} in the simulation shown in Figure 3.25, the proposed CRED detector achieves 4 dB WDR gain in comparison to the DACD detector. On the other hand, the MRD detector can not attain the target BER as given detailly in the Appendix A. The proposed detector is more robust than the others at the same WDR value in these simulations. In addition, the robustness of the watermarked image is tested against AWGN attack at 15 dB, 20 dB and 25 dB SNR in simulations shown in Figure 3.23 - Figure 3.25 respectively. If we set the target BER to 10^{-4} in the simulation shown in Figure 3.25, the proposed CRED detector achieves 5 dB WDR gain in comparison to the DACD detector. On the other hand, the MRD detector can not attain the target BER as given detailly in the Appendix A. Thus, we conclude that the

proposed CRED detector is more robust against AWGN than the MRD detector and CRED detector at the same SNR. Finally, the watermarked image is compressed with JPEG compression with quality factor 30 and 70 and its robustness is tested in simulations shown in Figure 3.26 - Figure 3.27 respectively. For example, when we set the target BER to 10^{-3} in simulation shown in the Figure 3.27, the proposed CRED detector achieves 2 dB WDR gain in comparison to the DACD detector. On the other hand, MRD detector can not attain the target BER as given detailly in the Appendix A.

In these simulations, as we decrease the value of the quantization parameter, WDR increases, hence, BER of the detectors decreases. However, as we decrease the watermark power via increasing the quantization parameter, the BER increases independently from the employed detector. In order to achieve a low BER while keeping an acceptable image quality one has to compromise between the WDR and PSNR which are given as a function of quantization parameter in Table 3.1. Also, the perceptual quality of the watermarked images can be subjectively evaluated from the Figure 3.6 - Figure 3.9 by using various quantization parameter such Q = 1, 4 and 6.

Quantization Parameter (Q)	WDR [dB]	PSNR [dB]
1	-20,0147	25.6803
2	-29,9845	35.1969
3	-34.3355	39.3697
4	-37,2580	42.3996
5	-39.3664	44.8551
6	-41.0229	46.2361

Table 3.1 : PSNR and WDR Results of the Watermarked Lena Image as a Function of Quantization Parameter (Q)

Figure 3.6 : Original Lena Image used as Host Signal

Figure 3.7: Watermarked Lena Image with $Q = 1$

Figure 3.8: Watermarked Lena Image with $Q = 4$

Figure 3.9: Watermarked Lena Image with $Q = 6$

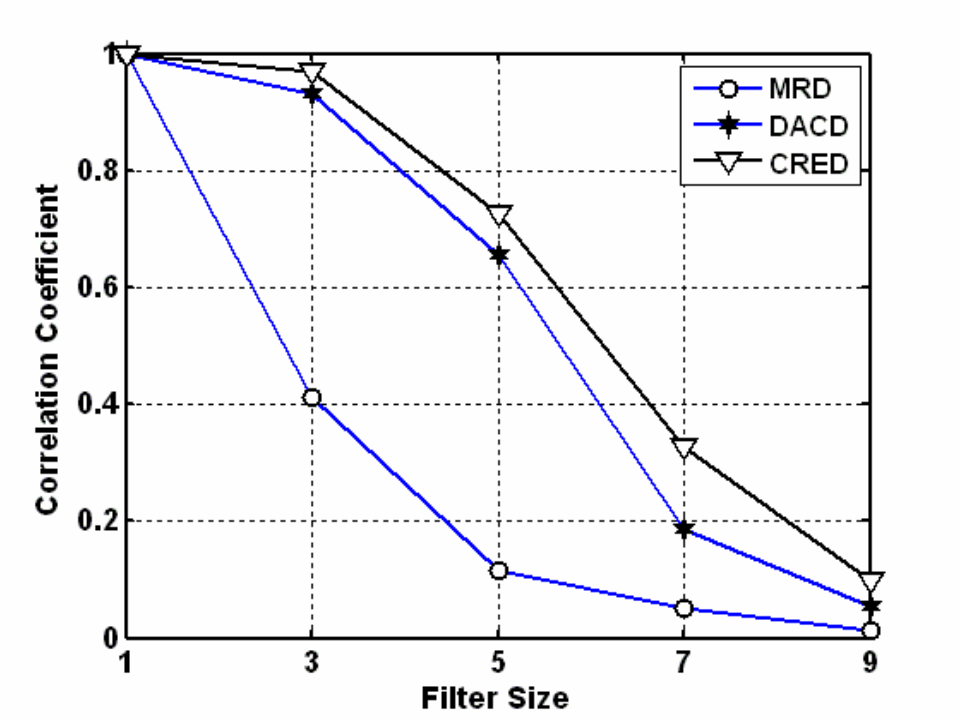

Figure 3.10: Detector Performances Against Mean Filtering Attack

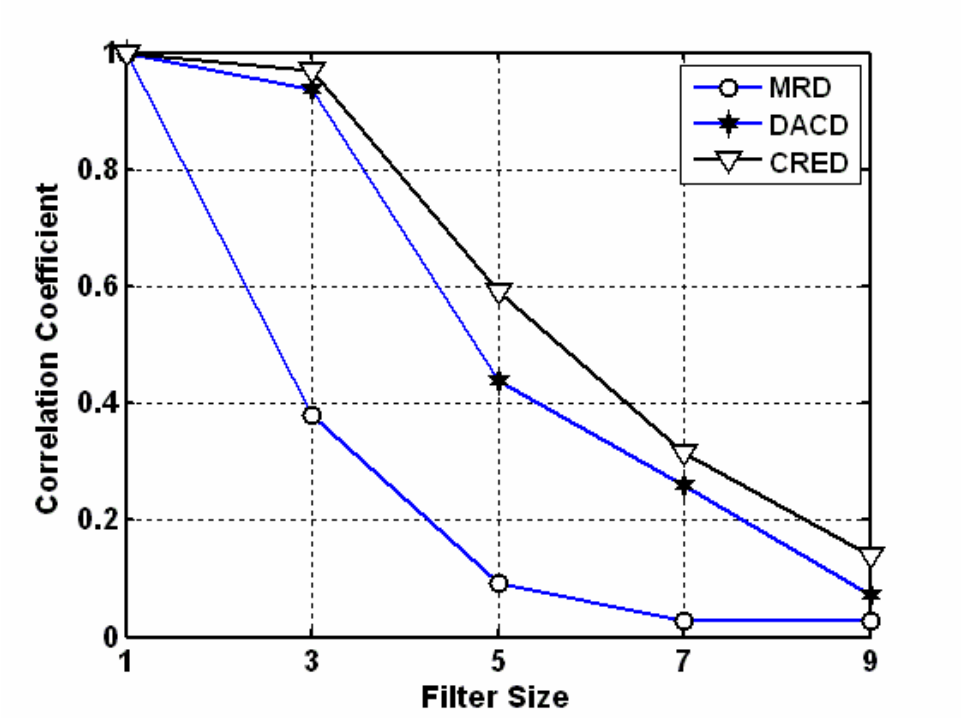

Figure 3.11: Detector Performances Against Median Filtering Attack

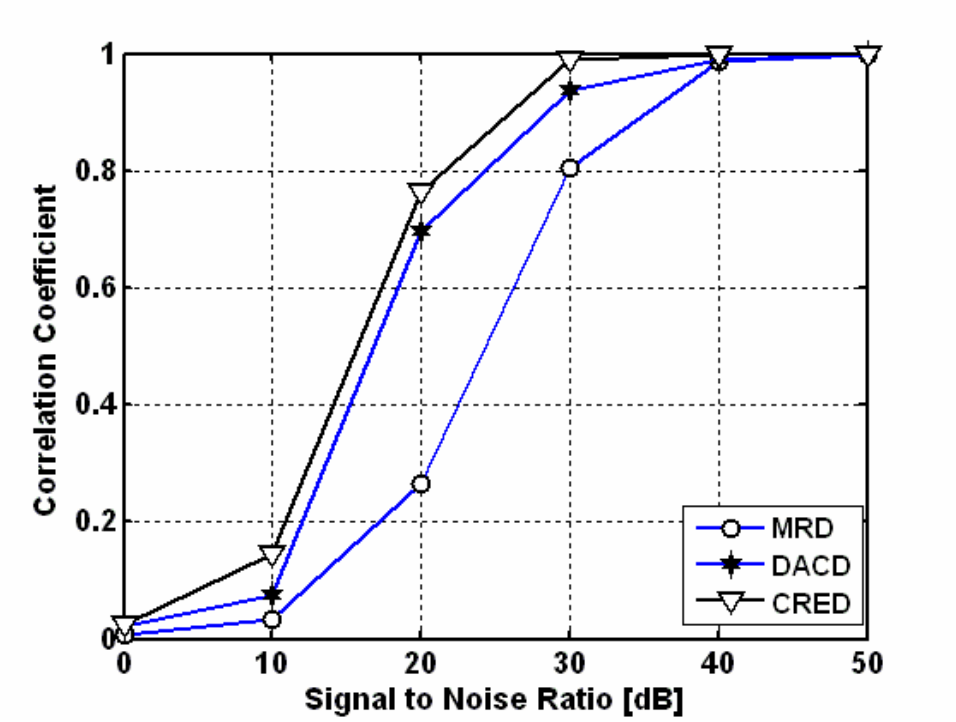

Figure 3.12: Detector Performances Against AWGN Attack

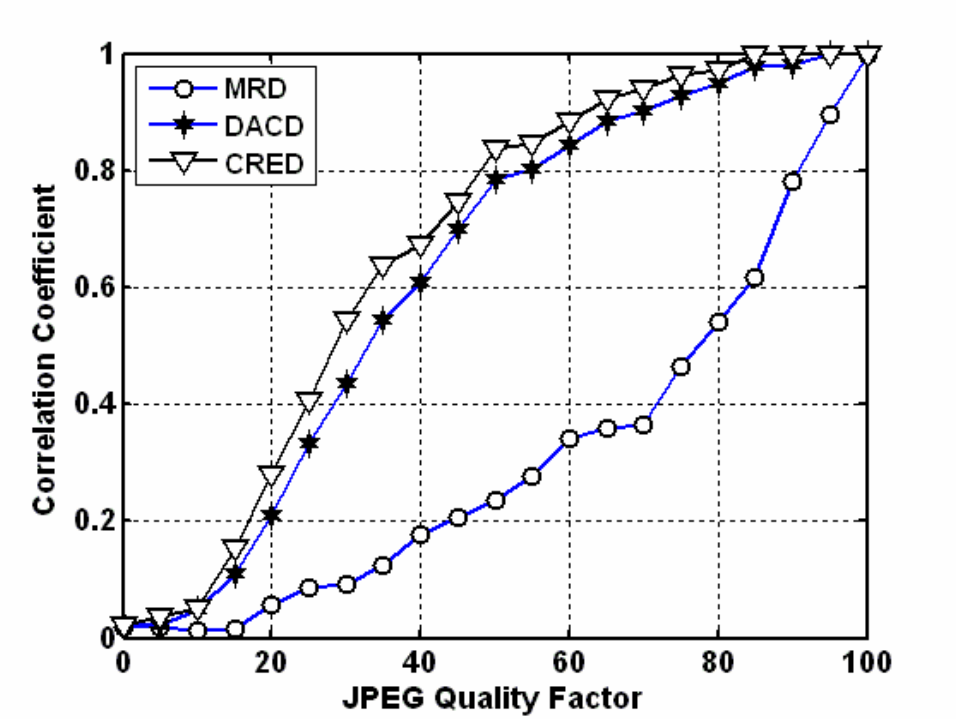

Figure 3.13: Detector Performances Against JPEG Compression Attack

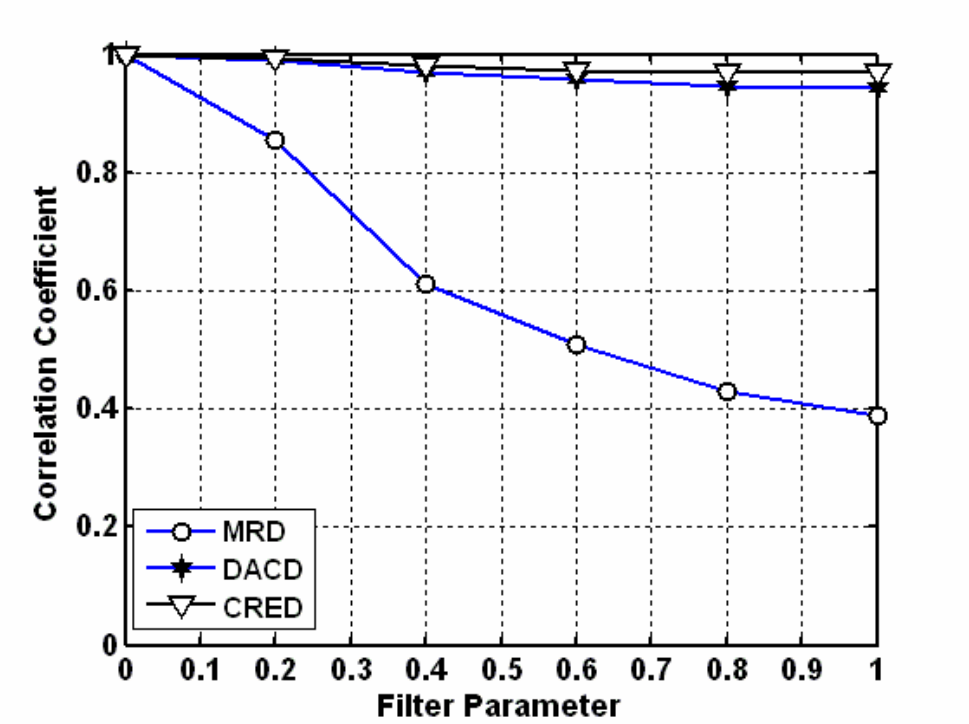

Figure 3.14 : Detector Performances Against *3x3* Gaussian Low-Pass Filter Attack

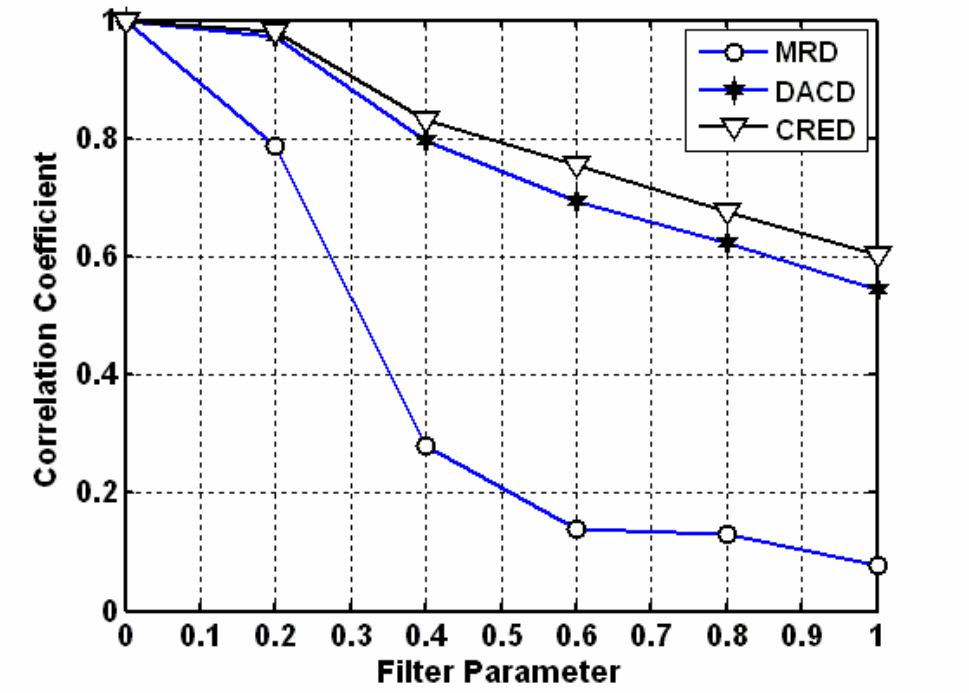

Figure 3.15: Detector Performances Against *5x5* Gaussian Low-Pass Filtering Attack

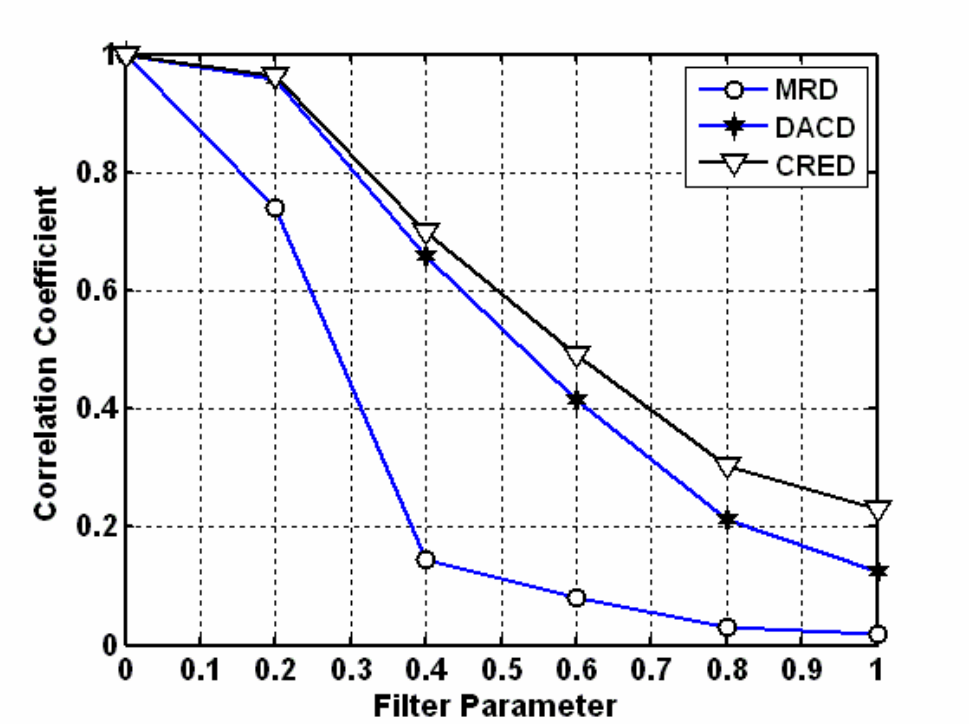

Figure 3.16: Detector Performances Against *7x7* Gaussian Low-Pass Filtering Attack

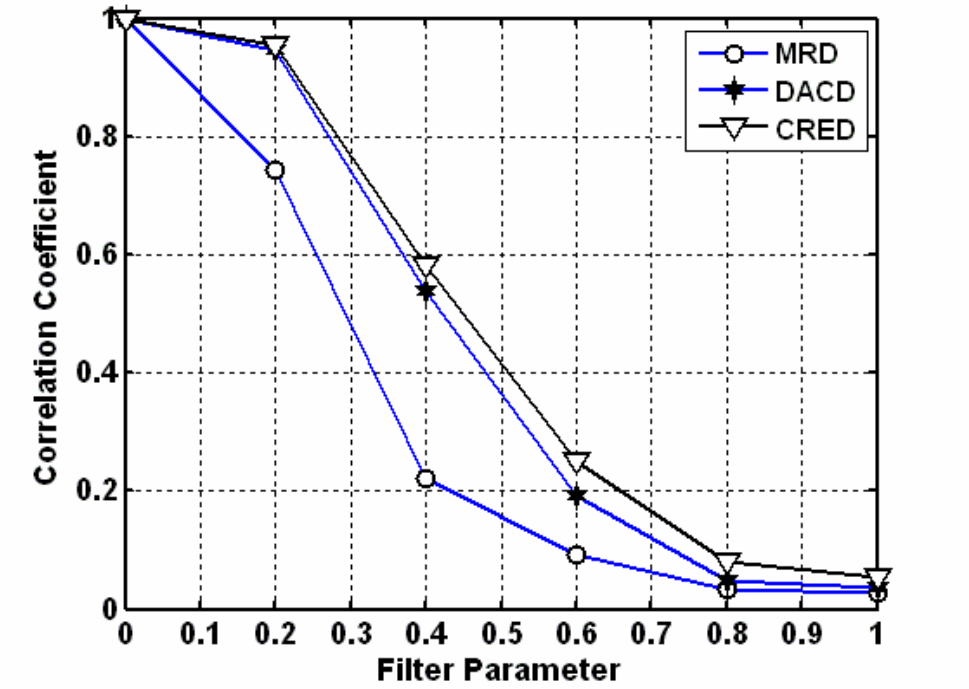

Figure 3.17: Detector Performances Against *9x9* Gaussian Low-Pass Filtering Attack

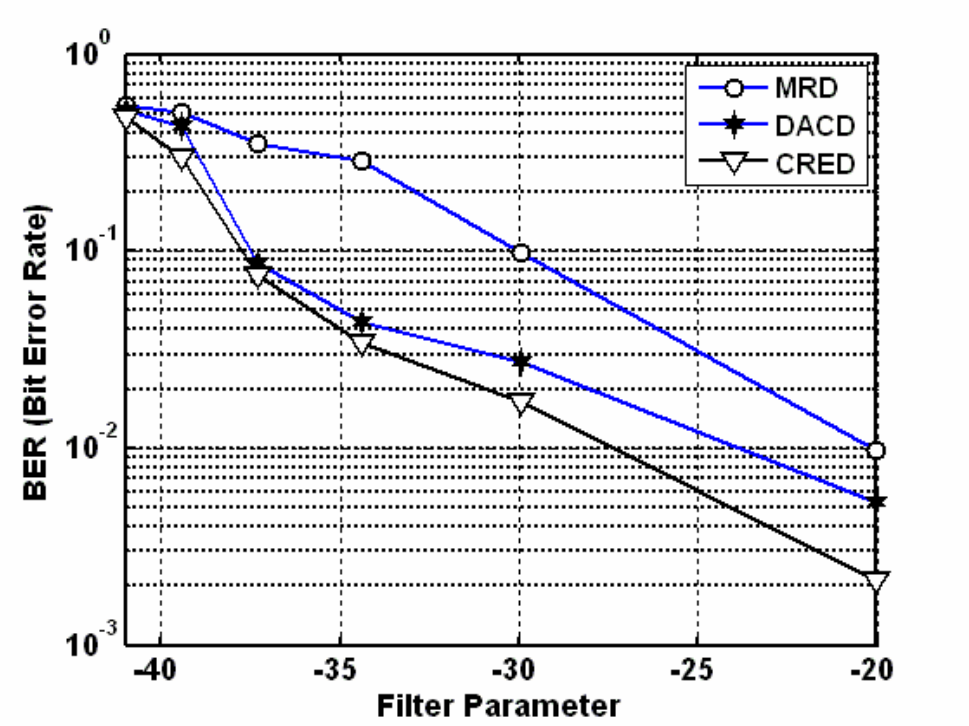

Figure 3.18: BER Performance of the Detectors versus WDR Against *5x5* Gaussian Low-Pass Filter with Parameter 0.4

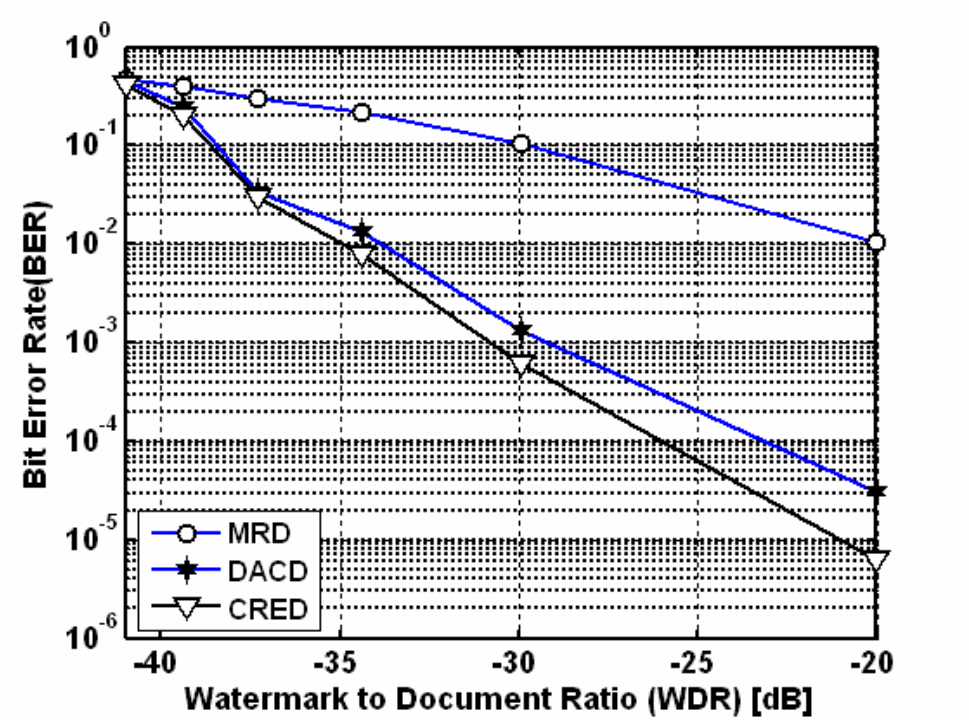

Figure 3.19: BER Performance of the Detectors versus WDR Against *3x3* Mean Filtering Attack

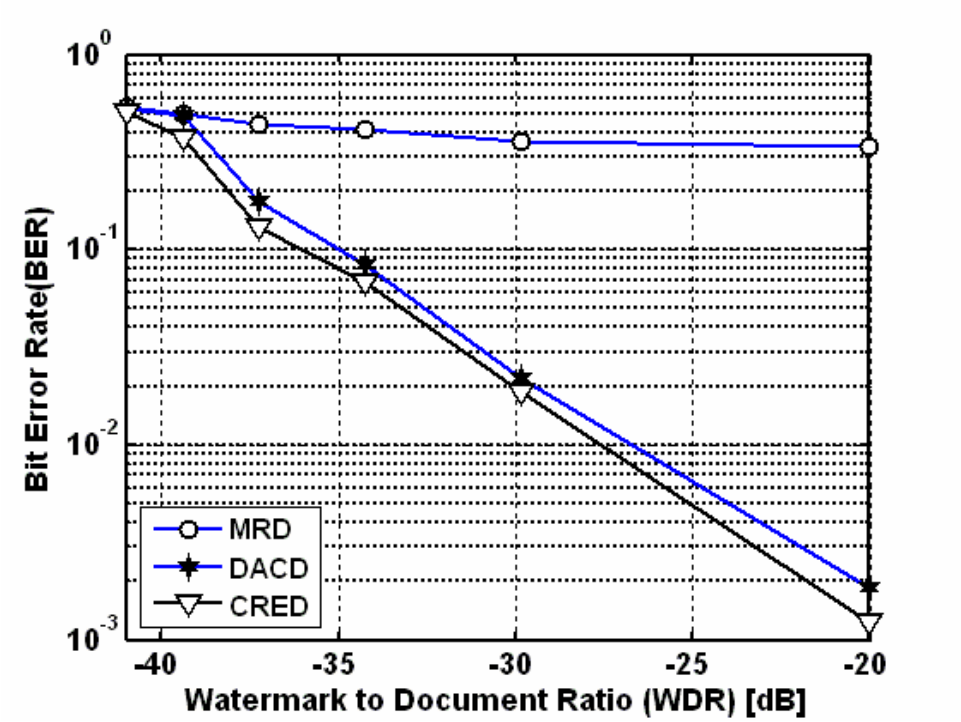

Figure 3.20 : BER Performance of the Detectors versus WDR Against *5x5* Mean Filtering Attack

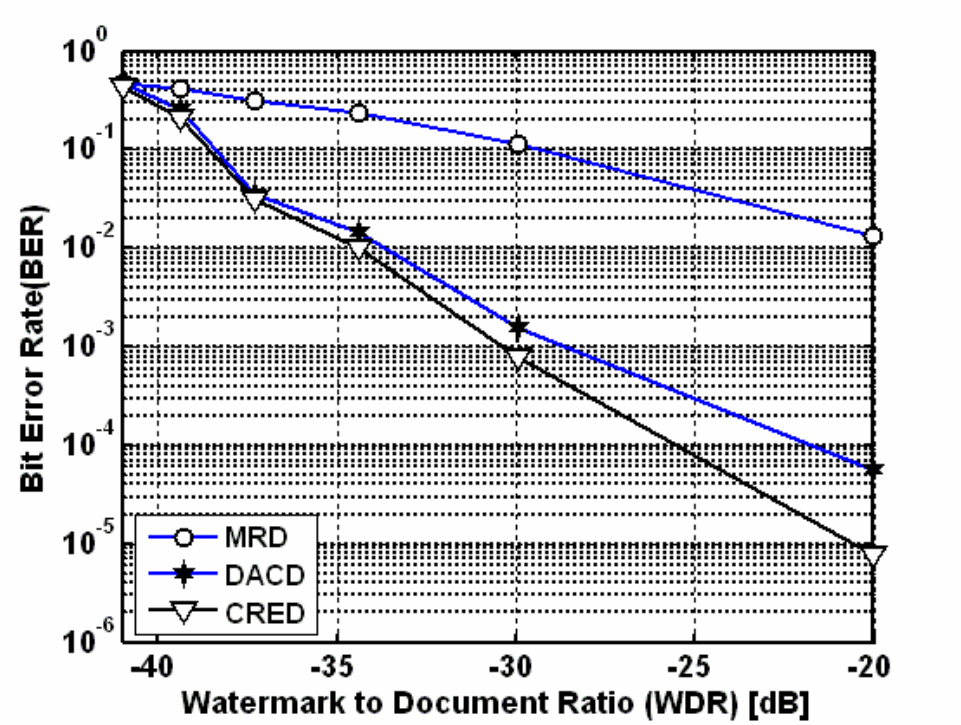

Figure 3.21: BER Performance of the Detectors versus WDR Against *3x3* Median Filtering Attack

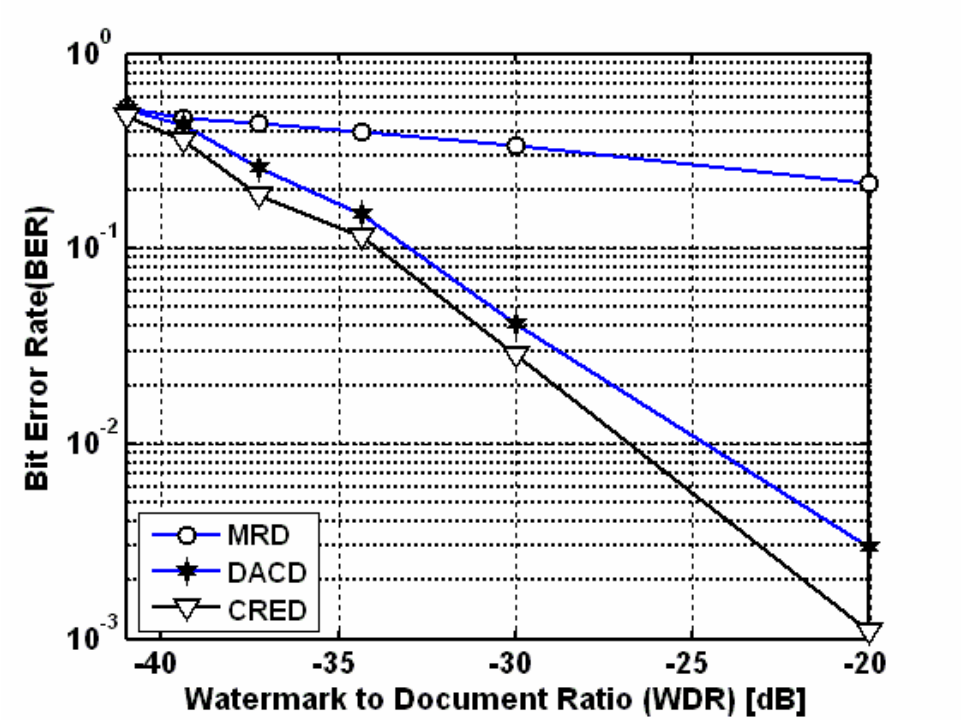

Figure 3.22 : BER Performance of the Detectors versus WDR Against *5x5* Median Filtering Attack

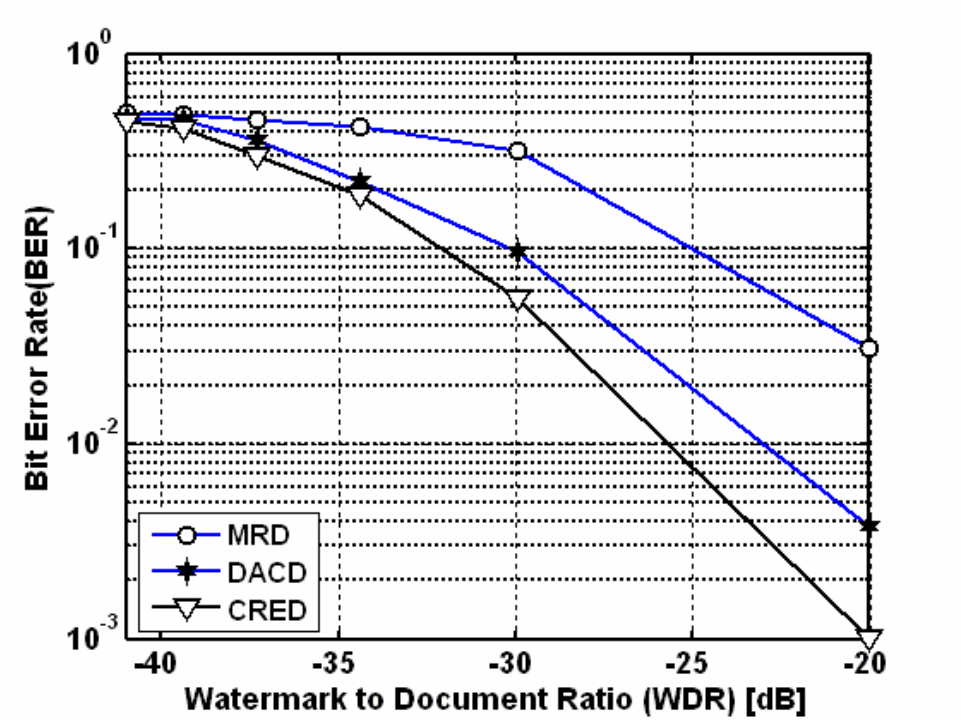

Figure 3.23 : BER Performance of the Detectors versus WDR Against AWGN Attack with 15 dB

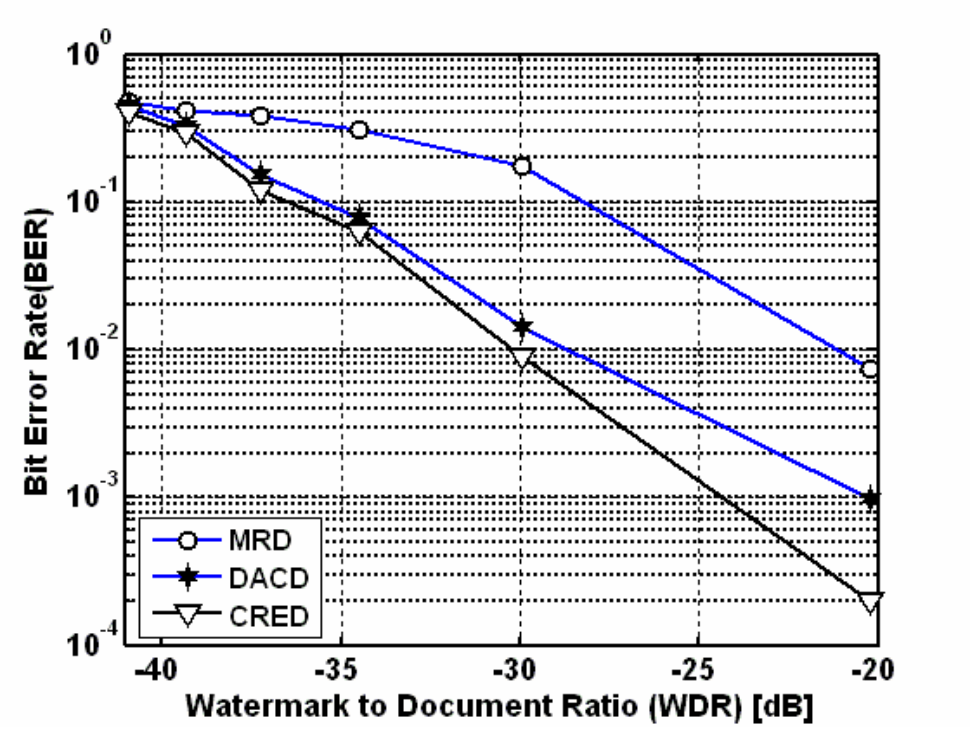

Figure 3.24 : BER Performance of the Detectors versus WDR Against AWGN Attack with 20 dB

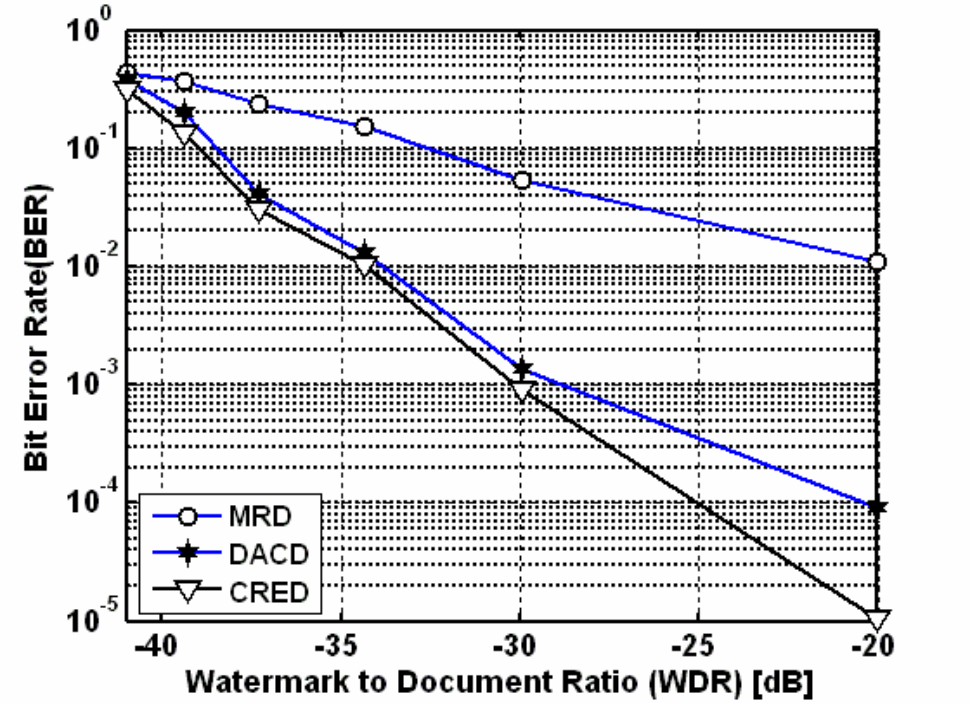

Figure 3.25: BER Performance of the Detectors versus WDR Against AWGN Attack with 25 dB

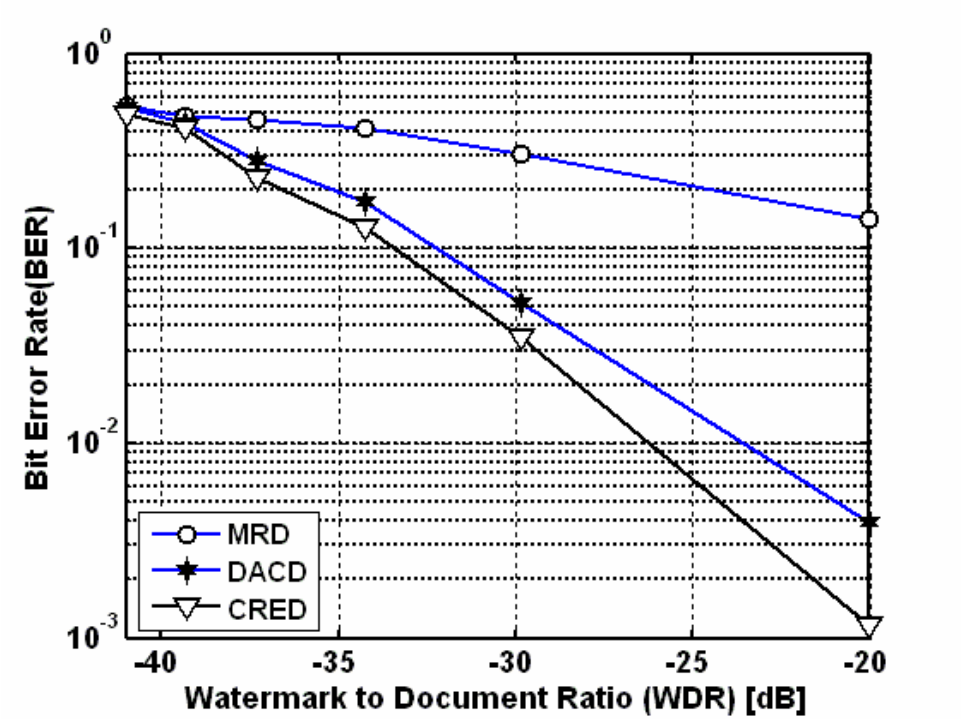

Figure 3.26 : BER of Performance of the Detectors versus WDR Against JPEG Compression with Quality 30

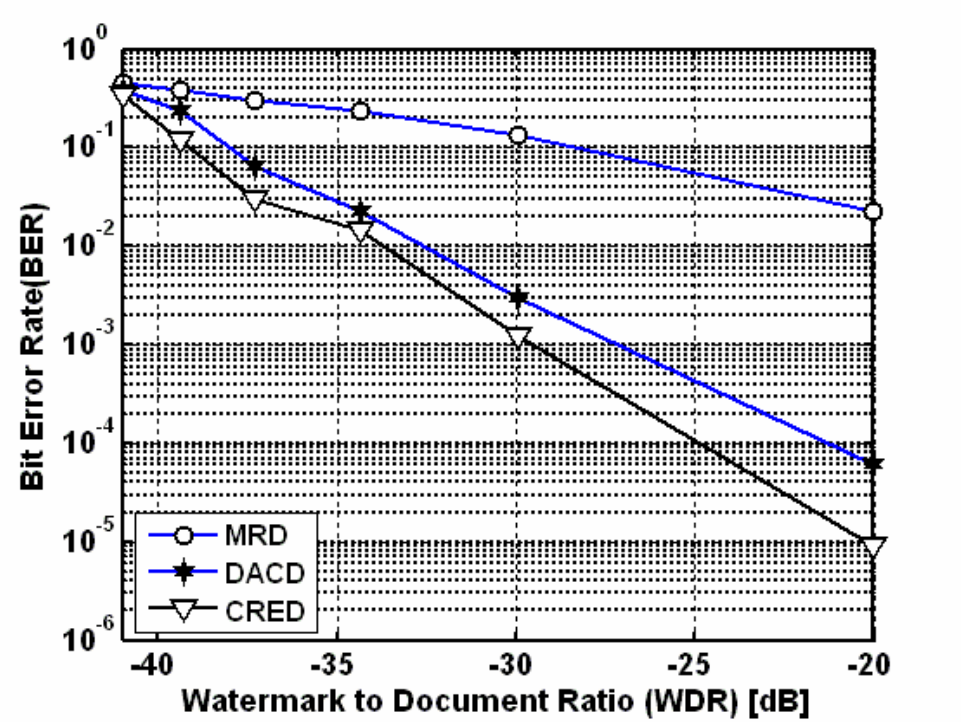

Figure 3.27 : BER of Performance of the Detectors versus WDR Against JPEG Compression with Quality 70

3.5. Conclusions

In this chapter, we develop a new blind detection method for quantization based watermarking system in DWT domain [36]. We apply the communication theory principles of diversity, channel estimation and threshold in order to improve the robustness of the system. This system does not vulnerable from the host signal interference problem. We consider the importance of a watermark detection stage which makes use of information concerning the attacker's actions to optimally estimate the watermark. By optimal we mean that the probability of bit error for watermark detection is minimized. We develop a new detection scheme that increases the detection performance of the watermarking system against channel distortions and attacks. In this scheme, first, the watermark sequence is repeatedly embedded within the host signal to provide diversity and to combat a broad class of degradations. Then, we model the digital watermarking system as a communication channel. Each embedded watermark repetition is modelled as travelling through watermark channel. The proposed detection method uses the reference watermarks in order to determine the reliabilities of the watermark channels. The unreliable watermark estimates decreases the performance of the system as in all estimation problems. The main contribution of the proposed detector is to employ a channel parameter to each of the watermark channels by first and second order statistics of the watermark channel reliabilities and the eliminating the unreliable watermark estimates by using the proposed threshold scheme. The proposed CRED detector is more robust against common channel distortions such as addition of white noise, filtering, lossy compression and decreases the BER for a given WDR and SNR. In addition, it, especially, shows superior performance in terms of bit error rate and correlation coefficient at the high WDR and SNR values. For example, if we set the target BER to 10^{-3} when the watermarked image is exposed to JPEG compression with quality factor 70, the proposed CRED detector achieves 7 dB WDR gain in comparison to the DACD detector. On the other hand, the MRD detector can not attain the target BER as given detailly in the Appendix A. Moreover, when we set the target correlation coefficient to 0.8; the proposed CRED detector achives 9 dB SNR gain in comparison to the DACD detector. It also achieves 3 dB SNR in comparison to the MRD detector as given detailly in the Appendix A. Finally, when we set the target correlation coefficient to 0.9; the proposed CRED detector decreases the JPEG quality factor from 76 to 62 in

comparison to the DACD detector. It also decreases the JPEG quality factor from 97 to 62 in comparison to the MRD detector as given detailly in the Appendix A. In other words, if the receiver employs the proposed CRED detector, the watermarked image can be compressed more aggressively the transmitter.

4. ROBUST NON-BLIND DETECTION FOR DCT DOMAIN WATERMARKING SYSTEM

In this chapter, we present non-blind digital watermarking system in DCT domain in Section 4.1. In this application, host image is available at the receiver side. In section 4.2, we introduce the employed detectors such as the proposed CRED watermark detector, MRD watermark detector and DACD watermark detector. These detectors explained in detail in Chapter 3. Then, we explain the image restoration algorithms applied to the degradated watermarked image in Section 4.3. We test and compare their performances against channel distortions, attacks and apply image restoration algorithms in Section 4.4. Finally, we conclude the overall system in Section 4.5.

4.1. Additive-Multiplicative Digital Watermarking System in DCT Domain

In the number of developing digital watermark algorithms, the embedding processes are carried out by using additive or additive-multiplicative method. The digital watermarking systems modify the host signal and embed the watermark information safely. Thus, the watermark should be embedded by taking into account the perceptual constraints in these systems. In addition, they should detect the embedded watermark in case of the channel distortions and attacks. The digital watermarking system, which Piva *et. al.* [37] proposed, achieves the trade-off between the perceptibility and the robustness by properly choosing the watermark embedding region and insertion strength. Actually, Piva *et. al.* [37] suggested a digital watermarking system based on the DCT that is the core of the JPEG technology. In this chapter, we develop the non-blind digital watermarking system that is very similar to the system presented in [37].

4.1.1. The Proposed Watermark Embedding Process

In the watermark embedding process, which is shown in Figure 4.1 - Figure 4.3, the host image of size *NxN* is transformed into DCT domain. The DCT coefficients are re-ordered by the using zig-zag scan. This method re-orders all the DCT coefficients from low frequency to high frequency. For most images, it is equivalent to sorting according to importance, since the perturbation in the low frequency components is generally more perceivable to human eyes than high frequency components. The main idea behind the selection criteria for the watermark embedding region is to preserve the perceptual quality while being robust the system against channel distortions and both intentional and unintentional attacks.

The way of the watermark embedding changes whether we use or not use the reference watermarks in order to characterize the watermark channel. If the watermarking system employs the DACD detector or the proposed CRED detector, the reference watermarks are used in the embedding process to characterize the channel distortions and attacks. Hence, we, first, generate the information and reference watermark sequences as described in Chapter 3 and [34], [36]. The information watermark sequence $\vec{m} = \left[m(1), m(2), ..., m(T) \right]$ of length T, whose elements are from the set $\{\pm 1\}$, is randomly generated. Also, the reference watermark sequence $\vec{r} = \left[r(1), r(2), ..., r(T) \right]$ of length T, whose elements are from the set $\{\pm 1\}$, is randomly generated. We combine the information and reference watermark to obtain the combined watermark sequence which is embedded into the host signal and denoted as $\vec{w}_c = \left[m(1), r(1), m(2), r(2), ..., m(T), r(T) \right]$. Then, the combined watermark sequence is repeated K times to obtain repetition-coded watermark vector $\vec{w}_r$ of length $T_r = K \times 2 \times T$. Next, we generate a spread-spectrum sequence $\vec{p}_c$ whose elements are from the set $\{\pm 1\}$ and length is $T_r = K \times 2 \times T$ using the security key K_1. Finally, we multiply the repetition-coded watermark vector $\vec{w}_r$ with the spread-spectrum sequence $\vec{p}_c$ to obtain the watermark sequence $\vec{w}$.

In the second case, if the digital watermarking system employs MRD watermark detector, there is no need to use the reference watermarks. In that case, only the information watermark $\vec{m} = \left[m(1), m(2), ..., m(T) \right]$ of length T, whose elements are from the set $\{\pm 1\}$, is randomly generated. Then, the watermark sequence is repeated $2xK$ times to obtain repetition-coded watermark vector $\vec{w}_r$ of length $T_r = 2 \times K \times T$. Next, we generate a spread-spectrum sequence $\vec{p}_c$ whose elements are from the set $\{\pm 1\}$ and length is $T_r = 2 \times K \times T$ using the security key K_1. Finally, we multiply the repetition-coded watermark vector $\vec{w}_r$ with the spread-spectrum sequence $\vec{p}_c$ to obtain the watermark sequence $\vec{w}$. Thus, we embed the constant number of watermark bits to the host image in both cases. In this scheme, we do not employ Watson's perceptual model since this model is valid in the *8x8* block DCT domain. On the other hand, we employ zig-zag scan to achieve a trade-off between the perceptual quality and the robustness.

Finally, we embed watermark sequence bits into the selected DCT coefficients as proposed in [37] by leaving the first L coefficients intact and adding the watermark sequence bits on the next M coefficients. Hence, after re-ordering the host image coefficients in DCT domain by using the zig-zag scan, we embed the watermark by using the additive-multiplicative embedding method as follows:

$$\vec{y}(i) = \vec{x}(i)\left(1 + \gamma \vec{w}(i)\right) \tag{4.1}$$

where $i=1,2,...,KxT$, K denotes the total number of embedded information and reference watermarks, T denotes the length of embedded watermark, $\vec{y}(i)$ denotes the watermarked coefficients in DCT domain, $\vec{x}(i)$ denotes the host image coefficients to be watermarked in DCT domain, $\vec{w}(i)$ denotes the watermark sequence and γ denotes insertion strength. Then, the watermarked coefficients re-ordered by using the inverse zig-zag scan in DCT domain. Finally, we obtain the watermarked image by performing inverse DCT.

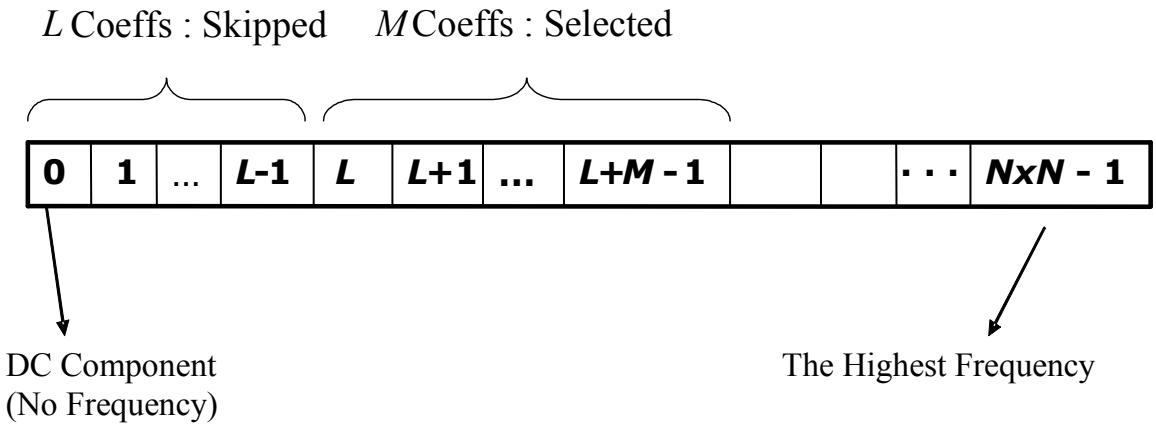

Figure 4.1 : Re-Ordered DCT Coefficient of *NxN* Host

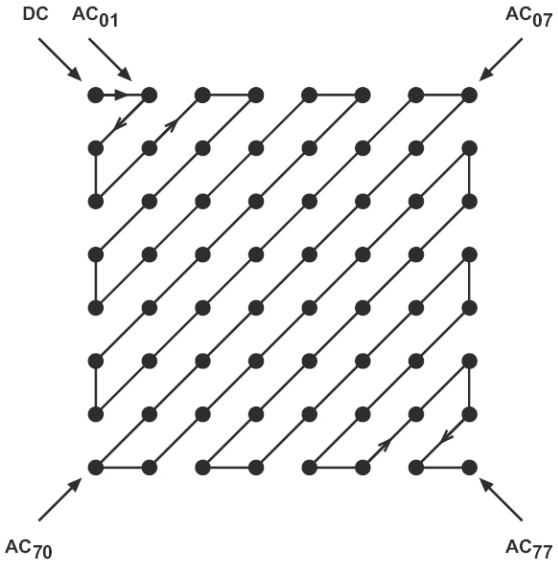

Figure 4.2 : DC and AC Coefficients of *8x8* DCT Block

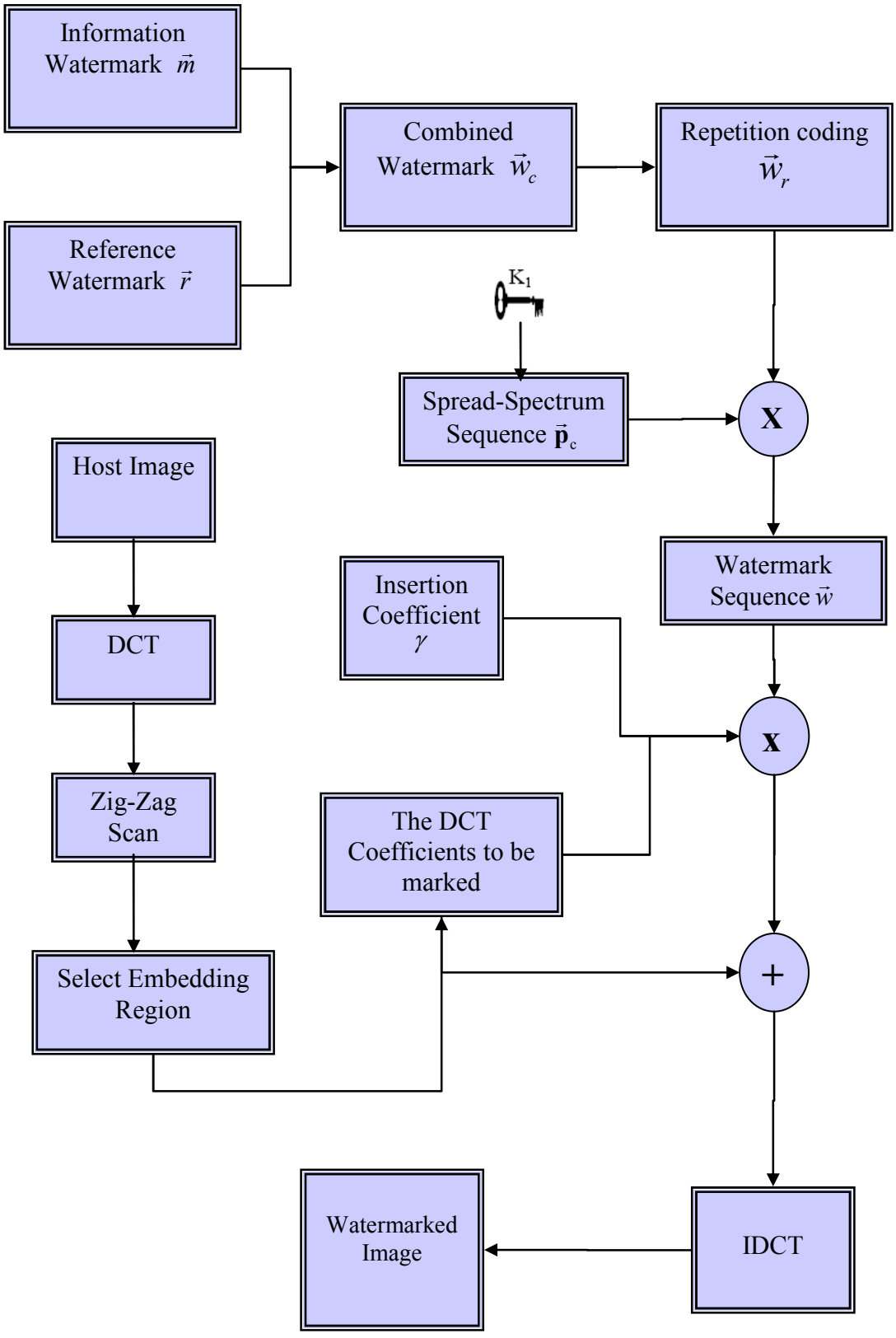

Figure 4.3 : The Watermark Embedding Process

4.1.2. The Watermark Extraction Process

Since we employ non-blind digital watermarking system, we have the host image at the receiver side. Hence, first, we compute the *NxN* DCT of both the watermarked image and host image in the extraction process as illustrated in the Figure 4.4. The DCT coefficients of both host image and watermarked image are re-ordered by using the zig-zag scan. Then, we subtract the watermarked image coefficients from the host image coefficients. The *L+1* to *L+M* DCT coefficients are selected since they are the coefficients in which the watermark sequence bits are embedded. Then, we re-generate the spread-spectrum sequence $\vec{p}_c$ whose length is $T_r = 2 \times K \times T$ using the security key K_1. Finally, the information and reference watermark bits are determined by using the sign function as follows:

$$\vec{w}(i) = \text{sgn}\left(\frac{\vec{y}(i) - \vec{x}(i)}{\vec{x}(i)\gamma} \right) \vec{p}_c(i) \tag{4.2}$$

where *i=1,2,...,KxT* , *K* denotes the total number of embedded information and reference watermarks, *T* denotes the length of information watermark sequence, $\vec{y}(i)$ denotes the watermarked image coefficients, $\vec{x}(i)$ denotes the host image coefficients, $\vec{w}(i)$ denotes the watermark sequence bits, $\vec{p}_c(i)$ denotes the spread-spectrum sequence bits and γ denotes insertion strength.

Finally, we determine the embedded watermark sequence bits by choosing the proper detection method. Thus, we recover the information watermark sequence bits and reference watermark sequence bits from the watermark sequence $\vec{w}(i)$.

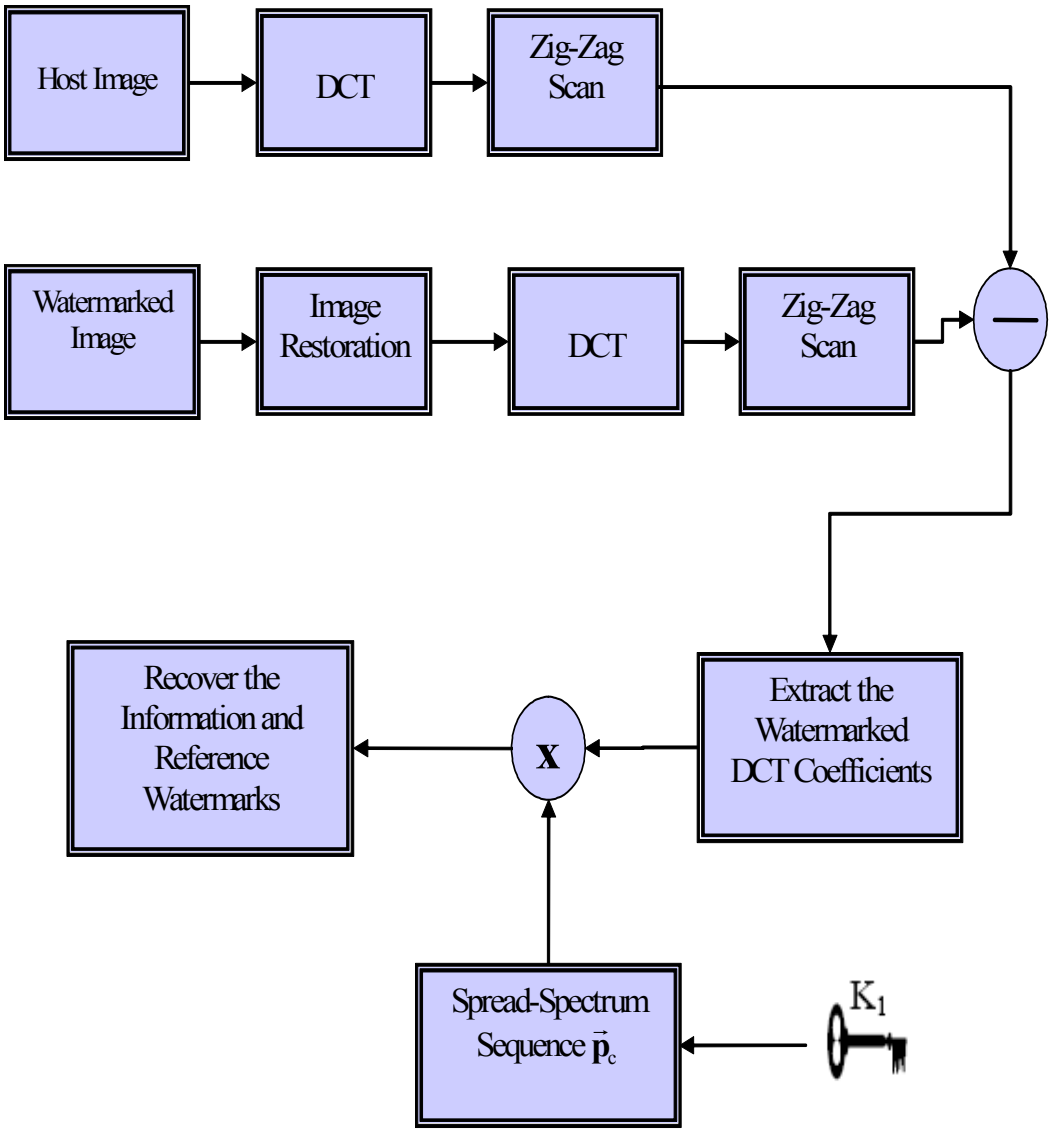

Figure 4.4 : The Watermark Extraction Process

4.2. The Proposed Watermark Detection Process

In this section, we employ the majority rule based watermark detector (MRD), diversity and attack characterization based watermark detector (DACD) and the proposed channel reliability estimation based watermark detector (CRED) as described in greater detail in Chapter 3. Then, we test and compare the performances of these

detectors in the non-blind watermarking system in DCT domain against various channel distortions, intentional and unintentional attacks such as mean filtering, median filtering, JPEG compression and AWGN.

4.3. Simulation Results and Discussions without Image Restoration Algorithms

In this chapter, we use the test image "Lena" of size *512x512* as a host image in all the simulations. In addition, we embed the randomly generated information and reference watermarks from the set {-1,1} into the host image as described in Chapter 3. In each simulation, 5000 experiments are done to test the performance of the detectors.

The selection of the watermark embedding regions is the one of the most important step in this algorithm. To what extent these regions can be invariant against attacks like filtering, compression and AWGN directly determines the how robust this digital watermarking system is. In order to obtain the simulation results, we chose to leave the first $L = 600$ DCT coefficients intact due to achieve the trade-off between the perceptual transparency and watermark energy. To test the performance of the majority rule based detector, we embed $2 \times K = 70$ randomly generated watermark whose elements are from the set {-1, 1}. Also, To test the performance of the proposed CRED detector and DACD detector, we embed $K = 35$ randomly generated information watermark and 35 randomly generated reference watermark whose elements are from the set {-1,1}. Therefore, in each experiment, we embed totally 17920 watermark bits into the host image constantly.

In experiments shown in Figure 4.5 - Figure 4.12, the insertion strength is set to 0.1 to achieve a trade-off between the perceptual quality and the robustness. As we increase the insertion strength, the power of the embedded watermark is increased. However, we lose the perceptual quality of the watermarked image as shown in Table 4.1.

We apply mean and median filtering attack to the watermarked image with various filter sizes in order to decrease the detection capability of the system in simulation shown in Figure 4.5 and Figure 4.6 respectively. We can claim from

simulation results that the proposed CRED detector is more robust against mean and median filtering attack than the MRD detector and DACD detector. On the other hand, we investigate the effects of Gaussian low-pass filter attack with various filter sizes and various filter parameters. The simulations shown in Figure 4.7 – Figure 10, the proposed CRED detector increases the watermark correlation coefficient at the same filter parameter. Thus, we conclude from the simulation results that the proposed CRED detector is more robust than the other detectors at the same filter size and with the same filter parameter.

Furthermore, we investigate the performance of the detectors against AWGN attack under various SNR values as shown in Figure 4.11. The proposed CRED detector shows the best performance among the employed detectors in terms of the correlation coefficient between the embedded and extracted watermark. For example, if we set the target correlation coefficient to 0.8; the proposed CRED detector achieves 2 dB SNR gain in comparison to the DACD detector. It also achieves 5 dB SNR gain in comparison to the MRD detector as given detailly in the Appendix B.

Then, we evaluate the performance of the watermark detectors against JPEG compression attack with varying quality factors which is shown in Figure 4.12. Since we embed the watermark by using the zig-zag scan, this makes the digital watermarking system more robust against JPEG compression as expected. The proposed CRED outperforms from the other watermark detectors, especially at low JPEG quality factors. In addition, when we set the target correlation coefficient to 0.9; the proposed CRED detector decreases the JPEG quality factor from 17 to 14 in comparison to the DACD detector. It also decreases the JPEG quality factor from 22 to 14 in comparison to the MRD detector as given detailly in the Appendix B. In other words, if the receiver employs the proposed detector, the transmitter can compress the watermarked signal with lower JPEG quality factors. Thus, it increases the amount of information to be sent.

The experiments shown in Figure 4.13 and Figure 4.14, we test and compare the BER performance of the watermark detectors with varying insertion strengths against mean filter attacks with filter size *3x3* and *5x5* respectively. When we evaluate these simulations at the same insertion coefficient level, the MRD detector shows the worst performance and the best performance belongs to the proposed CRED detector. Hence,

especially increasing the insertion strength, the proposed CRED detector improves the detection performance of the digital watermarking system against mean filtering attack which increases the correlation between the watermarked coefficients. Also, we evaluate the robustness of the watermark detectors against median filtering of size attack with *3x3* and *5x5* filter sizes as shown in Figure 4.15 and Figure 4.16. In these simulations, as the insertion increases, the watermark power increases. Hence, the BER performances of the watermark detectors are improved. Although the proposed CRED detector demonstrates superior performance, BER of the detectors is very high since the *5x5* median filtering is very strong attack. The proposed CRED watermark detector outperforms from the other detectors, especially, when the insertion strength is greater than 0.12. In addition, we test the BER performances of the detectors against Gaussian low-pass filter versus various insertion strengths in simulations shown in Figure 4.17 - Figure 4.19. The BERs of the recovered watermark decreases as the insertion strength increases in these simulations. Moreover, the proposed detector achieves lower BERs than the other detectors at the same insertion strength level.

In experiments shown in Figure 4.20 - Figure 4.22, the AWGN is added to the watermarked image with fixed SNR and various embedding strengths. In these simulations, we can observe the effects of the embedding strength over the BER performances of the watermark detectors at constant SNR. In these experiments, independent from the embedding strength, the proposed CRED detector is more robust to the AWGN attack at various SNRs. To investigate the effect of AWGN attack, we set insertion strength to 0.1 and add AWGN to the watermarked image with various SNRs as shown in Figure 4.23. In that simulation, the proposed CRED detector outperforms the other detectors, especially, at SNR values greater than 18 dB. In addition, when we set the target BER to 10^{-4}; the proposed CRED detector achieves 4 dB SNR gain in comparison to the DACD detector. It also achieves 7 dB SNR gain in comparison to the MRD detector as given detailly in the Appendix B.

We expect that the watermarking system to be robust against the JPEG compression since it is based on the zig-zag scan in DCT domain. The simulations that are shown in Figure 4.24 – Figure 4.27 demonstrate the robustness of the watermarking system against JPEG compression with various insertion strengths even if at low JPEG quality factors. However, we improve the detection performance of this system by using

the proposed CRED detector. In addition, we investigate the JPEG compression attack with different point of view. We set the insertion strength to 0.1 to make a trade-off between the perceptual quality and the robustness. Then, we evaluate the robustness of the detectors to JPEG compression with various quality factors. We conclude that the proposed CRED detector is more robust than MRD detector and the DACD detector in terms of BER.

Insertion Strength	PSNR [dB]	WDR [dB]
0.05	47.9463	-42.6374
0.06	46.3626	-41.0538
0.07	45.0237	-39.7148
0.08	43.8639	-38.5550
0.09	42.8408	-37.5320
0.10	41.9257	-36.6168
0.11	41.0978	-35.7889
0.12	40.3420	-35.0332
0.13	39.6468	-34.3379
0.14	39.0031	-33.6942
0.15	38.4038	-33.0950

Table 4.1 : PSNR and WDR values of Watermarked Lena Image with Various Insertion Strengths

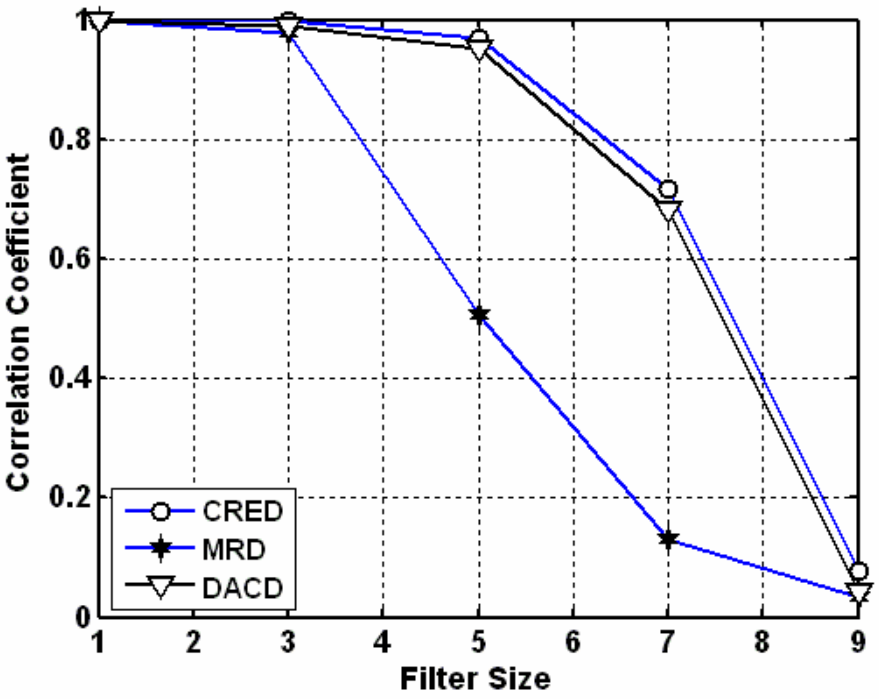

Figure 4.5 : Detector Performances Against Mean Filtering Attack

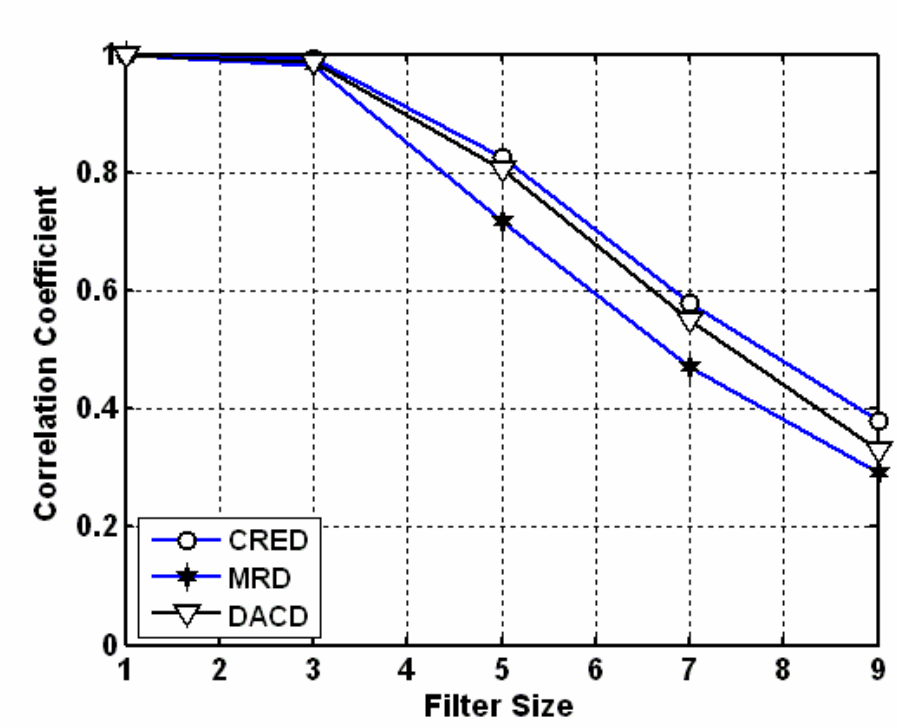

Figure 4.6 : Detector Performances Against Median Filtering Attack

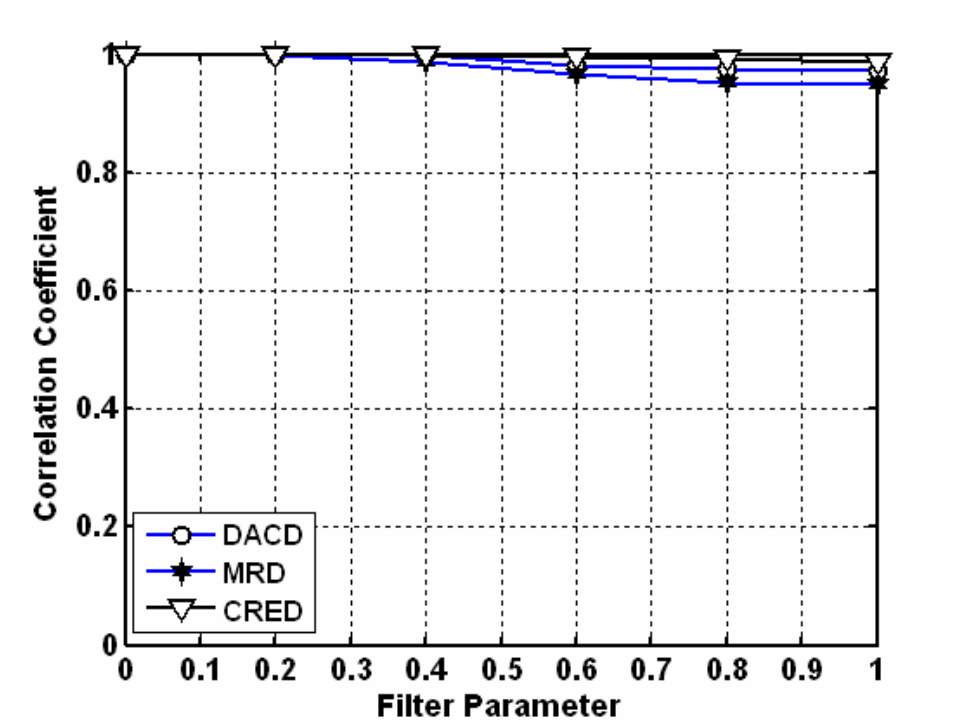

Figure 4.7 : Detector Performances Against *3x3* Gaussian Low-Pass Filter Attack

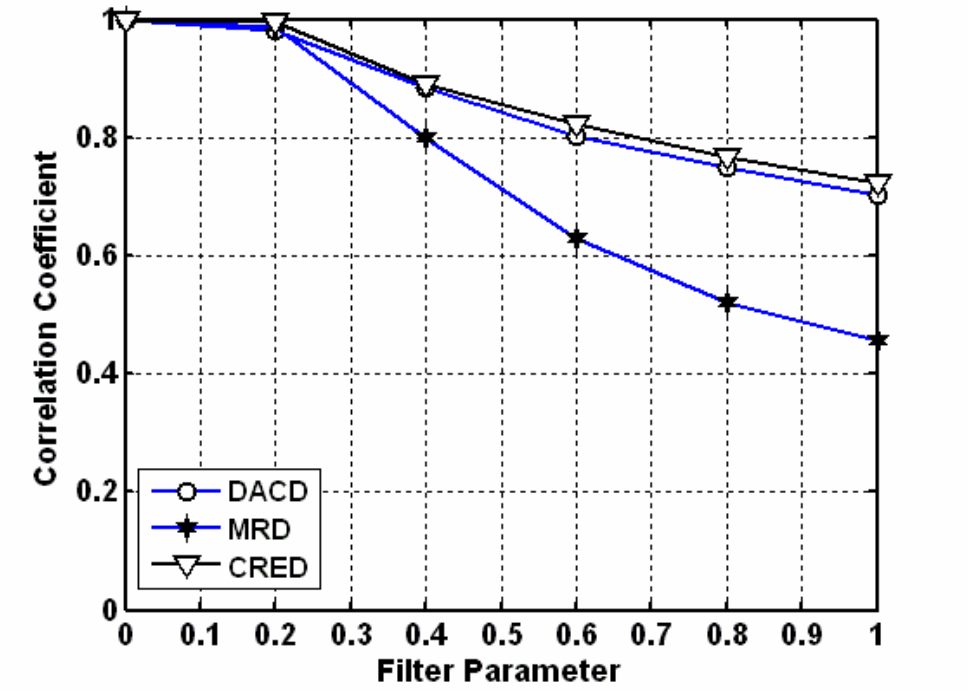

Figure 4.8: Detector Performances Against *5x5* Gaussian Low-Pass Filter Attack

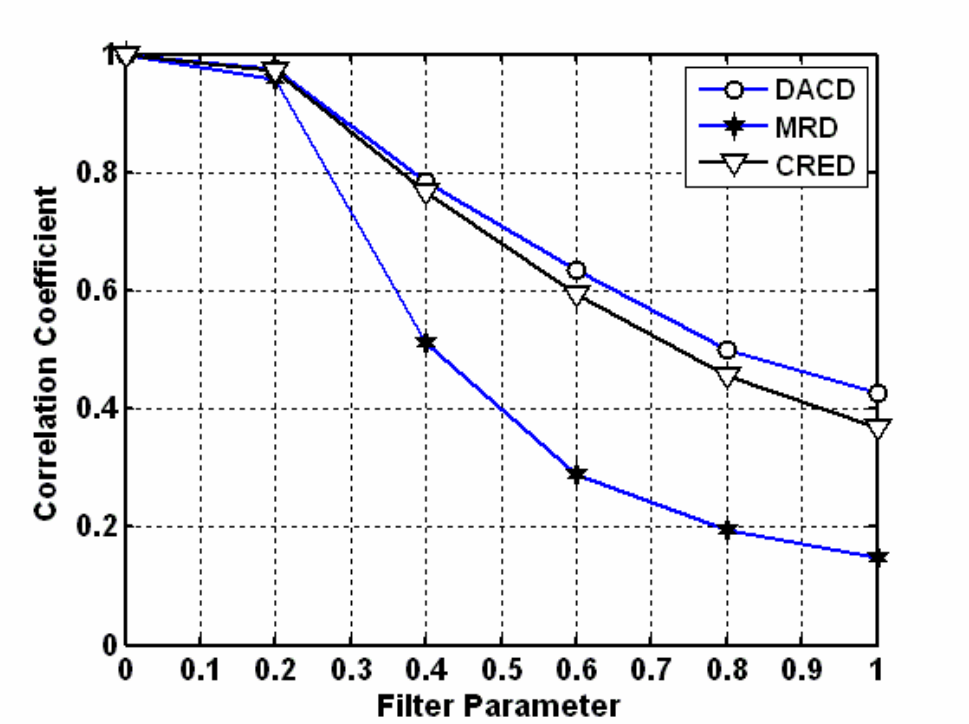

Figure 4.9: Detector Performances Against *7x7* Gaussian Low-Pass Filter Attack

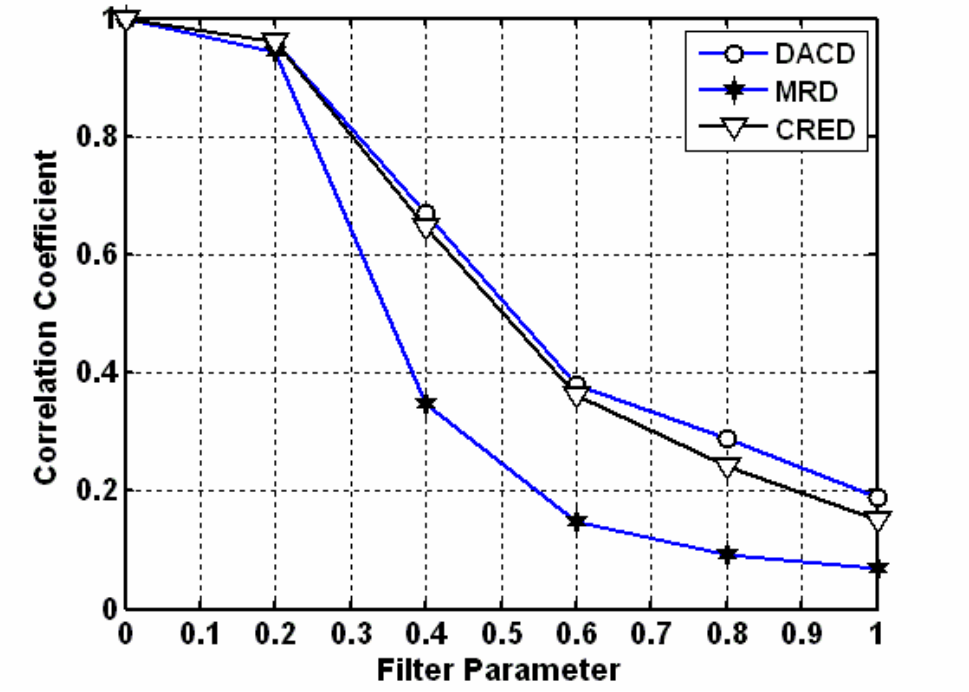

Figure 4.10: Detector Performances Against *9x9* Gaussian Low-Pass Filter Attack

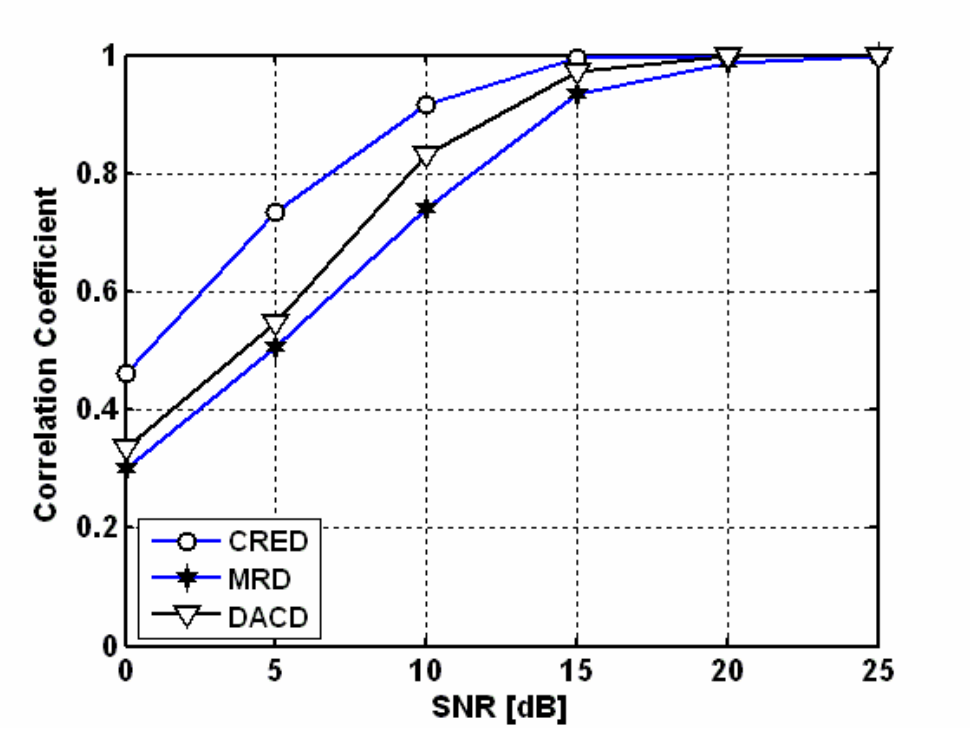

Figure 4.11 : Detector Performances Against AWGN Attack

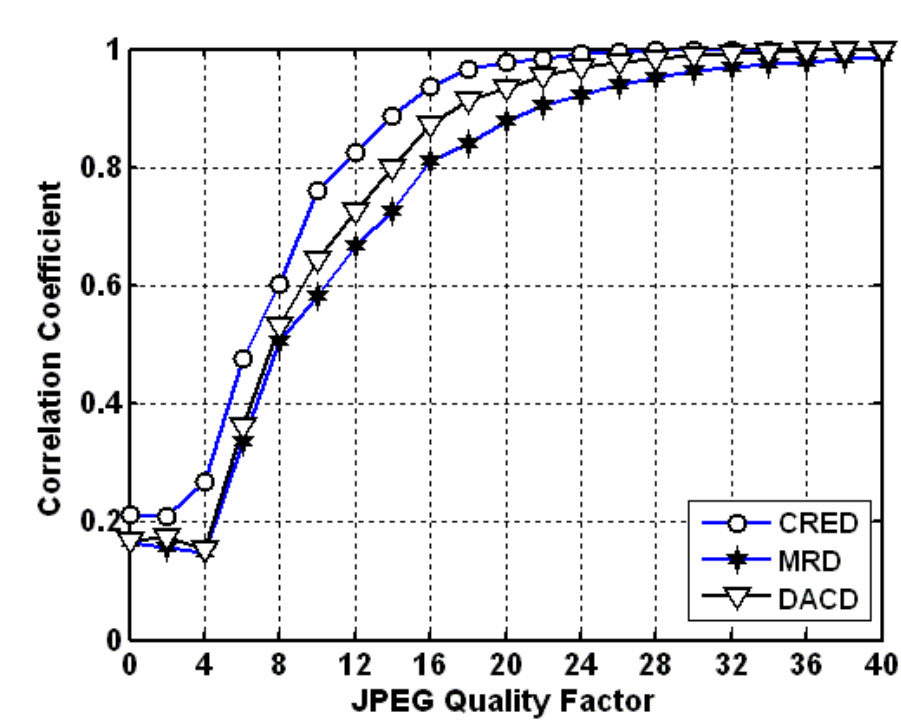

Figure 4.12 : Detector Performances Against JPEG Compression Attack

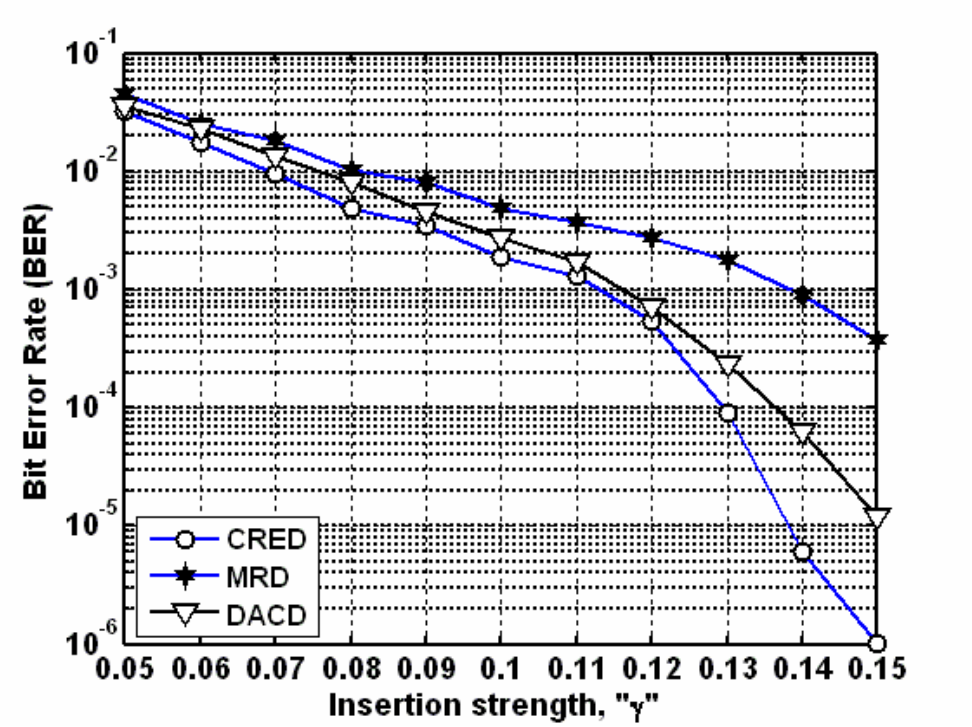

Figure 4.13 : Detector Performances Against *3x3* Mean Filtering Attacks versus Various Insertion Strengths

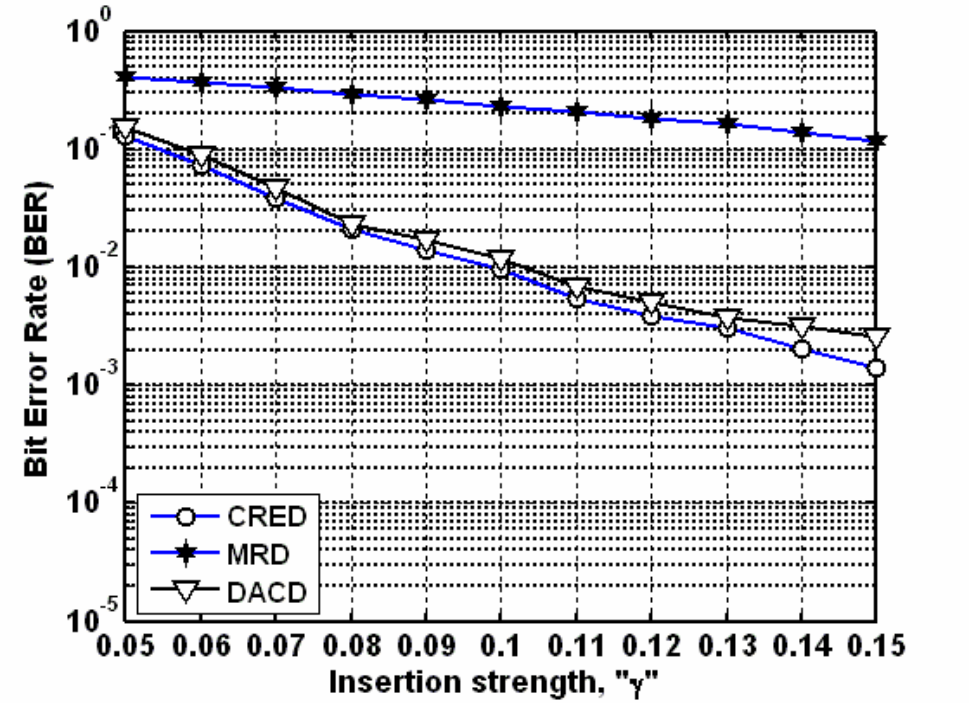

Figure 4.14 :Detector Performances Against *5x5* Mean Filtering Attacks versus Various Insertion Strengths

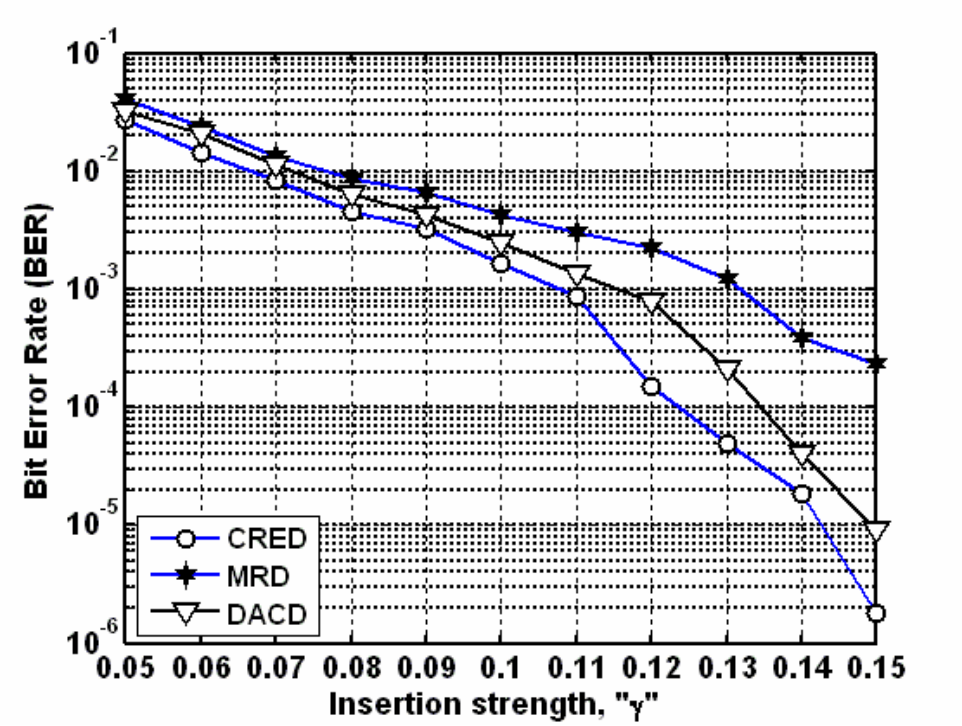

Figure 4.15 : Detector Performnces Against *3x3* Median Filtering Attacks versus Various Insertion Strengths

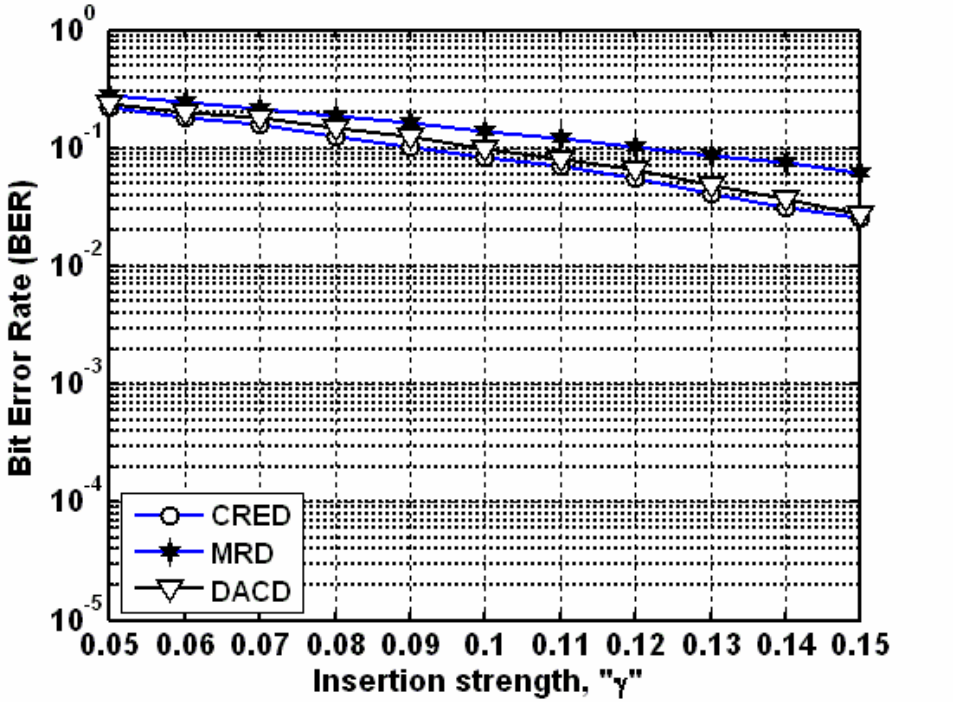

Figure 4.16 : Detector Performances Against *5x5* Median Filtering Attack versus Various Insertion Strengths

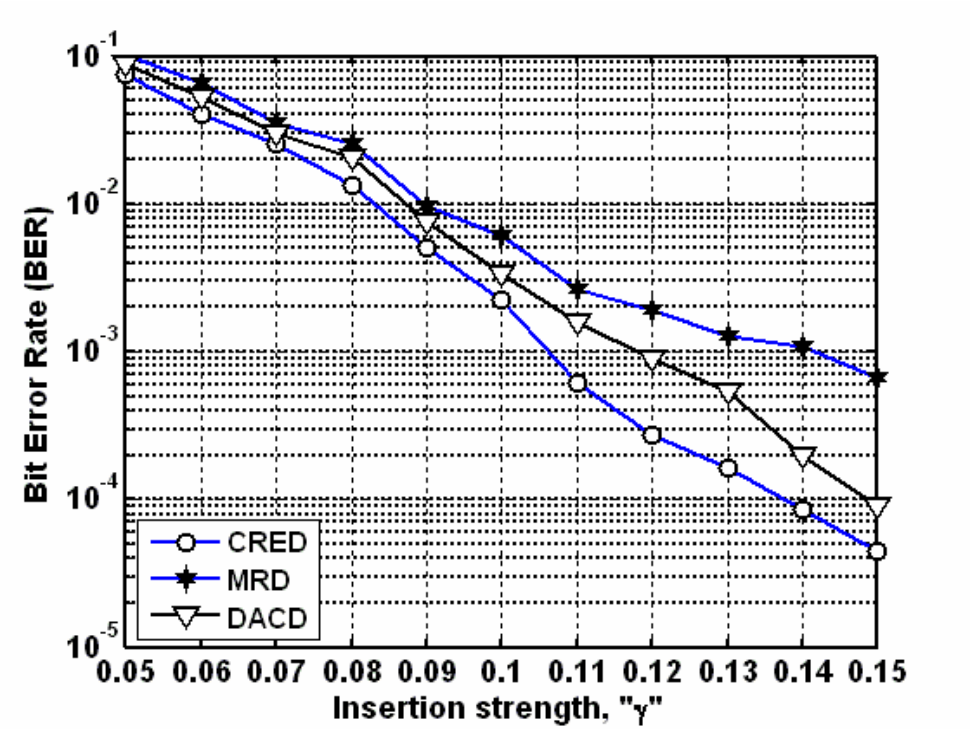

Figure 4.17: Detector Performances Against *3x3* Gaussian Low-Pass Filter with Filter Parameter 0.8 Attack versus Various Insertion Strengths

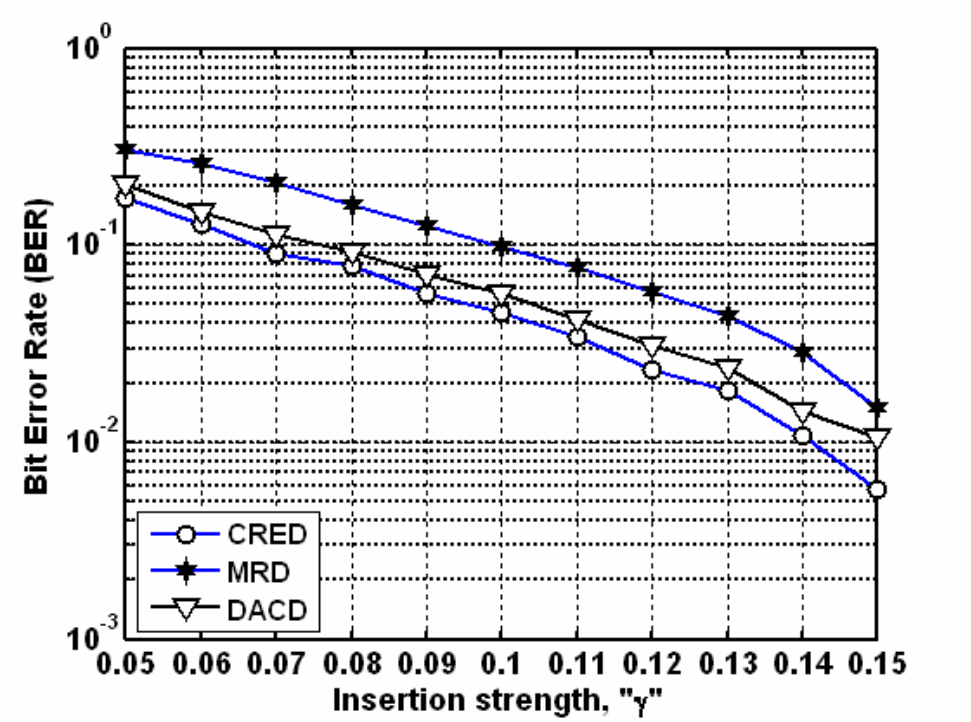

Figure 4.18: Detector Performances Against *5x5* Gaussian Low-Pass Filter with Filter Parameter 0.4 Attack versus Various Insertion Strengths

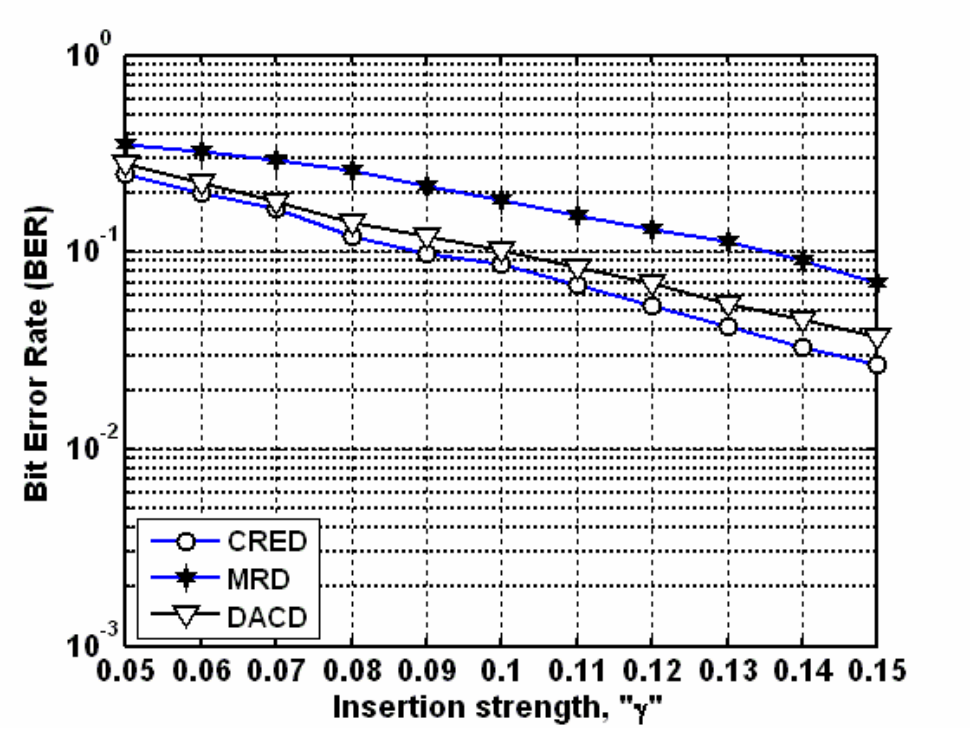

Figure 4.19: Detector Performances Against *5x5* Gaussian Low-Pass Filter with Filter Parameter 0.6 Attack versus Various Insertion Strengths

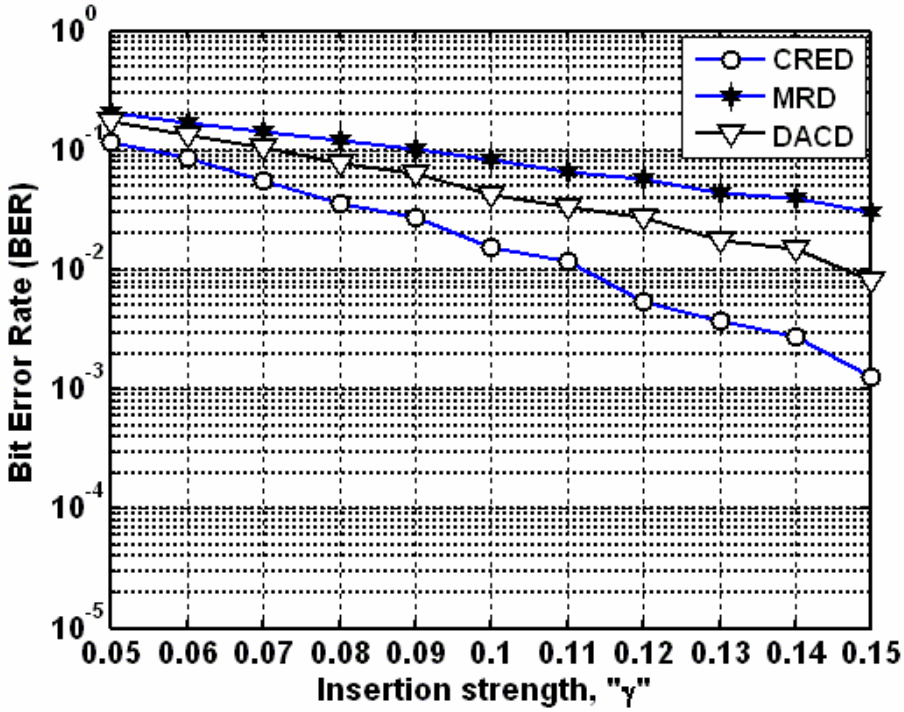

Figure 4.20 : Detector Performances Against AWGN Attack with 12 dB SNR

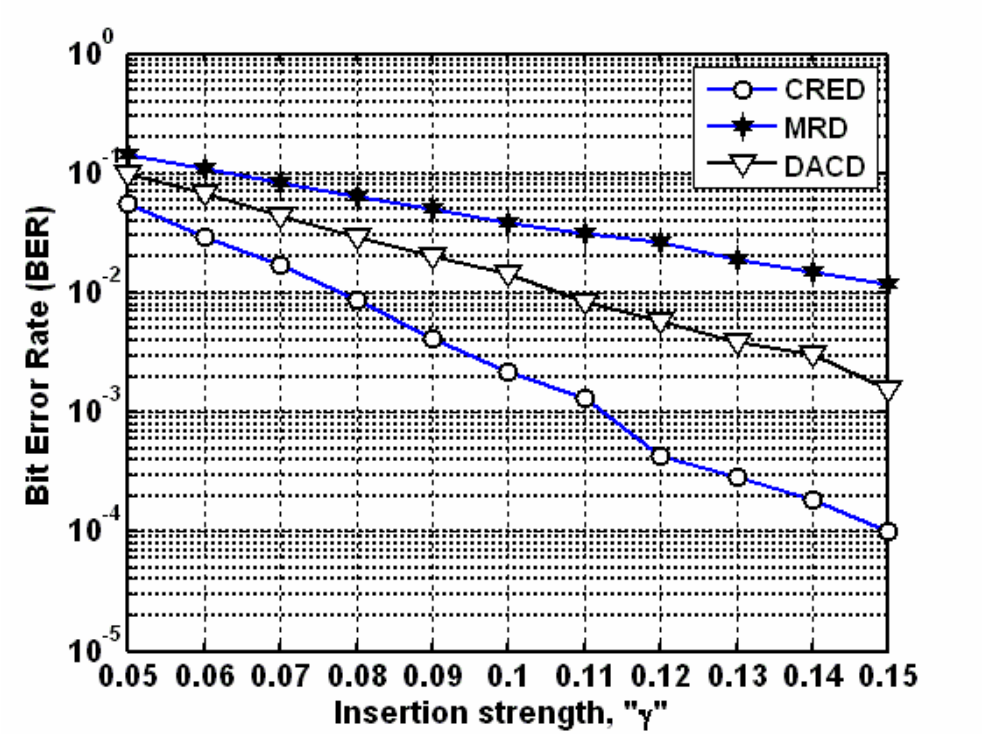

Figure 4.21 : Detector Performances Against AWGN Attack with 15 dB SNR

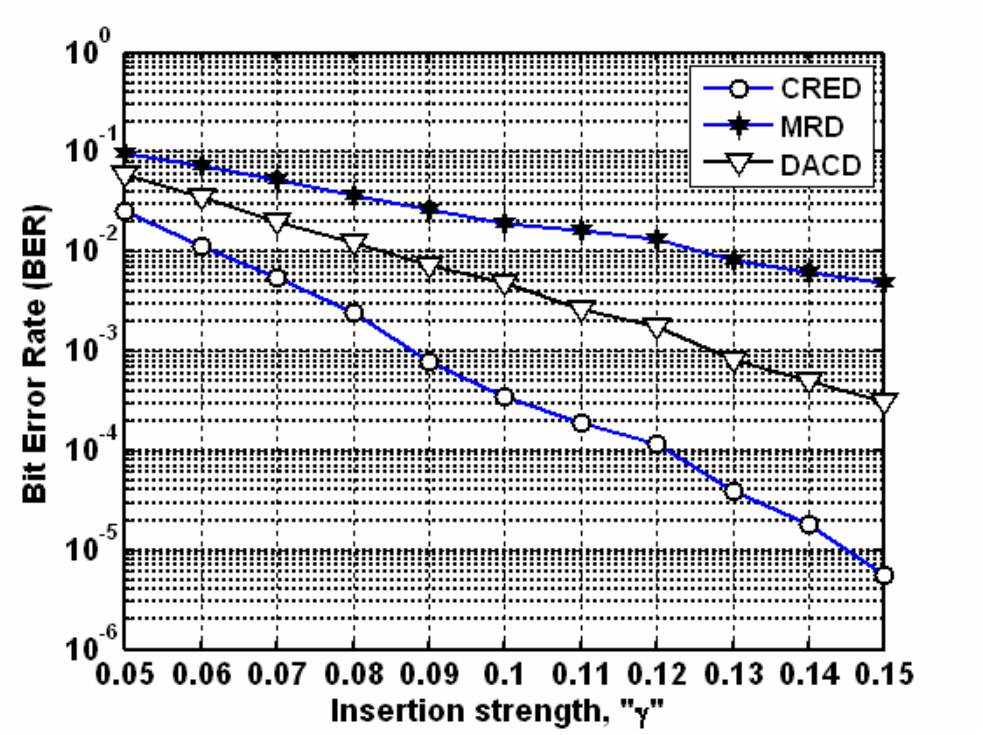

Figure 4.22 : Detector Performances Against AWGN Attack with 17 dB SNR

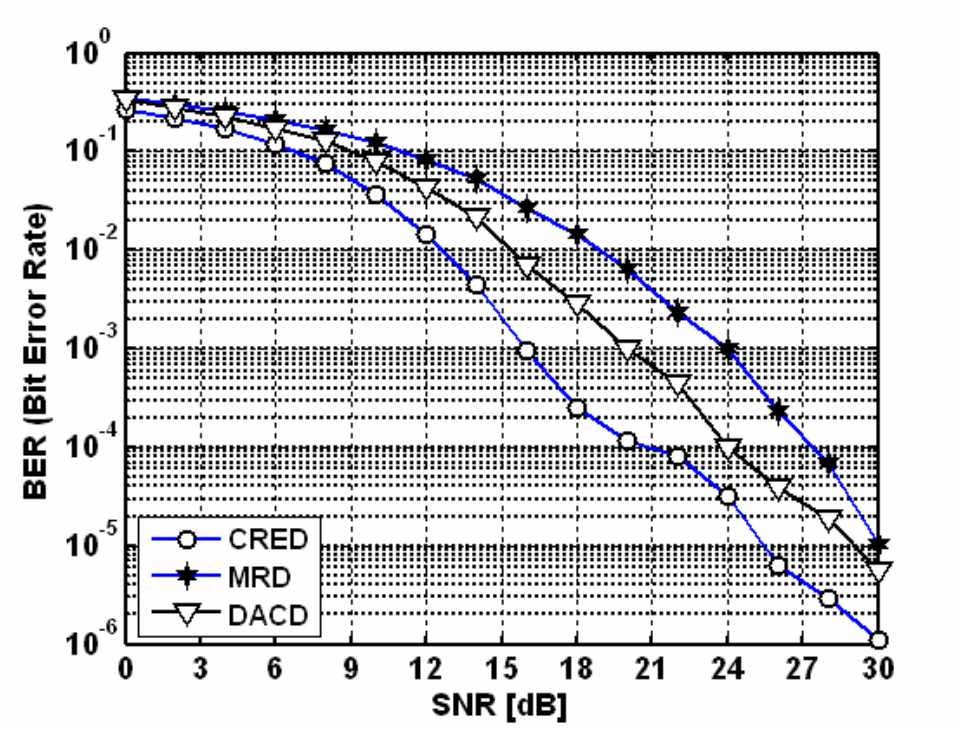

Figure 4.23 : BER Performance of the Detectors Against AWGN Attack at Various SNRs

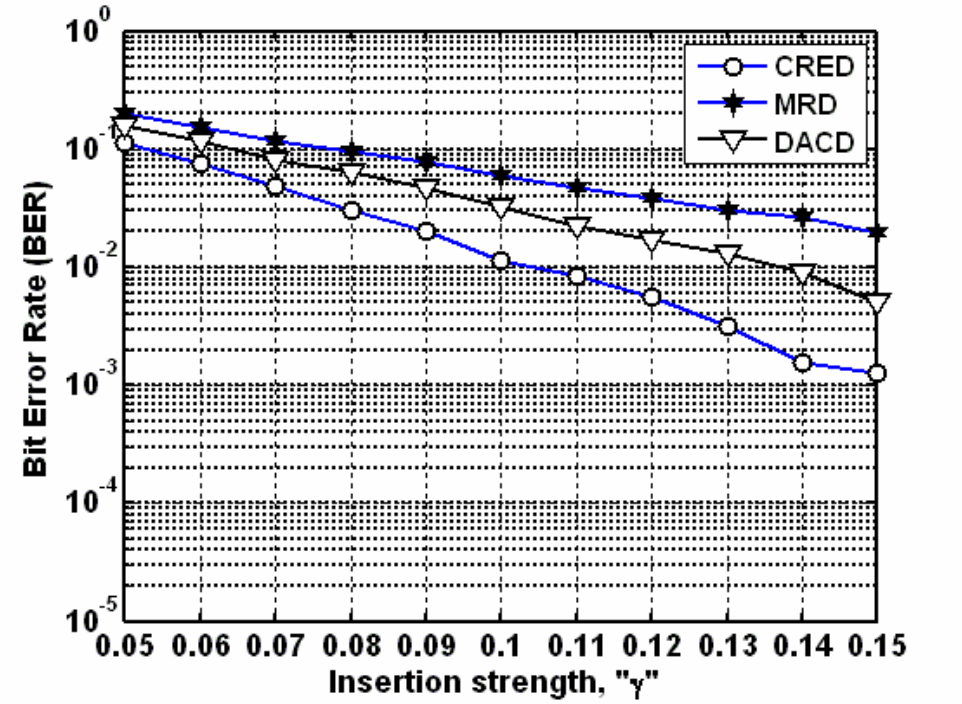

Figure 4.24 : Detector Performances Against JPEG Compression Attack with Quality Factor 20

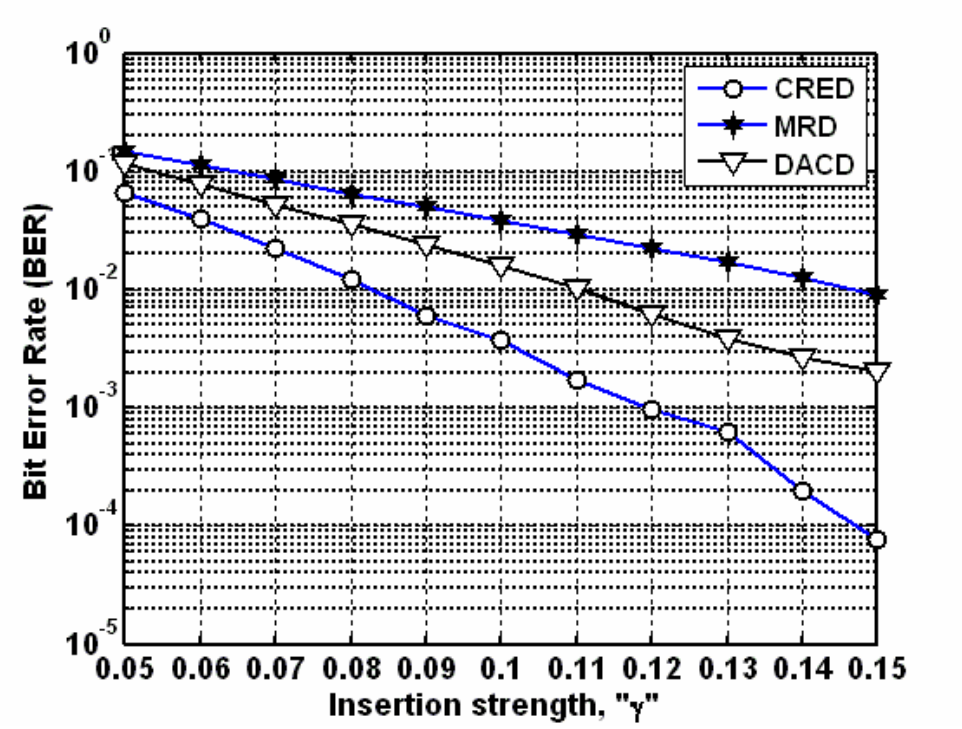

Figure 4.25 : Detector Performances Against JPEG Compression Attack with Quality Factor 24

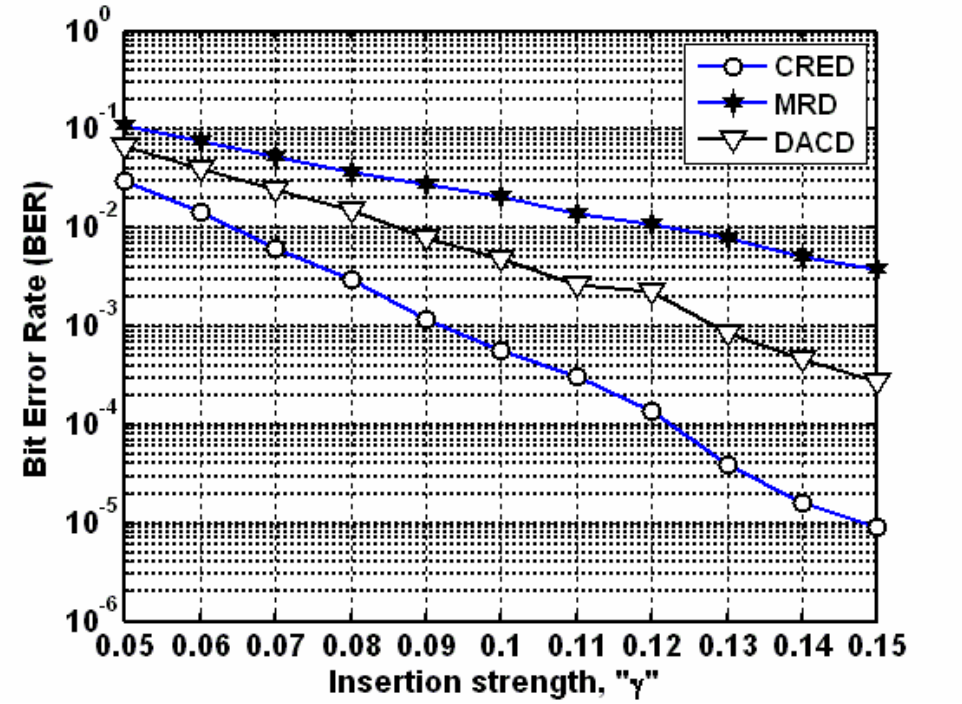

Figure 4.26 : Detector Performances Against JPEG Compression Attack with Quality Factor 30

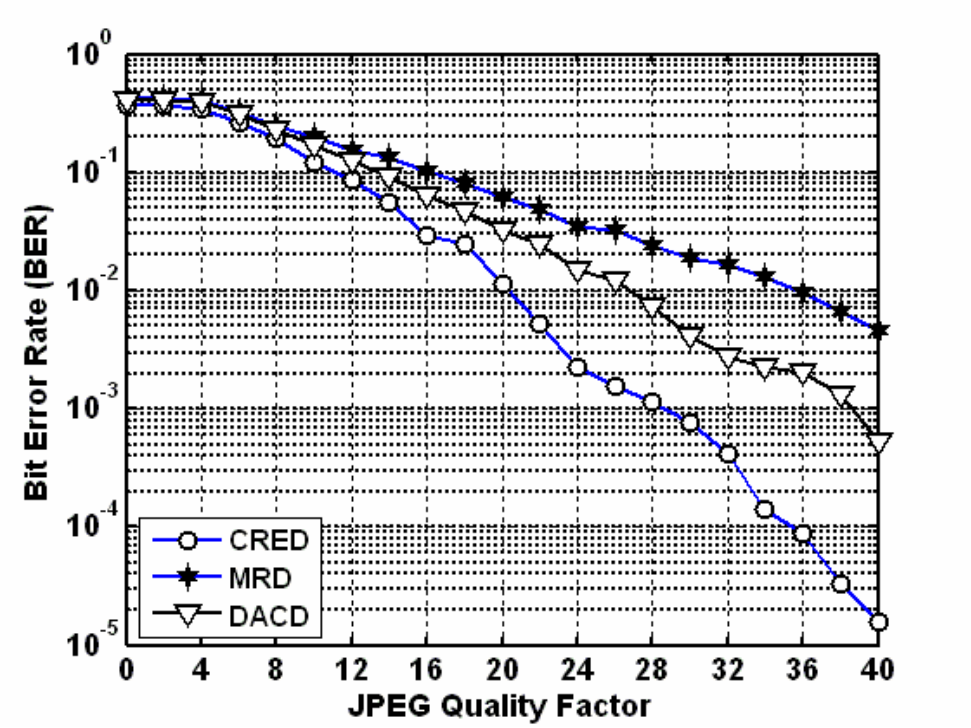

Figure 4.27 : BER Performances of Detectors with Various JPEG Quality Factors

4.4. Image Restoration Algorithms

In practical applications, the watermarked image suffers from the channel distortions and attacks in the channel as shown in Figure 4.28. These degradations cause the decrease in the recovering performance of the system. As a result, the recovered watermark has a high bit error rate and low correlation coefficient.

In this section, we propose using the existing image restoration algorithms in order to increase the quality of the watermarked image. If the receiver may predict or know the type of degradations, he can reduce the effects of them by using these algorithms and improve the detection performance of the system [38]. The purpose of image restoration is to “compensate for” or “undo” defects that degrade the watermarked image. In cases like filtering or blurring, it is possible to come up with a very good estimate of the actual blurring function and "undo" the blur to restore the

watermarked image. In cases where the watermarked image is corrupted by noise, the best we may hope to do is to compensate for the degradation it caused.

Now, we can describe our degradation model in the frequency domain as follows;

$$G[u,v] = F[u,v]H[u,v] + N[u,v] \tag{4.3}$$

where $G[u,v]$, $F[u,v]$, $H[u,v]$ and $N[u,v]$ denotes the degradated watermarked image, watermarked image, degradation function and additive noise in the frequency domain respectively. In addition, we have used the fact that the Fourier transform is a linear operator to show that additive noise in the spatial domain is also additive in the frequency domain.

In the sub-sections, we describe the algorithms used for restoring the degradated watermarked image.

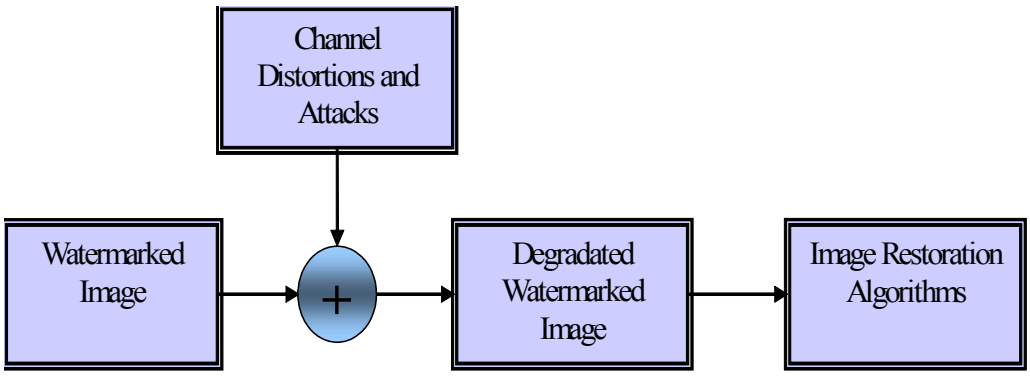

Figure 4.28 : The General Scheme for Image Restoration Algorithms

4.4.1. Wiener Filtering

Clearly the simplest way to implement deconvolution would be direct inverse filtering; since we know that convolution in the frequency domain is multiplication, to deconvolve the images we could just divide the degraded image by the point spread function (PSF) and obtain the clean image, as shown below [38]:

$$F[u,v] = \frac{G[u,v]}{H[u,v]} \tag{4.4}$$

However, this does not truly represent what our result would be with direct inverse filtering, because, as Equation (4.3) shows, we also have the problem of additive noise. If we take the noise into account, inverse filtering would give us a quite different result:

$$\hat{F}[u,v] = \frac{G[u,v]}{H[u,v]} + \frac{N[u,v]}{H[u,v]} = F[u,v] + \frac{N[u,v]}{H[u,v]} \tag{4.5}$$

This result shows that even if we know the PSF, we can not fully recover the clean image because of the additive noise. This also presents another problem, because if the degradation function contains small values, the second term in Equation (4.4) will be very large, and our estimated image will be dominated by noise. Therefore, we need a different approach to deconvolution which will take these issues into account.

The Wiener filter is the optimum filter, in the mean square sense. That is, the Wiener filter finds the estimate of the clean image such that the mean square error between the estimate and the original is minimized. This is also called the minimum mean square error (MMSE) approach to filtering. Put in mathematical terms, the clean and estimated images are treated as random processes, and a cost function, defined as the mean square value of the error, is minimized. We define the error function as the difference between the clean image and the restored image:

$$e[i,j] = f[i,j] - \hat{f}[i,j] \tag{4.6}$$

The cost function is defined as;

$$J = E\left\{e[i,j]e^*[i,j]\right\} = E\left\{\left|e[i,j]\right|^2\right\} \tag{4.7}$$

where $E\{.\}$ denotes the statistical expectation operator.

The Wiener filter is the optimum filter in the sense that it minimizes the value of the cost function *J*. It is important to note that mean-square optimality does not necessarily mean visual optimality; that is, even though the Wiener filter is optimum in the sense of minimizing the mean-square error, this does not necessarily mean that the estimated image from the Wiener filter will look the best compared to other deconvolution solutions. Visual clarity is a subjective criterion, while mathematical optimality is objective, and they do not have to be equal.

It can be shown that the solution to the MMSE problem in the frequency domain takes the following form:

$$\hat{F}[u,v] = \left[\frac{H^*[u,v]}{\left|H[u,v]\right|^2 + \dfrac{S_n[u,v]}{S_f[u,v]}}\right] G[u,v] \tag{4.8}$$

where $S_n[u,v]$ is the power spectrum of the noise and $S_f[u,v]$ is the power spectrum of the clean image.

It is easy to see that if the noise is zero, the Wiener filter reduces to the inverse filter given in Eq. (4.1) and we theoretically get the exact clean image if we know the PSF. Since our problem is finding an estimate of the clean image, this inherently means that we do not have a copy of the clean image (if we did, we wouldn't need to find an estimate of it). Therefore, we do not have access to the image power spectrum $S_f[u,v]$.

We can modify the Wiener filter to take this into account by replacing the noise-to-signal power ratio $\frac{S_n[u,v]}{S_f[u,v]}$ with a constant K as an estimate of the ratio:

$$\hat{F}[u,v] = \left[\frac{H^*[u,v]}{|H[u,v]|^2 + K} \right] G[u,v] \tag{4.9}$$

The best value for K in Equation (4.9) can be found either by using random values until a desirable result is achieved or by searching through a range to find the most suitable result. This parameter most likely will need to be recomputed for different images; this is a drawback of Wiener filtering because we cannot use the same value of K to filter a variety of images.

4.4.2. Constrained Least Squares (Regularized) Filtering

As stated in the previous section, the problem with Wiener filtering is the need to know the power spectrum of the clean image. Although we can use the parameter K to estimate the Wiener filter, this causes more computations to be done to find the correct value for each filtering operation. To solve this problem we can use the constrained least squares, or regularized, filtering method to perform deconvolution. As is the case with the Wiener filter, we need to know the PSF to perform this operation, and in fact, the equation for this filter looks very similar to the Wiener filter. The development of the regularized filtering method uses the Laplacian operator. The Laplacian is a second-order derivative operator used for image enhancement as defined in [38]

$$\nabla^2 f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} \tag{4.10}$$

Substituting the values of the partial derivates into Eq. (5.1) gives us the following formula for implementing the Laplacian in the spatial domain:

$$\nabla^2 f = \left[f(x+1,y), f(x-1,y), f(x,y+1), f(x,y-1) \right] - 4f(x,y) \tag{4.11}$$

This can be realized in the discrete spatial domain by using an image mask of

$$p[x,y] = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 0 \end{pmatrix} \tag{4.12}$$

In contrast to the Wiener filter, the method of regularized filtering bases optimality on the measure of smoothness; since taking the second derivative of an image will smooth it out, this is why the Laplacian operator is used in the formulation of the filter. The degradation process in matrix notation for the *MxN* image is [39], [40]:

$$\mathbf{g} = \mathbf{H}\mathbf{f} + \mathbf{n} \tag{4.13}$$

where **g** denotes the lexicographic order of the degradated image of size *MNx1*, **f** denotes the the lexicographic order of the undegradated image of size *MNx1*, **n** denotes the lexicographic order of the noise of size *MNx1*, **H** denotes the lexicographic order of the Toeplitz matrix of size *MNxMN* and it is called the degradation function.

We need to find the minimum of the criterion function

$$\left\| C\hat{\mathbf{f}} \right\|^2 \tag{4.14}$$

where $\hat{\mathbf{f}}$ is the estimated of the undegradated image and $C = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left[\nabla^2 f(x,y) \right]^2$, and subject to the constraint

$$\left\| \mathbf{g} - \mathbf{H}\hat{\mathbf{f}} \right\|^2 = \left\| \mathbf{n} \right\|^2 \tag{4.15}$$

where $\|\mathbf{n}\|^2 \triangleq \mathbf{n}^T\mathbf{n}$ is the Euclidean norm and $\hat{\mathbf{f}}$ is the estimate of the undegradated image.

It can be shown that the solution to this constrained optimization problem in the frequency domain is:

$$\hat{F}[u,v] = \left[\frac{H^*[u,v]}{|H[u,v]|^2 + \lambda |P[u,v]|^2} \right] G[u,v] \tag{4.16}$$

where $P[u,v]$ is the Fourier transform of the (zero-padded) Laplacian matrix in Equation (4.12), and the parameter λ is the Lagrange multiplier, or the regularization parameter, which is computed so that the constraint in Equation (4.15) is satisfied; λ controls tradeoff between the mean square error and the smoothness of the solution. Larger values of λ introduce more ringing into the restored image, while smaller values amplify the noise. Equation (4.16) is very similar in form to the Wiener filter, and we can see that if λ is set to zero, this becomes the ideal inverse filter.

4.4.3. Lucy- Richardson Algorithm

Apart from those two methods, there are some iterative approaches to the subject of deblurring as well. The transform between the clean image and the observed blurred image being known, one could expect that applying the invert transform would result in a perfectly restored image. However, this is not true due to the noise in the image, which will be strongly emphasized by the invert transform. Iterative restoration algorithms have been developed to find a solution for that problem. At each pass, they tend to ameliorate the PSF towards a single pixel. When the best compromise between the image detail enhancement and the noise has been reached, the iterations should be stopped. One of these iterative approaches applied in the Lucy-Richardson (LR) Algorithm [41]. The LR algorithm is an iterative technique for image restoration, used extensively for restoring astronomical images. The LR algorithm works very well restoring images with Poisson noise, which is the predominant noise source in astronomical imaging. The algorithm is derived by maximizing the likelihood of the

restored image, and indeed converges to the maximum likelihood solution for images with Poisson noise statistics. The LR algorithm is popular because of the fact that restored images are robust to small errors in the degradation function, the algorithm forces the image to be non-negative, and it conserves the total energy.

There are many ways to maximize the likelihood function. One of the ways the iterative Richardson-Lucy algorithm in the spatial domain can be expressed is by the following equation:

$$f_{app}^{k+1}[x,y] = f_{app}^{k}[x,y] \bullet \left(h\ [x,y] \odot \frac{g[x,y]}{r[x,y]} \right) \triangleq \Psi\left(f_{app}^{k}[x,y] \right) \tag{4.17}$$

and

$$r[x,y] = h[x,y] \otimes f_{app}^{k}[x,y] \tag{4.18}$$

where, $f_{app}^{k}[x,y]$ is the estimate of the restored image after k iterations of the algorithm, $\odot$ denotes correlation, $\otimes$ denotes convolution, $r[x,y]$ called the reblurred image, and $\bullet$ denotes point-wise multiplication. Also, the division operation in Equation (4.17) is done by point-wise. This algorithm finds an image estimate which closely resembles the original clean image. The correlation operator is used for matching and to check the similarity between two images. An initial image estimate f^0 needs to be provided at the start of the algorithm; as Biggs and Andrews recommended [38] , we have used $h \otimes g$ as this initial input. If the noise is Gaussian in nature, an alternative to the Equation (4.17) is given by:

$$f_{app}^{k+1}[x,y] = f_{app}^{k}[x,y] + h\ [x,y] \odot \left(g[x,y] - f_{app}^{k}[x,y] \otimes h\ [x,y] \right) \tag{4.19}$$

The algorithm as stated above is not efficiently computable; it requires iteration over all of the pixels of the image for each iteration of the algorithm. Fortunately, the Equation (4.17) can also be implemented partially in the frequency domain. Since

multiplication and division in the spatial domain do not correspond to multiplication and division in the frequency domain, the entire iteration can not be directly transformed. Instead, some transforming and inverse transforming needs to take place to compute each iteration. The convolution and correlation operations can be done in the frequency domain, while the division and multiplication can be done in the time domain This would modify Equation (4.16) as shown below:

$$f_{app}^{k+1}[x,y] = f_{app}^{k}[x,y] \bullet \left(\Im^{-1} \left\{ H^{*}[u,v] \bullet \Im \left\{ \frac{g[x,y]}{\Im^{-1}\left\{ H[u,v] \bullet F_{app}^{k}[u,v] \right\}} \right\} \right\} \right) \qquad (4.19)$$

where $\bullet$ denotes point-wise multiplication and the division operation in Equation (4.19) is done by point-wise.

There are some drawbacks to the LR algorithm applied with Equation (4.17). The first is that it can be slow to converge to the maximum likelihood solution. To solve this problem, there have been several adaptations to the conventional algorithm [42]. The first adaptation is accelerating the algorithm so that less iterations are needed to get to a particular point along the curve to the maximum likelihood solution; this can be done with a variety of methods. One possible way to accelerate this algorithm is to add an exponential factor to Equation (4.17):

$$f_{app}^{k+1}[x,y] = f_{app}^{k}[x,y] \bullet \left(h[x,y] \; o \; \frac{g[x,y]}{h[x,y] \otimes f_{app}^{k}[x,y]} \right)^{\nu} \qquad (4.20)$$

where $\nu > 1$ and $\bullet$ denotes point-wise multiplication. However, this approach may become unstable after many iterations.

The second major drawback to the LR algorithm is that of noise amplification. Noise amplification is a general problem with maximum likelihood techniques [42]. The more iterations that are run for the algorithm the higher the noise can get, especially with smooth objects present in the image. One solution for this is to stop the algorithm when noise starts becoming a factor. Of course, this can be difficult to ascertain, as the

number of iterations at which point this happens will differ based on the image being restored and its noise statistics. A way to determine the termination point for the algorithm is to compute the normalized change in energy at each iteration from the previous iteration and compare it to a threshold. For example, a possible termination point could happen when

$$\frac{\|f_{k+1} - f_k\|^2}{\|f_k\|^2} \leq \varepsilon \tag{4.26}$$

where ε is some threshold defined by the user.

4.5. Simulations Results and Discussions with Image Restoration Algorithms

The watermarked image may undergo the channel distortions and attacks in the channel. The image restoration algorithms remove or minimize some known degradations in the watermarked image. Our primarily goal is to characterize the degradations by employing the proposed CRED detector and decrease the effects of them by applying image restoration algorithms. Thus, we improve the detection performance of the system.

In order to obtain the simulation result shown in Figure 4.29, the watermarked image is blurred with mean filter of various filter sizes such as *3x3, 5x5, 7x7* and *9x9*. Then, it is reconstructed by using the Wiener filter with true PSF. Actually, Wiener deconvolution can be used effectively when the frequency characteristics of the image and additive noise are known, to at least some degree. In the absence of noise, the Wiener filter reduces to the ideal inverse filter. When the watermarked image is blurred and deblurred with mean filter of size *3x3*, the detection performance of the digital watermarking system is almost perfect. As the size of the mean filter increases, the attack gets stronger and the BER rate of the recovered watermark is increased. We can conclude from simulation that the proposed CRED detector improves the detection performance of the watermarking system in case of restoration.

The Figure 4.30 demonstrates the BER performance of the detectors when the watermarked image, first, is exposed to *3x3* mean filtering attack and AWGN attack at various SNRs. Although the attack is very strong, the proposed detection method works satisfactorily. The BER performances of the detectors are almost the same. In addition, as the SNR increases we get lower BERs as expected.

We test and compare the performances of the watermark detectors in case of the watermarked image is *3x3* mean filtered and then AWGN is added with various SNRs. We employ Wiener filter restoration method to decrease the degradations caused by the filtering and AWGN. The BER performance of the detectors is improved as shown in Figure 4.31. Especially, the proposed CRED detector outperforms in comparison to the other detectors at 18 dB and greater SNR values. In this simulation, when we set the target BER to 10^{-4}; the proposed CRED detector achieves 4 dB SNR gain in comparison to the DACD detector. It also achieves 7 dB SNR gain in comparison to the MRD detector as given detailly in the Appendix C.

Then, we employ Lucy-Richardson algorithm in order to deblur the degradated watermarked image. The experiment shown in Figure 4.32, we apply Lucy-Richardson restoration algorithm to the watermarked image. In this experiment, we assume that the receiver knows the true PSF but nothing knows about the noise. We aim at reducing the degradation caused by *3x3* mean filter and AWGN. The algorithm increases the detector performances considerably. In this simulation, when we set the target BER to 10^{-4}; the proposed CRED detector achieves 3 dB SNR gain in comparison to the DACD detector. It also achieves 6 dB SNR gain in comparison to the MRD detector as given detailly in the Appendix C.

Finally, we apply regularized filter to the degradated watermarked image for decreasing the effects of the degradations as shown in Figure 4.33. In this experiment, we assume that the receiver knows the true PSF but nothing knows about the noise. The simulation shown in Figure 4.33, the BER performance of the proposed CRED detector increases as the SNR increases. It has lower BERs than the other detectors especially at 18 dB SNR levels. In this simulation, when we set the target BER to 10^{-4}; the proposed

CRED detector achieves 3 dB SNR gain in comparison to the DACD detector. It also achieves 6 dB SNR gain in comparison to the MRD detector as shown in Appendix C.

We compare the BER performances of the detectors before applying the restoration algorithms and after applying restoration algorithms in simulation shown in Figure 4.34 - Figure 4.36. We can conclude from the simulations that the restoration algorithms improve the detection performance of the digital watermarking system since they decrease the effects of the degradations caused by the channel distortions and attacks. In addition, we can observe that the proposed CRED detector achieves the maximum performance improvement after applying the restoration algorithms. On the other hand, depending on the particular application and the media being watermarked, computational complexity can be a significant factor in the assessment of the feasibility of a watermarking system. For example, in DVD players watermark extraction must be performed in real-time. Hence, computational complexity is very critical for these applications. In this thesis, the proposed CRED detector has the lowest computational complexity since it employs thresholding scheme. In addition, the MRD detector is less complex than the DACD detector, since it does not estimate the channel parameters by using the reference watermarks and does not assign channel parameter.

The watermarked image is exposed to *3x3* Gaussian low-pass filter attack with filter parameter 0.8 and AWGN attack at various SNRs in Figure 4.30. In this simulation, the proposed CRED detector decreases the BER at the same SNR level. Then, we employ Wiener filter restoration method to decrease the degradations caused by the Gaussian low-pass filter and AWGN. The BER performance of the detectors is improved as shown in Figure 4.38. In this simulation, if we set the target BER to 10^{-4}; the proposed CRED detector achieves 2 dB SNR gain in comparison to the DACD detector. On the other hand, the MRD detector can't attain the target BER as given detailly in the Appendix C.

The experiment shown in Figure 4.39, we apply Lucy-Richardson restoration algorithm to the watermarked image. Our goal is to reduce the degradation caused by *3x3* Gaussian filter and AWGN. The algorithm decreases the BERs of the recovered watermarks considerably. In this simulation, if we set the target BER to 10^{-4}; the

proposed CRED detector achieves 2 dB SNR gain in comparison to the DACD detector. However, MRD detector can't attain the target BER as given detailly in the Appendix C.

The experiment shown in Figure 4.40, we apply regularized filter to the degradated watermarked image. In this experiment, the BER performance of the detectors increases as the SNR increases. For example, if we set the target BER to 10^{-4}; the proposed CRED detector achieves 3 dB SNR gain in comparison to the DACD detector but the MRD detector can't attain the target BER level as given detailly in the Appendix C.

Finally, we investigate the effects of image restoration algorithms on the BER performance of the detectors in simulation shown in Figure 4.41 - Figure 4.43. Thus, we can conclude from the simulations that the restoration algorithms improve the detection performance of the watermarking system considerably. In addition, we can claim that the proposed CRED detector achieves the maximum performance improvement after the restoration algorithms.

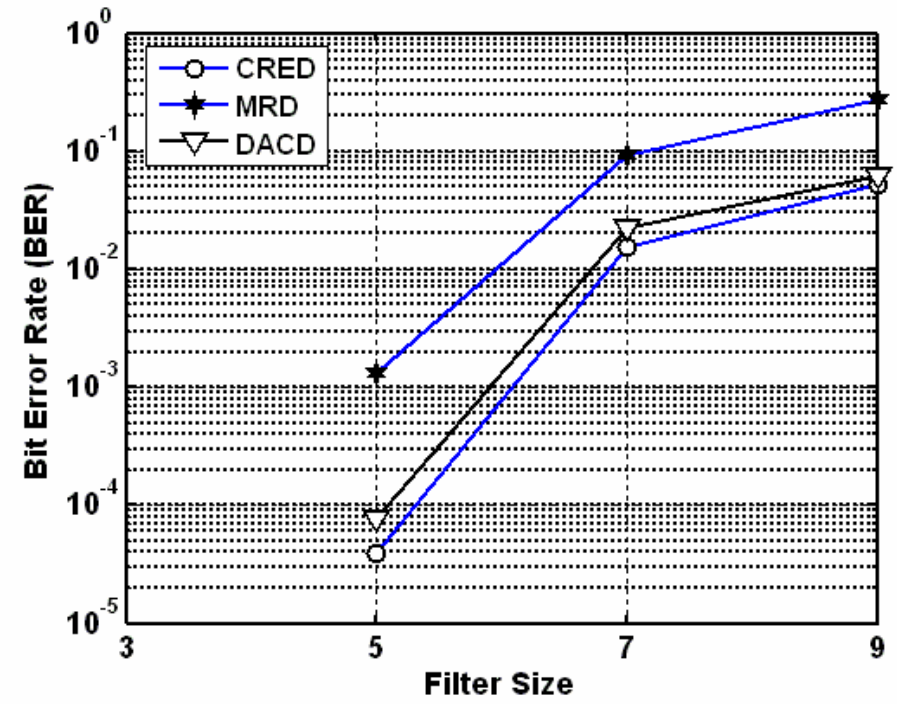

Figure 4.29 : BER Performances of the Detectors with Blurring Mean Filter of Various Filter Sizes and Wiener Filter Restoration

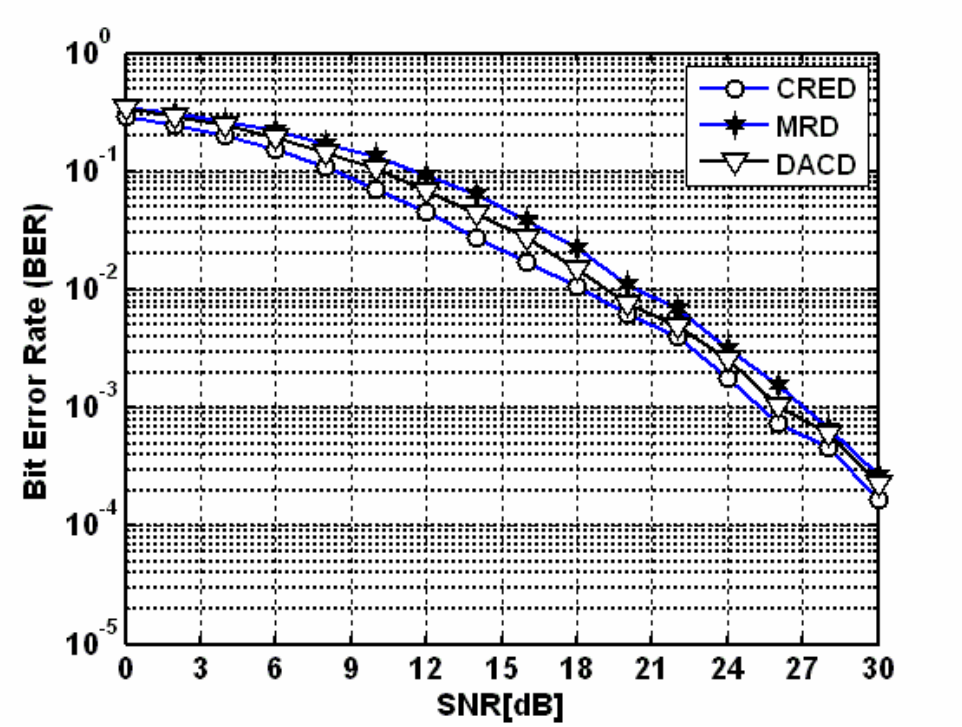

Figure 4.30 : BER Performances of the Detectors Against *3x3* Mean Filter and AWGN at Various SNRs

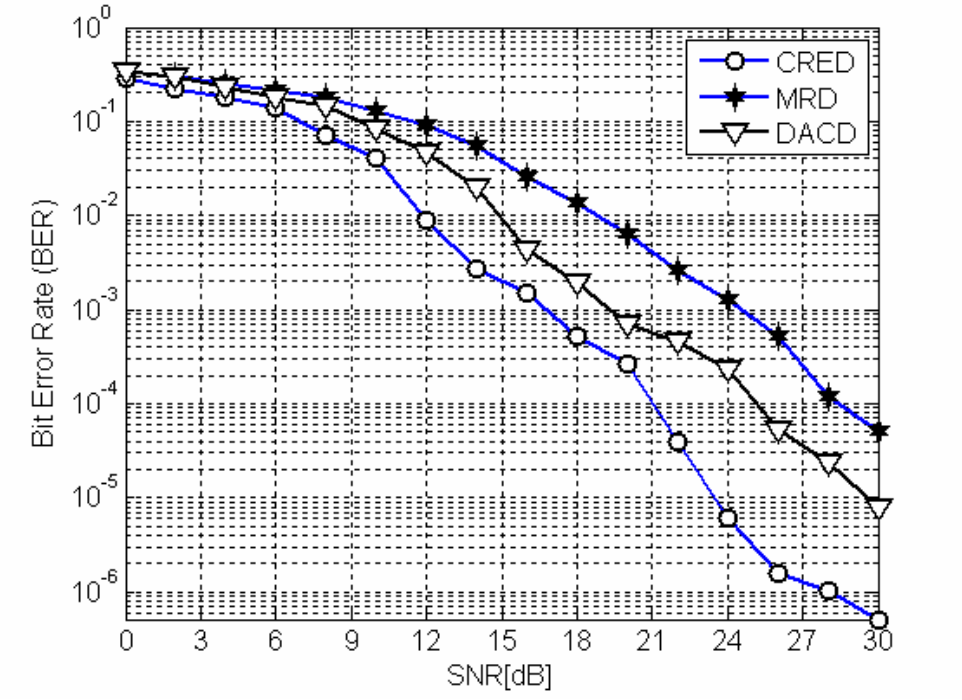

Figure 4.31 : BER Performances of the Detectors Agianst *3x3* Mean Filter and Applying Wiener Filter Restoration Against AWGN at Various SNRs

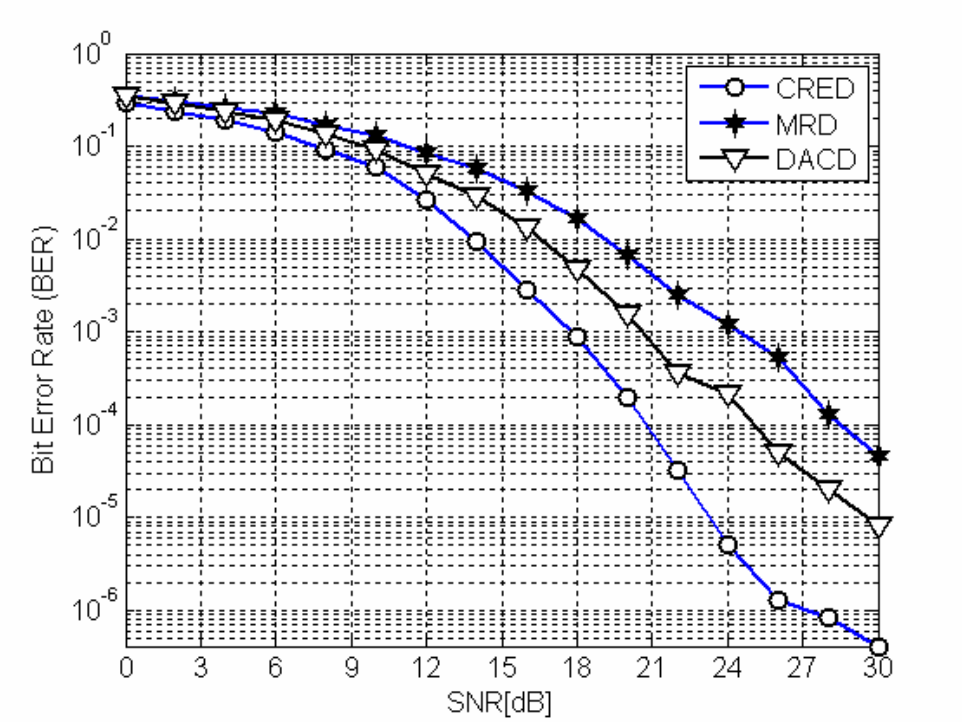

Figure 4.32 : BER Performances of the Detectors Against *3x3* Mean Filter and Applying Lucy-Richardson Restoration Algorithm Against AWGN at Various SNRs

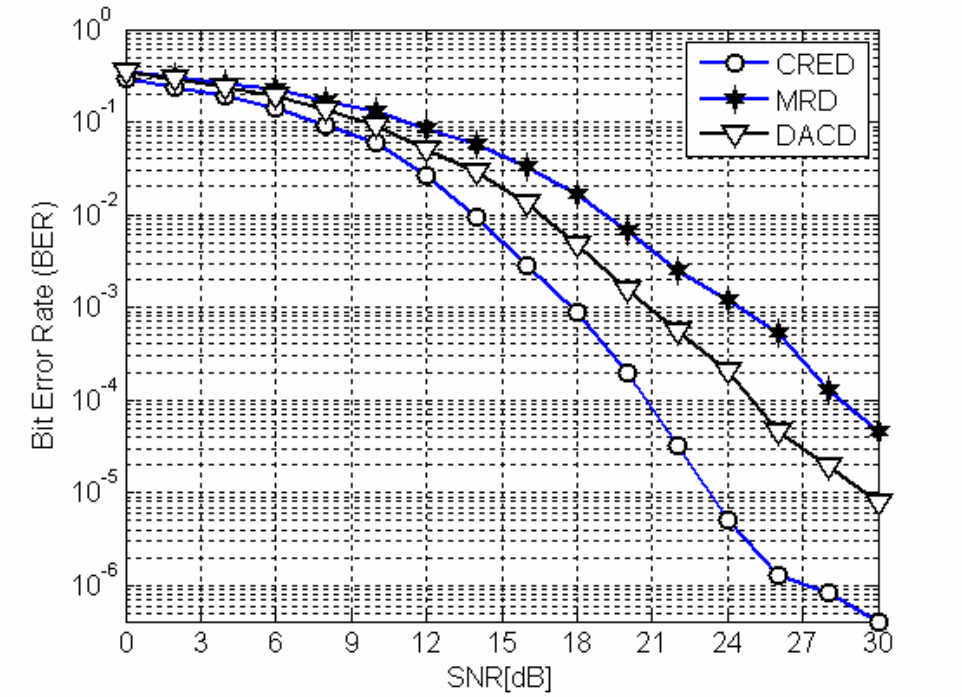

Figure 4.33 : BER Performances of the Detectors Against *3x3* Mean Filter and Applying Regularized Filter Restoration Against AWGN at Various SNRs

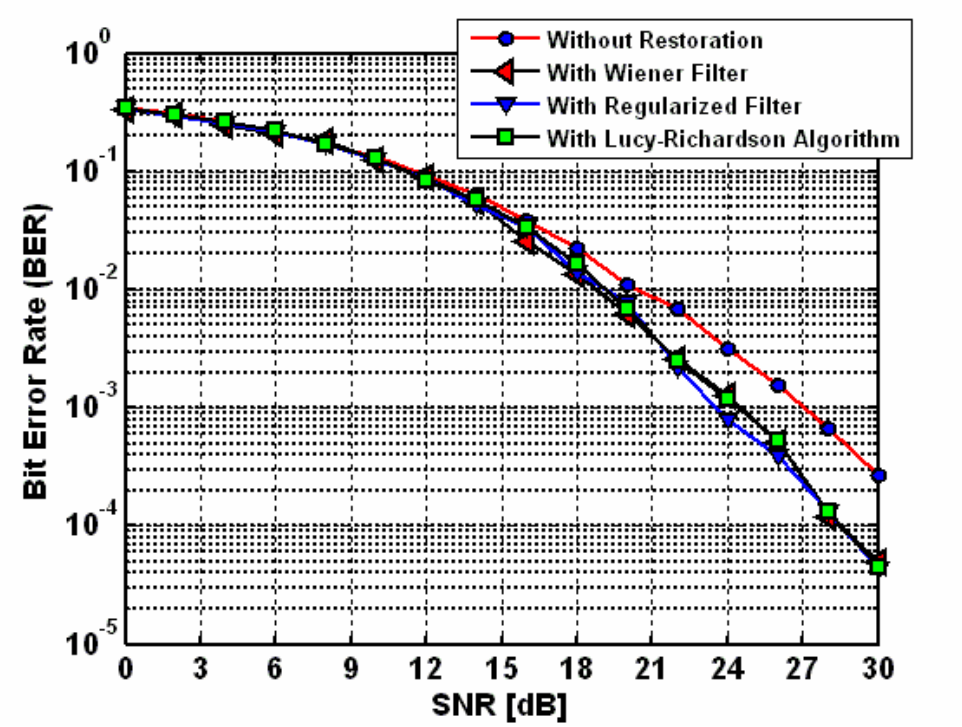

Figure 4.34 : BER Performance of MRD Detector Against *3x3* Mean Filter and Various Restoration Methods

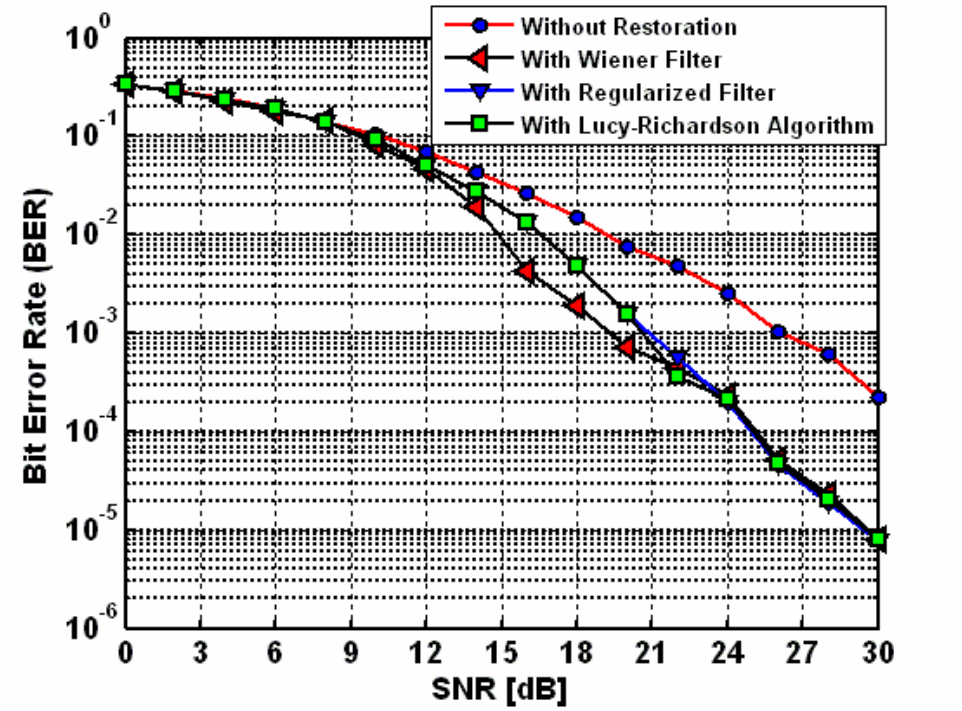

Figure 4.35 : BER Performance of DACD Detector Against *3x3* Mean Filter and Various Restoration Methods

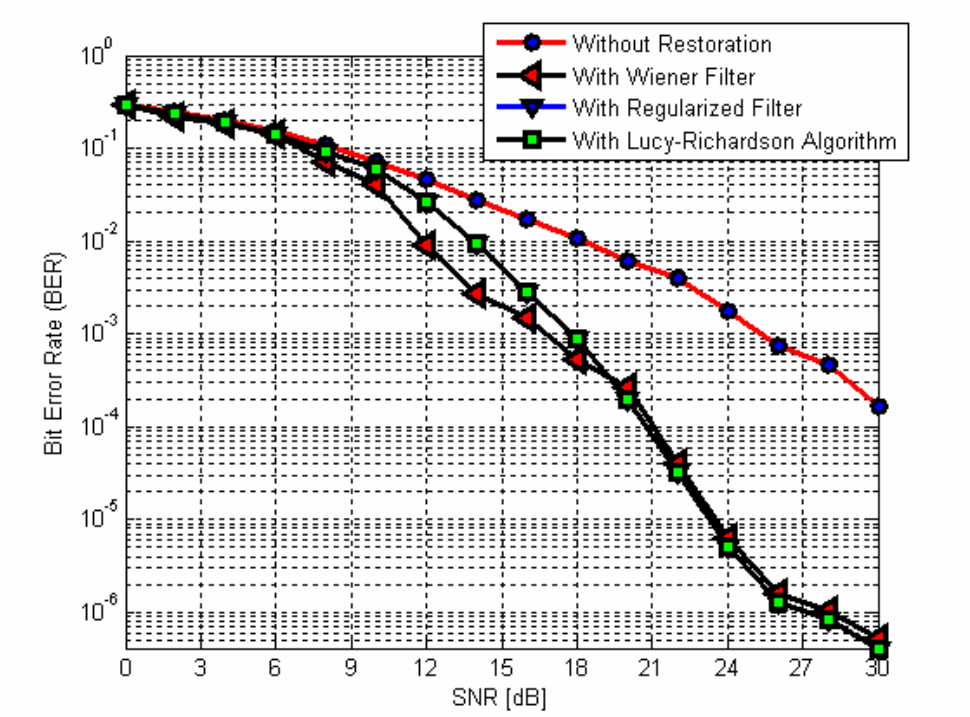

Figure 4.36 : BER Performance of the Proposed CRED Detector Against *3x3* Mean Filter and Various Restoration Methods

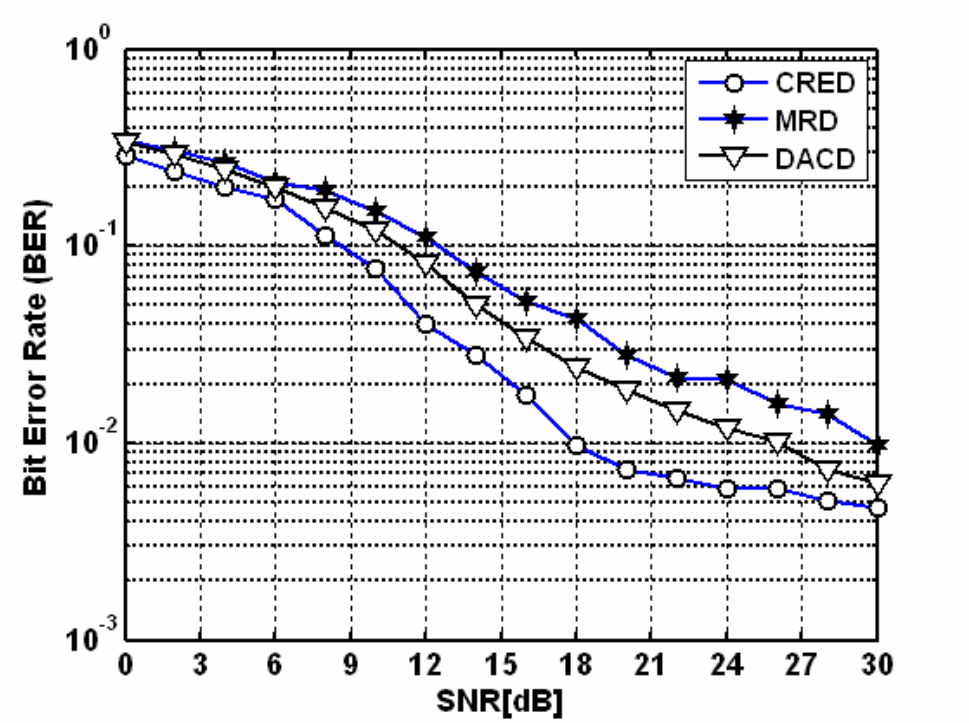

Figure 4.37: BER Performances of the Detectors Against *3x3* Gaussian Low-Pass Filter with Parameter 0.8 and AWGN at Various SNRs

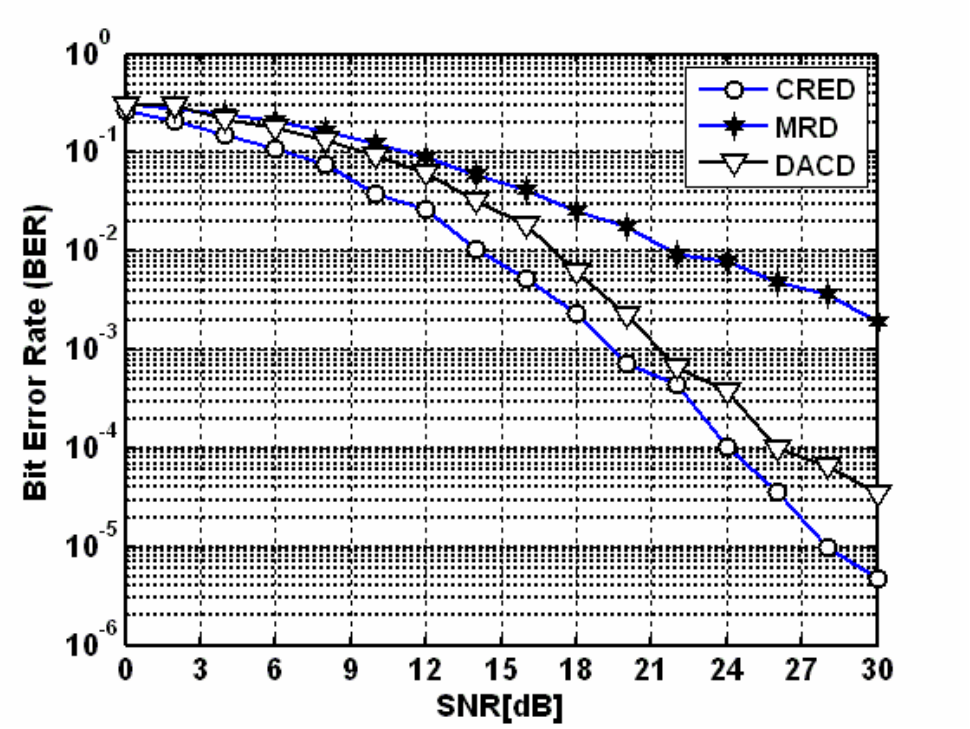

Figure 4.38: BER Performances of the Detectors Against *3x3* Gaussian Low-Pass Filter with Parameter 0.8 and Applying Wiener Filter Restoration Against AWGN at Various SNRs

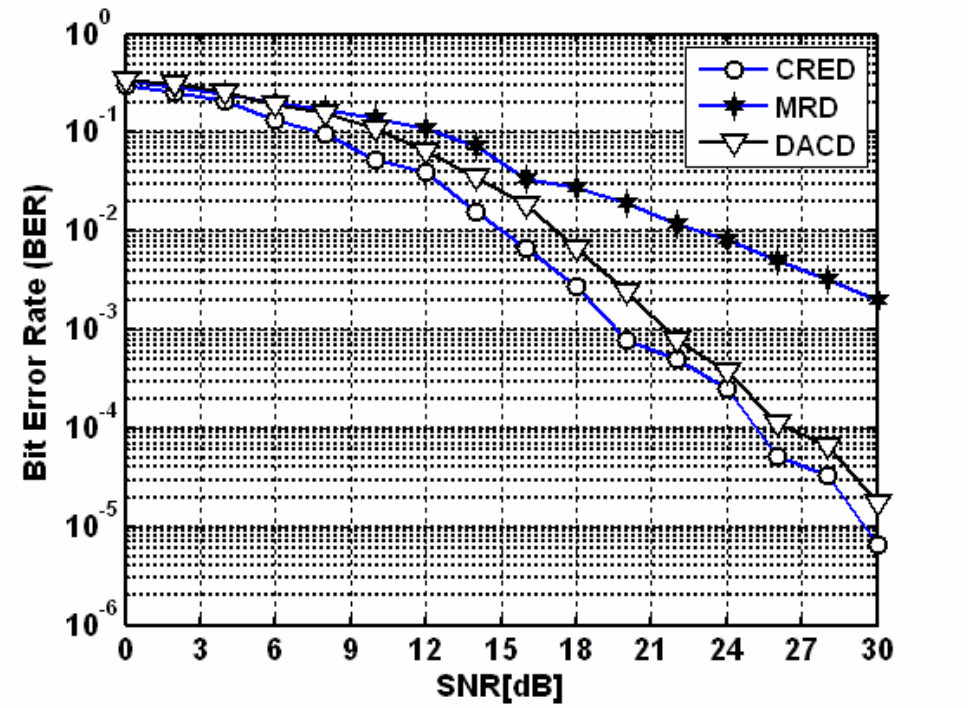

Figure 4.39: BER Performances of the Detectors Against *3x3* Gaussian Low-Pass Filter with Parameter 0.8 and Applying Lucy-Richardson Restoration Algorithm Against AWGN at Various SNRs

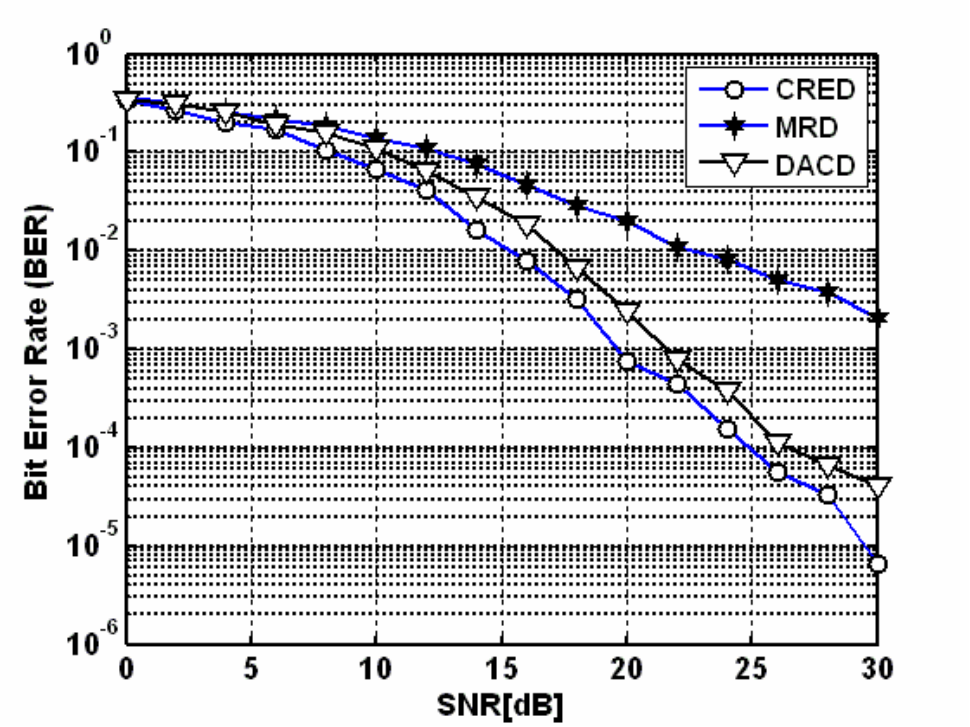

Figure 4.40: BER Performances of the Detectors Against *3x3* Gaussian Low-Pass Filter with Parameter 0.8 and Applying Regularized Filter Restoration Against AWGN at Various SNRs

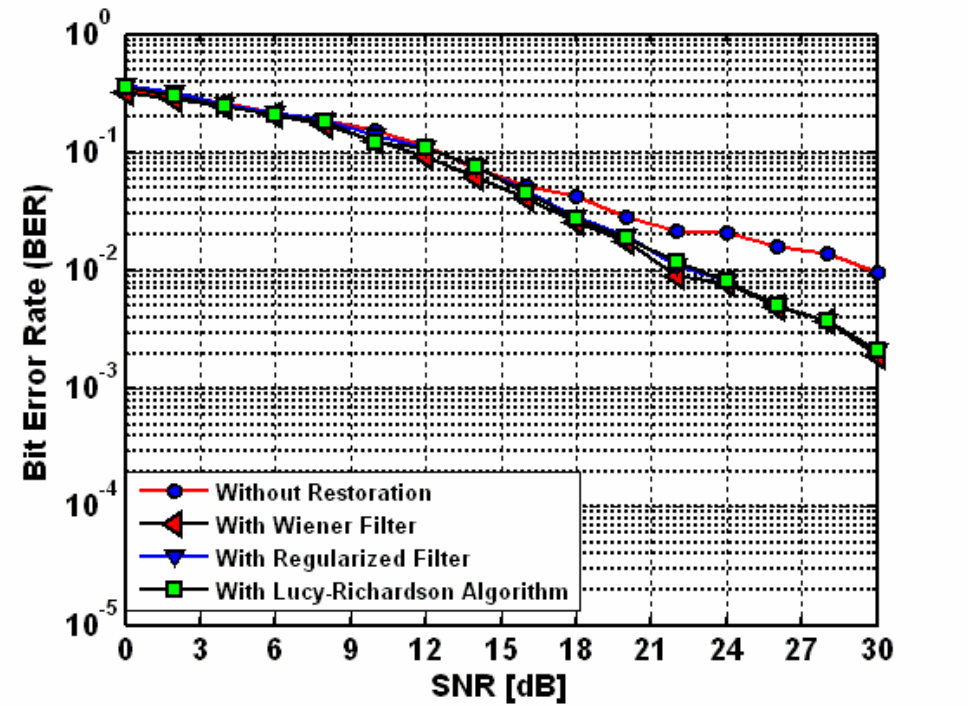

Figure 4.41: BER Performance of the MRD Detector Against *3x3* Gaussian Low-Pass Filter with Parameter 0.8 and Various Restoration Methods

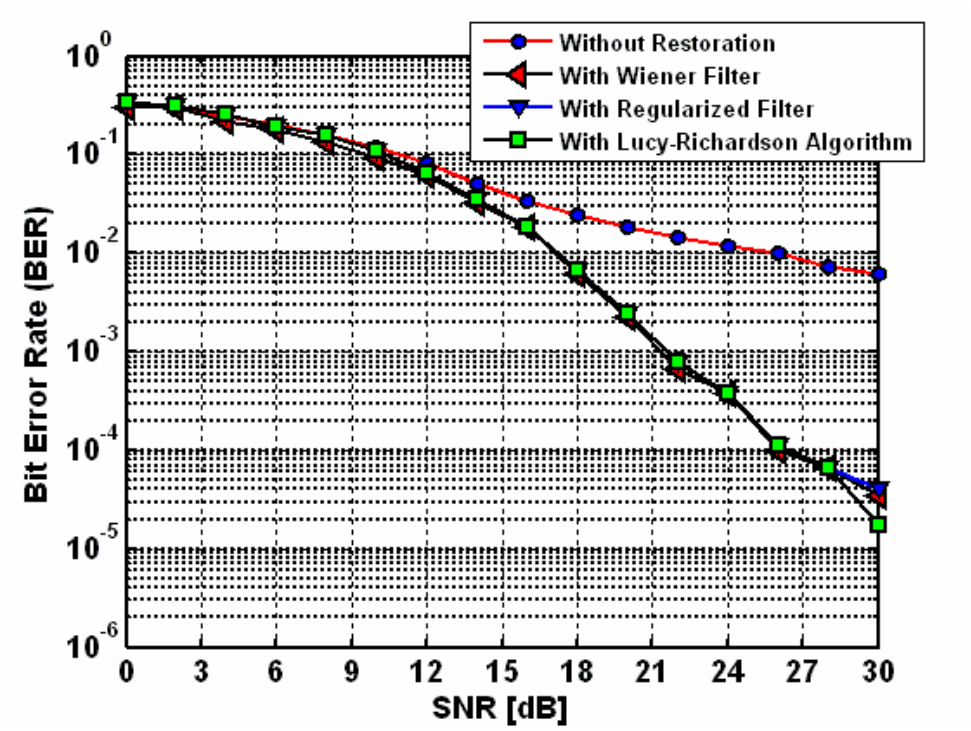

Figure 4.42: BER Performance of the DACD Detector Against *3x3* Gaussian Low-Pass Filter with Parameter 0.8 and Various Restoration Methods

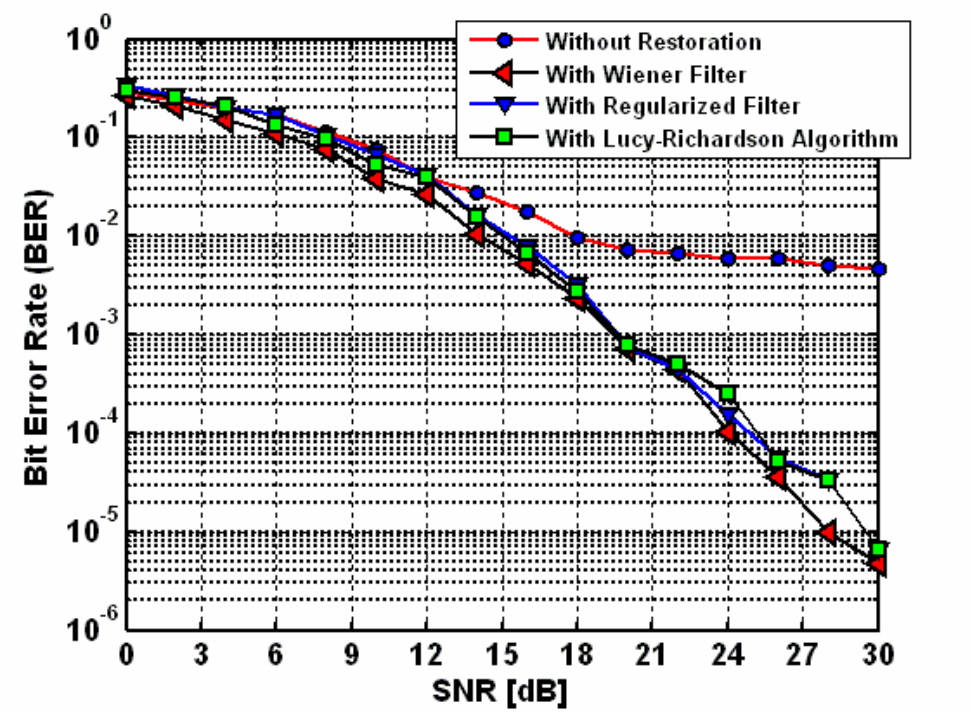

Figure 4.43: BER Performance of the Proposed CRED Detector Against *3x3* Gaussian Low-Pass Filter with Parameter 0.8 and Various Restoration Methods

4.6. Conclusions

In this chapter, we investigate the performances of the watermark detectors described in Chapter 3, in the non-blind watermarking system in DCT domain. Our primarily concern is to both characterize the degradations by employing the proposed CRED detector and decrease effects of them by using image restoration algorithms.

We can conclude from the simulation results that the proposed CRED detector increases the detection performance of the watermarking system both in terms of BER and in terms of correlation coefficient between the embedded and the recovered watermark against pre-mentioned channel distortions and attacks. For example, when we set the target correlation coefficient to 0.7; the proposed CRED detector decreases the JPEG quality factor from 12 to 9 in comparison to the DACD detector. It also decreases the JPEG quality factor from 14 to 9 in comparison to the MRD detector. Thus, we can conclude that if the receiver employs the proposed CRED detector, the transmitter can more aggressively compress the watermarked signal. In addition, the image restoration algorithms improve the system capacity, robustness and the decreases the BER of the recovered watermark by decreasing the effects of the degradations. Especially, the proposed CRED detector achieves the major improvement when the image restoration algorithms applied. For example, when we set the target BER to 10^{-4} in the Wiener filter restroration; the proposed CRED detector achieves 4 dB SNR gain in comparison to the DACD detector. It also achieves 7 dB SNR gain in comparison to the MRD detector.

Finally, we compare the required detection time for the employed detection algorithms. The simulations are run on a PC with 512 MB RAM, Intel Celeron 1,5 GHz CPU, and Windows XP operating system. The MRD detector requires 5,305070 seconds, the DACD detector requires 5,23121 seconds, and the proposed CRED detector requires 5,272602 seconds. Thus we can claim that the proposed CRED detector has the lowest computational complexity.

5. CONCLUSIONS & FUTURE WORK

The performance of digital watermarking systems is limited with the watermark detection methods used for recovering the embedded watermark. In this thesis, we develop several watermark detection schemes for various digital watermarking systems.

The simulations results demonstrate that the digital watermarking systems, which employ the proposed watermark detection methods, improve their detection performance both in terms of bit error rate and the correlation coefficient between the recovered watermark and embedded watermark. On the other hand, we may test the robustness of the detectors against different channel distortions and attacks such cropping, copying, rotation etc. by employing Stirmark benchmark tool [43].

In this thesis, we only employ repetition coding. In the future work, as we model the digital watermarking system as a communication channel, we can employ more intelligent error correction codes such as hamming codes, turbo codes, LPDC codes etc. in order to recover the embedded watermark with low bit error rates. In addition, the watermarked image may be pre-processed with the improved and more intelligent image restorations algorithms for reducing and compensating the effects of channel distortion and attacks just before the watermark detection process. Furthermore, we can employ JPEG quantization table in the embedding process in the spread spectrum based watermarking system. Thus, we can investigate the effects of quantization on the host signal interference.

APPENDIX A – SNR AND WDR GAIN TABLES TO ACHIEVE SOME TARGET BER AND CORRELATION COEFFICIENTS FOR QUANTIZATION BASED WATERMARKING SYSTEM

Target Correlation Coefficient	Required SNR for MRD Detector	Required SNR for DACD Detector	Required SNR for CRED Detector
0,4	22 dB	15 dB	13 dB
0,5	25 dB	12 dB	15 dB
0,6	26 dB	18 dB	17 dB
0,7	28 dB	20 dB	18 dB
0,8	30 dB	24 dB	21 dB
0,9	35 dB	30 dB	27 dB

Table 1: Target Correlation Coefficients versus Required SNR for Detectors

Target Correlation Coefficient	Required JPEG Quality Factor for MRD Detector	Required JPEG Quality Factor for DACD Detector	Required JPEG Quality Factor for CRED Detector
0,4	71	29	25
0,5	78	36	30
0,6	83	40	33
0,7	87	44	42
0,8	91	56	46
0,9	97	76	62

Table 2: Target Correlation Coefficients versus Required JPEG Quality Factor for Detectors

Target BER	Required WDR for MRD Detector	Required WDR for DACD Detector	Required WDR for CRED Detector
10^{-3}	--	-28 dB	-30 dB
10^{-4}	--	-20 dB	-25 dB
10^{-5}	--	--	-20 dB

Table 3: Target BERs versus Required WDR for Detectors at 25 dB SNR

Target BER	Required WDR for MRD Detector	Required WDR for DACD Detector	Required WDR for CRED Detector
10^{-3}	--	-28 dB	-30 dB
10^{-4}	--	-20 dB	-25 dB
10^{-5}	--	--	-20 dB

Table 4: Target BERs versus Required WDR for Detectors when the Watermarked Image is exposed to JPEG Compression with Quality Factor 70

Target BER	Required WDR for MRD Detector	Required WDR for DACD Detector	Required WDR for CRED Detector
10^{-3}	--	-28 dB	-32 dB
10^{-4}	--	-23 dB	-27 dB
10^{-5}	--	--	-21 dB

Table 5: Target BERs versus Required WDR for Detectors when the Watermarked Image is exposed to *3x3* Mean Filter attack

Target BER	Required WDR for MRD Detector	Required WDR for DACD Detector	Required WDR for CRED Detector
10^{-3}	--	-29 dB	-31 dB
10^{-4}	--	-22 dB	-26 dB
10^{-5}	--	--	-21 dB

Table 6: Target BERs versus Required WDR for Detectors when the Watermarked Image is exposed to *3x3* Median Filter attack

APPENDIX B – SNR GAIN AND JPEG QUALITY FACTOR TABLES TO ACHIEVE SOME TARGET BER AND CORRELATION COEFFICIENTS WITHOUT IMAGE RESTORATION FOR NON-BLIND WATERMARKING SYSTEM

Target BER	Required SNR for MRD Detector	Required SNR for DACD Detector	Required SNR for CRED Detector
10^{-3}	24 dB	20 dB	16 dB
10^{-4}	27 dB	24 dB	20 dB
10^{-5}	30 dB	29 dB	25 dB

Table 7: Target BER versus Required SNR for Detectors

Target Correlation Coefficient	Required JPEG Quality Factor for MRD Detector	Required JPEG Quality Factor for DACD Detector	Required JPEG Quality Factor for CRED Detector
0,5	8	7	6
0,6	10	9	8
0,7	14	12	9
0,8	16	14	11
0,9	22	17	14

Table 8: Target Correlation Coefficient versus Required JPEG Quality Factor for Detectors

Target Correlation Coefficient	Required SNR for MRD Detector	Required SNR for DACD Detector	Required SNR for CRED Detector
0,5	6 dB	4 dB	2 dB
0,6	7 dB	6 dB	3 dB
0,7	9 dB	8 dB	4 dB
0,8	12 dB	9 dB	7 dB
0,9	15 dB	13 dB	10 dB

Table 9: Target Correlation Coefficient versus Required SNR for Detectors

Target BER	Required Insertion Strength for MRD Detector	Required Insertion Strength for DACD Detector	Required Insertion Strength for CRED Detector
10^{-3}	0,14	0,113	0,11
10^{-4}	--	0,116	0,13
10^{-5}	--	0,15	0,138

Table 10: Target BER versus Required Insertion Strength for Detectors against *3x3* Mean Filter Attack

Target BER	Required Insertion Strength for MRD Detector	Required Insertion Strength for DACD Detector	Required Insertion Strength for CRED Detector
10^{-3}	0,13	0,113	0,11
10^{-4}	--	0,132	0,121
10^{-5}	--	0,15	0,141

Table 11: Target BER versus Required Insertion Strength for Detectors Against *3x3* Median Filter Attack

APPENDIX C - SNR GAIN AND JPEG QUALITY FACTOR TABLES TO ACHIEVE SOME TARGET BER AND CORRELATION COEFFICIENTS WITH IMAGE RESTORATION FOR NON-BLIND WATERMARKING SYSTEM

Target BER	Required SNR for MRD Detector	Required SNR for DACD Detector	Required SNR for CRED Detector
10^{-3}	24 dB	19 dB	16 dB
10^{-4}	28 dB	25 dB	21 dB
10^{-5}	---	30 dB	23 dB

Table 12: Target BER versus Required SNR in case of Wiener Filter Restoration for Detectors against Mean Filter+AWGN

Target BER	Required SNR for MRD Detector	Required SNR for DACD Detector	Required SNR for CRED Detector
10^{-3}	24 dB	20 dB	18 dB
10^{-4}	28 dB	25 dB	22 dB
10^{-5}	---	30 dB	23 dB

Table 13: Target BER versus Required SNR in case of the LR Algorithm Restoration for Detectors Mean Filter+AWGN

Target BER	Required SNR for MRD Detector	Required SNR for DACD Detector	Required SNR for CRED Detector
10^{-3}	24 dB	20 dB	18 dB
10^{-4}	28 dB	25 dB	22 dB
10^{-5}	---	30 dB	23 dB

Table 14: Target BER versus Required SNR in case of Regularized Filter Restoration for Detectors Mean Filter+AWGN

Target BER	Required SNR for MRD Detector	Required SNR for DACD Detector	Required SNR for CRED Detector
10^{-3}	--	21 dB	19 dB
10^{-4}	--	26 dB	24 dB
10^{-5}	---	--	28 dB

Table 15: Target BER versus Required SNR in case of Wiener Filter Restoration for Detectors Gaussian Low-Pass Filter+AWGN

Target BER	Required SNR for MRD Detector	Required SNR for DACD Detector	Required SNR for CRED Detector
10^{-3}	--	22 dB	20 dB
10^{-4}	--	26 dB	25 dB
10^{-5}	---	--	29 dB

Table 16: Target BER versus Required SNR in case of the LR Algorithm Restoration for Detectors Gaussian Low-Pass Filter+AWGN

Target BER	Required SNR for MRD Detector	Required SNR for DACD Detector	Required SNR for CRED Detector
10^{-3}	--	22 dB	19 dB
10^{-4}	--	26 dB	25 dB
10^{-5}	---	--	29 dB

Table 17: Target BER versus Required SNR in case of Regularized Filter Restoration for Detectors Gaussian Low-Pass Filter+AWGN

REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding: A Survey”, Proc. IEEE, 87(7):1062–1078, July 1999.

[2] I.J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. Image Processing, vol. 6, pp 1673-1687, Dec. 1997.

[3] B.M. Macq and Macq and J.J Quisquater, “Cryptology for digital TV broadcasting”, Proceedings of IEEE, vol. 83, pp. 944-957, June 1995.

[4] S.C. Katzenbeisser, “Principles of Steganography”, Information Techniques for Steganography and Digital Watermarking, Eds. Northwood, MA: Artec House, pp 2-40 , Dec. 1999

[5] J.R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure," IEEE Trans. Image Processing, vol. 9, pp 55-68, Jan. 2000.

[6] N. Komatsu and H. Tominaga “Authentication system using concealed images in telematics” Memoirs of the School of Science and Engineering, Waseda University, 52:45.60, 1988.

[7] Ingemar J.Cox, Matthew L.Miller, and Jeffrey A.Bloom,“Digital Watermarking,” Morgan Kaufmann Publishers, 2002.

[8] Digimarc Corporation. Corporate website, http://www.digimarc.com/.

[9] F. Pérez-González, P. Comesaña, and F. Balado, “Dither-Modulation Data hiding with distortion-compensation: exact performance analysis and an improved detector for JPEG attacks,” In Inter. Conf. on Image Processing, Barcelona, Spain, Sep 2003.

[10] F.Perez-Gonzalez, M.Amado, and J.R.Hernandez, “Performance Analysis of Existing and New Methods for Data Hiding with Known-Host Information in Additive Channels,” IEEE Trans. Signal Processing, vol. 51, pp. 960 - 980, April 2003.

[11] Alexia Briassouli, Panagiotis Tsakalides, "Hidden Messages in Heavy Tails: DCT-Domain Watermark Detection Using Alpha-Stable Models," IEEE Trans. Multimedia., vol. 7, pp 700-715, August 2005.

[12] I.J. Cox, M.L. Miller, and J.A. Bloom, “Watermarking Applications and Their Properties,” Proc. of Inter, Conf. on Information Technology: Coding and Computing - ITCC2000, pp. 6-10, 2000.

[13] I.J. Cox, M.L. Miller, J. M. G. Linnartz, and T. Kalker, “A Review of Watermarking Principles and Practices”, DSP for Multimedia Systems, K. K. Parhi, T. Nishitani (eds.), Marcell Dekker, Inc. NY, pp. 461-485, (1999).

[14] J.J.Eggers, J.K. Su, and B. Girod, “Robustness of a Blind Watermarking Scheme,” Proc. IEEE International Conference on Image Processing, ICIP-2000, Vancouver, Canada, Sept 2000.

[15] I.J.Cox, M.L. Miller, and A.L. McKellips, “Watermarking as Communications with Side Information,” Proc. of IEEE, 87(7), pp. 1127-1141, (1999).

[16] W.Trappe, M. Wu, Z. Wang, K.J.R. Liu, “Anti-collusion Fingerprinting for Multimedia,” IEEE Trans. on Signal Processing, Vol. 51(4), pp.1069-1087, April 2003.

[17] H. Zhao, M. Wu, Z.J. Wang, and K.J.R. Liu, “Performance of Detection Statistics Under Collusion Attacks on Independent Multimedia Fingerprints,” Proc. ICME'03, Baltimore, MD, July 2003.

[18] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, “Perceptual Watermarks for Digital Images and Video”, Proce. IEEE, Vol. 87(7), pp. 1108-1126, July 1999.

[19] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney, “Robust audio watermarking using perceptual masking,” Signal Processing, vol. 66, pp. 337-355, 1998.

[20] D. Kundur, “Multiresolutation Digital Watermarking: Algorithms and Implications for Multimedia Signals”, Ph. D. Dissertation, University of Toronto, 1999.

[21] D. Kundur, “Improved Digital Watermarking through Diversity and Attack Characterization”, Proc. Workshop on Multimedia Security at ACM Multimedia ‘99, pp. 53-58, Orlando, Florida, Oct 1999.

[22] D. Kundur, and D. Hatzinakos, “Attack Characterization for Effective Watermarking," Proc. ICIP’99, pp. 240-244, Oct 1999.

[23] D. Kundur, and D. Hatzinakos, “Improved Robust Watermarking through Attack Characterization”, Optics Express focus issue on Digital Watermarking, vol. 3(12), pp. 485-490, Dec 1998.

[24] J. A. Bloom, I. J. Cox, T. Kalker, J-P Linnartz, M. L. Miller, and B. Traw, “Copy Protection for DVD Video”, Proc. of IEEE, 87 (7), pp 1267-1276, 1999.

[25] T. Kalker, G. Depovere, J. Haitsma and M. Maes, “A video watermarking system for broadcast monitoring,” in the Proceedings of SPIE: Security and Watermarking of Multimedia Contents, San Jose, CA, 1999

[26] I.J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. Image Processing, vol. 6, pp 1673-1687, Dec. 1997.

[27] A. J. Ahumada and H. A. Peterson, "Luminance-model-based DCT quantization for color image compression", Proc. SPIE on Human Vision, Visual Processing, and Digital Display III, vol. 1666, pp. 365-374, 1992.

[28] J. A. Solomon, A. B. Watson, and A. J. Ahumada, "Visibility of DCT basis functions: Effects of contrast masking," in Proc Data Compression Conf., Snowbird, UT, 1994, pp. 361-370.

[29] A. B. Watson, "Visual optimization of DCT quantization matrices for individual images," in Proc. AIAA Computing in Aerospace 9, .San Diego, CA, 1993, pp. 286-291.

[30] K. A. Birney and T. R. Fischer, "On the modelling of DCT and subband image data for compression," IEEE Trans. Image Processing, vol. 4, pp 186-193, Feb. 1995.

[31] Çağatay Karabat, Mehmet Keskinöz, “Block Normalization Based Blind Detectors for Spread Spectrum Watermarking Systems” in Proc. IEEE, SIU 2007, Eskisehir, Turkey

[32] Fabien A. P. Petitcolas and Ross J. Anderson, "Evaluation of copyright marking systems," in Proc. IEEE Multimedia Systems’99, Florence, Italy, vol. 1, 7-11 June 1999, pp. 574–579.

[33] D.Kundur and D.Hatzinakos, "Digital Watermarking using Multiresolution Wavelet Decomposition," in Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, Seattle, Washington, vol. 5, pp. 2969-2972, May 1998.

[34] D.Kundur and D.Hatzinakos, "Diversity and Attack Characterization for Improved Robust Watermarking," IEEE Trans. Image Processing, vol. 49, pp. 2383-2396, Oct. 2001.

[35] D.Kundur, “Multiresolution digital watermarking: Algorithms and implications for multimedia signals,” Ph.D. dissertion, Univ. Toronto, Toronto, Canada, August 1999.

[36] Çağatay Karabat, Mehmet Keskinöz, “A New Blind Detection Method Based On Channel Reliability Estimates for Robust Watermarking” IEEE, in Proc. IEEE, SIU 2007, Eskisehir, Turkey

[37] A.Piva, M.Barni, F.Bartolini and V.Cappelini, “DCT-Based watermark recovering without resoting the uncorrupted image,” in *IEEE ICIP,* 1997.

[38] Gonzalez, R.C. & Woods, R.E. , “Digital Image Processing, ” Upper Saddle River, NJ: Prentice Hall., 2002.

[39] Boland, F. Doyle, T. , “Deconvolution in Real Time Noisy Signals,” Acoustics, Speech, and Signal Processing, IEEE International Conference on ICASSP, 1982.

[40] Mehmet Bilgen, Hsien-Sen Hung “Constrained least-squares filtering for noisy images blurred by random point spread function,” in SPIE, Volume 33, Issue 6, pp. 2020-2023, 1994.

[41] Richard L. White, “Image restoration using the damped Richardson-Lucy method”, in Proc.of the Restoration of HST Images and Spectra II, Baltimore, MD, 1994.

[42] David S. C. Biggs and Mark Andrews, “Iterative blind deconvolution of extended objects”, in Proc. ICIP ’97, volume II, pages 454–457, Santa Barbara, CA, October1997.

[43] www.petitcolas.net/fabien/watermarking/stirmark