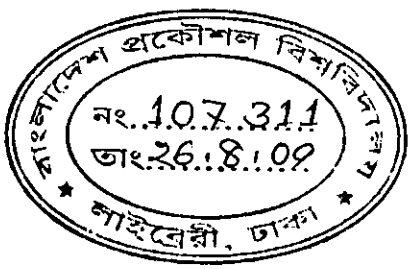
A Statistical Method for Detection of Watermarks in Digital Images

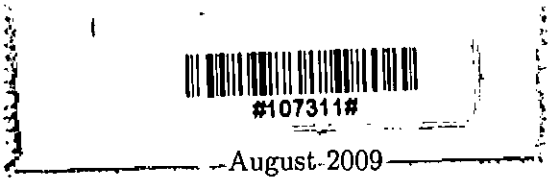
by

Rubaiya Rahman



MASTER OF SCIENCE IN ELECTRICAL AND ELECTRONIC ENGINEERING

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY



August 2009

The thesis entitled **"A Statistical Method for Detection of Watermarks in Digital Images"** submitted by Rubaiya Rahman Roll No.: 100706230P, Session: October, 2007 has been accepted as satisfactory in partial fulfillment of the requirements for the degree of **Master of Science in Electrical and Electronic Engineering** on August 17, 2009.

BOARD OF EXAMINERS

1. _____ **Chairman**
(Dr. Mohammed Imamul Hassan Bhuiyan) (Supervisor)
Assistant Professor
Department of Electrical and Electronic Engineering
Bangladesh University of Engineering and Technology
Dhaka - 1000.

2. _____ **Member**
(Dr. Aminul Hoque) (Ex-officio)
Professor and Head
Department of Electrical and Electronic Engineering
Bangladesh University of Engineering and Technology
Dhaka - 1000.

3. _____ **Member**
(Dr. Newaz M. Syfur Rahim)
Associate Professor
Department of Electrical and Electronic Engineering
Bangladesh University of Engineering and Technology
Dhaka - 1000.

4. _____ **Member**
(Dr. Shaikh Anowarul Fattah)
Assistant Professor
Department of Electrical and Electronic Engineering
Bangladesh University of Engineering and Technology
Dhaka - 1000.

5. _____ **Member**
(Dr. Farruk Ahmed) (External)
Professor
Department of Computer Science and Engineering
North South University, Dhaka - 1209.

Declaration

It is hereby declared that this thesis or any part of it has not been submitted elsewhere for the award of any degree or diploma.

Signature of the candidate

(Rubaiya Rahman)

Dedication

To my beloved husband.

Acknowledgements

In the course of my life, each accomplishment that I have made, every success that I have acquired, was not a stand alone outcome, rather they were influenced by people around me, specially those having special place in my life. This thesis also owes to some people, without whose support it would be difficult for me to complete it. Among those people, the one person who stands out above the rest is my respectable supervisor, Dr. Mohammed Imamul Hassan Bhuiyan. I am greatly indebted to him for his guidance, limitless patience and constant support that was critical for completing this research. It was an honor working with him.

I would like to thank Prof. Dr. Aminul Hoque, the Head of the EEE department, BUET, for his time, valuable suggestions and correction for my thesis. I like to express my gratitude to Prof. Dr. Farruk Ahmed for his time for reviewing the thesis and be a part of my M.Sc. thesis defense committee. I would also like to thank Drs. Newaz M. Syfur Rahim and Shaikh Anowarul Fattah for their kind consideration to be members for the defense committee and review the thesis.

I would be always indebted to my parents who have provided me all necessary things of my life even before I asked for it. Their endless effort, and continuous guidance and support have made me reach the position where I am today. I would like to express my heartiest gratitude to my husband without whom it would be nearly impossible for me to complete this thesis while passing through a critical phase of life. His persistent inspiration and guidance helped me in every crucial steps of my academic life.

And last but not the least, I must express my gratitude towards Almighty *Allah*, *Who* blessed me with *His* endless mercy, *Filled* me with diligence and perseverance, and most importantly, *Created* kindness in so many people who provided me with the necessary support I required.

Contents

List of abbreviations

BKF	Bessel K Form
CDF	Cumulative Density Function
DCT	Discrete cosine transform
DFT	Discrete Fourier transform
DWT	Discrete Wavelet Transform
GG	Generalized Gaussian
HVS	Human Visual System
JND	Just Noticeable Distortion
KLD	Kullback-Leibler Divergence
KSD	Kolmogorov-Smirnov Distance
MAP	Maximum A Posterior
ML	Maximum Likelihood
pdf	Probability Density Function
PRS	Pseudo-Random Sequence
PSNR	Peak Signal to Noise Ratio
ROC	Receiver Operating Characteristic
S α S	Symmetric Alpha Stable
SNIG	Symmetric Normal Inverse Gaussian
WDR	Watermark to Document Ratio

List of Figures

List of Tables

Abstract

Watermarking is an effective tool for providing copyright protection to data such as digital image, video and audio from illegal manipulations. Since accurate data modeling is key to properly detect watermarks in images, blind watermark detection by statistics of the data has received lots of attention in recent past. Discrete Cosine Transform (DCT) based watermark detection techniques are quite popular due to the use of DCT in various image and video processing standards. Several DCT based statistical methods have been proposed in the literature for watermark detection. However, these methods have drawbacks such as the inability of the prior probability density function (pdf) to appropriately model the DCT coefficients and lack of closed-form expression for the pdf. Recently, the Symmetric Normal Inverse Gaussian (SNIG) pdf has been shown to be a highly effective prior for modeling the DCT coefficients of digital images. The aim of this thesis is to develop an efficient DCT based method for watermark detection by using the SNIG pdf as the modeling prior. Analytical expression are obtained for the Bayesian log-likelihood ratio, and corresponding conditional mean and variances. Extensive simulations are carried out to study the effectiveness of the proposed method and compare it with that of the state-of-the-art methods. The results show that the proposed method performs better than the other methods in terms of the associated probabilities of detection and false alarm, and probability of detection for watermarks of varything strength. Finally, a study is conducted to show that the SNIG pdf is equally effective for modeling video DCT coefficients and thus has potential to be employed for developing an efficient watermark detector for video data.

Chapter 1

Introduction

1.1 Watermarking

Today, we live in an age of pervasive digital information technology that has brought us high quality video compression, increasing network bandwidth and accessibility, dense portable storage media (e.g. CD-R, DVD-R), and compounding processing power on every desktop. The digitized multimedia documents are not only easy to reproduce, but also can be quickly and massively transferred across the internet. The ease of acquisition, storage, reproduction and distribution of digitized documents has created an urgent need for copyright enforcement technologies that can protect copyright ownership of multimedia objects. Digital image watermarking is one such technology that has been developed to protect digital images from illegal manipulations.

Digital watermarking is a process that embeds an imperceptible and statistically undetectable signature to multimedia content (e.g. images, video and audio sequences). The term 'watermark' stands for the hiding of some message or other kind of information into an image. This information is called 'watermark' and the image that hosts it is the 'cover image'. The embedded watermark may contain certain information (signature, logo, ID number, etc.) associated exclusively to the owner, distributor or the multimedia file itself. Therefore, watermarks can be used to prevent illegal use, copy or manipulation of the cover image, as proof of ownership or tampering and others. In this manner, the watermark travels with the data, which thus remains protected until its intended receiver removes it. In Fig. 1.1, a general watermarking scheme is shown to give an idea of the different operations involved in the process.

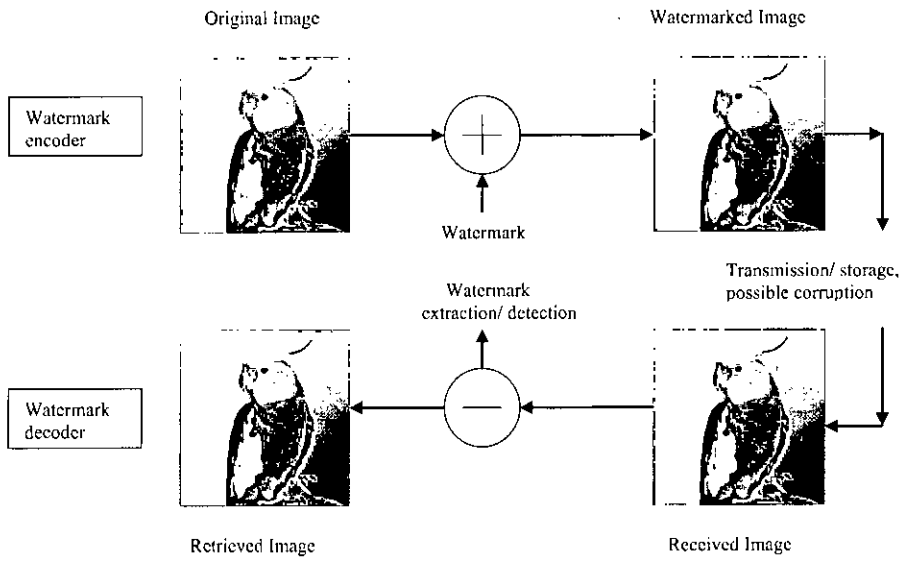


Fig. 1.1: General watermarking scheme

Like watermarking, there are some other traditional methods that has been used as security application for data, i.e. the addition of access control headers, cryptography and steganography. But, in these methods, once the copyright control mechanisms are surmounted, the original data remains unprotected. Watermarking differs from these data protecting mechanism in the way that, even if the entire embedding algorithm is known to an attacker, its security depends only on a secret key [1].

Considering the type of embedded content, two main types of watermarking schemes exist. A watermarking system may embed a specific piece of information in the data, such as identification numbers used for image tracking or classification and for video distribution. In this case, the embedded watermark communicates a message which must be extracted with accuracy. The other type of system, often used in copyright-protection applications, embeds a watermark which modifies the original data, but does not necessarily communicate a message. Hence, only the presence of the watermark needs to be verified in order to determine whether or not the data is protected.

Again, regarding the process of watermarking, current digital watermarking techniques can be grouped into three major classes: spatial-domain, transform-

domain and hybrid watermarking techniques [2], [3]. Commonly used transform-domain techniques include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT).

Spatial domain techniques directly add the watermark to pixel values, which allow to easily exploit the characteristics of the Human Visual System (HVS) for better hiding the data.

Transformed domain techniques are also referred as frequency domain technique as they add the watermark to the coefficients of a full-frame transform (DFT, DCT, Mellin, Radon, Fresnell) of the image. These do not allow to localize precisely the watermarking disturb over the image, and thus make it difficult to tune it to the HVS characteristics.

Finally, hybrid techniques (mainly using block-wise DCT, and wavelets) are those working in a transformed domain, but without completely loosing spatial localization.

The main strengths of spatial domain methods are that they are conceptually simple and have very low computational complexities. As a result they have proven to be most attractive for watermarking applications where real-time performance is a primary concern. But, compared to pixel domain techniques, transform domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms. Spatial domain watermarks exhibit some disadvantages not only in terms of the trade-off between invisibility and robustness, but also for the fact that a common picture-cropping operation can eliminate the watermark [4], [5].

Usually transformed domain techniques spreads the watermark over the whole image, which makes them intrinsically more resistant to cropping than spatial domain techniques where resistance to cropping can only be granted by repeating the watermark across the whole image [6]. Generally the main drawback of transform domain methods is their higher computational requirement.

Hybrid techniques try to trade off between the advantages of spatial domain techniques in the localization of the watermarking disturb, and the good resistance to attacks of transformed domain techniques.

Invisible watermarking can be really useful in several areas of interest involving digital images. Some important applications of watermark include fingerprinting,

indexing, copyright protection and owner identification, broadcast monitoring, copy protection, data authentication, covert communications, medical safety etc.

1.1.1 Properties of Watermark

The effectiveness of a digital watermarking method depends on some crucial factors, for example its imperceptibility, and robustness to common image manipulations like compression, filtering, rotation, scaling cropping, collusion attacks among many other digital signal processing operations.

The factors that must be considered in image or video watermarking are:

- Perceptual invisibility, i.e. how easily the watermark can be discerned by the user. A watermark should not hurt the commercial or art value of the host.
- Robustness, i.e. the resistance of the watermark to alterations of the original conteut such as compression, filtering or cropping. A watermark should be resistant to a variety of manipulations, either unintentional or malicious.
- Indelibility; the watermark must be difficult or even impossible to remove by a hacker, at least without obviously degrading the original signal.
- Capacity, i.e. the amount of information that can be put into the watermark and recovered without errors.
- Unambiguity, i.e. the owner should be identified unambiguously through retrieval of the watermark, and the accuracy of identification should degrade gracefully in the face of attack.
- Statistically undetectable, i.e. a pirate should not be able to detect the watermark by comparing several watermarked signals belonging to the same author.
- Trustworthy detection; the detection should be accurate and especially the false-alarm rate should be very small.
- Computational efficiency; for various applications, realtime watermarking is desirable.

These factors are inter-dependent; for example, increasing the capacity will decrease the robustness and increase the visibility. Therefore, it is essential to consider all these factors for a fair evaluation or comparison of watermarking algorithms.

1.2 Watermark Detection

The watermark detection method can take on different approaches depending on the way the watermark is inserted, and the nature of the watermarking algorithm. In some watermark recovery methods, a watermark can be extracted in its exact form, which is usually referred as watermark extraction. In other cases, we can only detect whether a specific given watermarking signal is present in an image, which can be referred as watermark detection. Both of these approaches have significant applications [7] , [8]. For example in an image authentication application, a robust hash function of the image is embedded as a watermark. Later, this embedded hash value is extracted and compared against the computed hash value to assert whether an image is authentic or has been significantly modified. In contrast, for a broadcast monitoring application, a monitoring station is placed by a news agency in the broadcast region of each local station. This monitoring station continually examines local broadcast content for clips that contain the specific watermark of the news agency. Presence of a watermark indicates that its content was aired by the local station and for which charges would be due. Here, the monitoring station need only detect the presence of a watermark. There are no information bits that need to be extracted from the watermarked content [7] , [8].

Watermark detection is a typical binary hypothesis testing problem to decide whether the watermark is present or not . An important issue concerning watermark recovery (detection or extraction) techniques is the availability of the original data. Regarding this issue, there are two basic approaches for watermark detection: Non-blind and blind detection.

Non-blind Detection

Here, watermark recovery is facilitated when the host data is available, since one can then detect any distortions in the data and invert them to accurately recover

the hidden signal.

Blind Detection

In blind decoding the decoder does not need the original image or any information derived from it, to recover the watermark. These methods usually employs only the secret key to perform detection process.

Although non-blind decoding is beneficial to some extent in terms of robustness, it is not desirable in many cases, where the availability of the original data can not be granted [1]. It is important in many practical applications such as data monitoring or tracking on the Internet, where the access to original data is not possible; or database watermarking, where the storage and retrieval in a huge database might become a heavy burden. Moreover, in many multimedia settings, e.g., in video watermarking, the use of the host data is impractical because of its large volume. This is why most current watermark detection methods aim to extract the watermark without use of the original host signal, using the secret key only [1], [9].

1.3 Motivation

The focus of this thesis is on the problem of watermark detection in digital images, i.e., the problem of verifying whether the image is watermarked or not. As the principal aim of all data protecting scheme is to identify whether the document has been corrupted by an attacker or not, watermark detection can serve this purpose adequately without the consideration of watermark extraction. Although there have been many watermark detectors designed so far [1], [7], [10], [11], there is still demand for the development of efficient and effective detectors. This thesis considers transform domain watermarking as it is inherently more resistant and effective than spatial domain techniques [3]. Among the different transform domain methods, DCT-based watermark embedding and detection is the classic and still most popular approach. This work addresses watermarking in the DCT domain, since it leads to better implementation compatibility with popular compression standards (JPEG/MPEG) widely used in commercial application. The new wavelet-based JPEG-2000 image compression standard has received so far only very limited endorsement from digital camera manufacturers and software

developers. As a matter of fact, the classic JPEG still dominates the consumer market and the near-totality of pictures circulated on the internet is compressed using this old standard. Moreover, the Block-DCT is the workhorse on which even the latest MPEG video coding standards rely upon. There are no convincing indicators suggesting that the current trend is about to change any time soon.

Statistical methods incorporate the image statistics which perform significantly better than Gaussian-correlator or spatial domain methods. Several DCT domain statistical image data models are proposed in the literature [1], [12 - 16]. Most of these methods suffer from the inability of prior pdfs in capturing the image statistics appropriately and lack of closed-form expression of the pdfs. There is still demand for an accurate and effective data model. In this thesis, a symmetric normal inverse Gaussian (SNIG) pdf modeling of the DCT coefficients for developing an efficient watermark detection method. The use of SNIG pdf is motivated from [17] where it is reported to be a highly effective prior for modeling the DCT coefficients of natural images. As the accuracy of data modeling directly affects the detector performance, the SNIG-based detector is more likely to perform better than the other pdf-based detectors. Rigorous mathematical analysis for different hypotheses and extensive simulation results would corroborate the superiority of SNIG pdf based watermark detector. Furthermore, there is motivation to explore the suitability of SNIG pdf for modeling video DCT coefficients, given its potential in developing efficient watermark detector for video data.

1.4 Objectives

Our thesis has some definite objectives and potential scope in data protection field which may be stated as the following:

1. To develop an effective statistical watermark detector for digital images using Symmetric Normal Inverse Gaussian (SNIG) model. The image data would be first modeled by SNIG distribution and then applied for designing the detector.

2. To investigate the performance of the SNIG model based watermark detec-

tor. The performance will be analyzed by relating the probability of detection to the probability of false alarm for watermarks of different strength.

3. To study the effectiveness of using the SNIG pdf in modeling digital video data to find its potential in developing efficient watermark detector for video.

1.5 Organization of the Thesis

This thesis consists of five chapters. Following introduction in Chapter 1, a brief review of the state-of-the-art watermark detectors are discussed in Chapter 2. After reviewing watermark embedding rules, various detection methods reported in the literatnre are described. In Chapter 3, the proposed watermark detector with its mathematical framework is presented. The performance analysis of the detector is shown in terms of Receiver Operating Characteristic (ROC) curves and relation between detection probability and watermark strength. Chapter 4 presents a study on the effectiveness of the SNIG pdf in modeling video data in the DCT domain. Finally, in Chapter 5, a summary of the thesis work is given and some suggestions about the future scope of this work is provided.

Chapter 2

Watermark Generation and Detection Methods

2.1 Introduction

Before presenting the proposed statistical watermark detector me, an overview of the previous work in this field is provided in this chapter. The chapter begins with a closer look at the state of the art practices in digital watermarking of visual data, and then particular attention is paid to watermark recovery as it has significant impact on the final reliability of the whole watermarking system.

2.2 Watermark Embedding

Watermark embedding is the first step to be considered when a watermarking system is designed. Traditionally, the choice of a particular embedding strategy was driven by perceptual considerations. It has been demonstrated that, the choice of the embedding rule can be effectively made in such a way to optimize the performance of the watermark recovery step [18], [19].

Once the host features are chosen, the embedding rule is specified. Commonly, watermarks are embedded in an additive or multiplicative manner. For additive one,

$$y_i = x_i + \gamma m_i \tag{2.1}$$

where, x_i is the ith component of the original feature vector, m_i the ith sample of the watermark, γ is a parameter controlling the watermark strength, and y_i is the ith component of the watermarked feature vector; and for the multiplicative

one,

$$y_i = x_i + \gamma m_i x_i \tag{2.2}$$

where, the symbols have the same meaning as in equation (2.1). Additive watermarks are mainly used in spatial and hybrid techniques, while multiplicative watermarks are often found in transform domain techniques.

2.2.1 Perceptual Hiding

The merits of perceptual hiding is two-fold: on one side perceptual considerations allow to better hide the watermark, thus making it less perceivable to the eye, on the other side they allow the use of the highest possible watermark strength, thus positively influencing the performance of the watermark recovery step.

In watermark embedding, properties of the human visual system (HVS) must be taken into account to guarantee imperceptibility of the hidden signal. The area of the image where the eye is less sensitive to noise, in fact, are suitable to heavy watermark embedding. The following principles can be followed in this regard:

1. the eye is more sensitive to noise in uniform areas than in highly textured ones,
2. the eye is more sensitive to noise around edges than in highly textured areas, and
3. the eye is less sensitive to noise in extremely dark and bright regions.

In spatial domain watermarking, visual masking is achieved by simply weighting [20] each sample of the watermark vector by a value depending on the local characteristics of the image. The weights are obtained by using the principles outlined above.

In blockwise DCT-based hybrid techniques, the well known Just Noticeable Distortion (JND) values, derived from the literature on compression algorithms, can be used for weighting the watermark coefficients [21].

For wavelet based algorithms, similar weighting maps can be used. The maps can either depend solely on the particular embedding sub-band [21] or, more effectively, also on local image characteristics [22].

Transformed domain techniques require a more complicated treatment [23]. Their peculiarity is that they spread the watermark uniformly all over the image, i.e., the same watermark energy is added to the areas were the eye is more sensitive to noise and to those were it is less sensitive. In order to exploit the iso-frequency masking effect, the multiplicative embedding rule is preferred.

2.3 Watermark Recovery

Recovery (detection/extraction) of the watermark is an integral part of watermarking scheme, and undoubtedly it is vitally important to perform the recovering procedure with a high degree of reliability in all practical applications. No need to say, then, that the watermark decoder must be carefully designed in order to extract from data as much information as possible. Of course, watermark recovery can not leave out of consideration the embedding rule used to insert the watermark within the host data. Some state of art methods for watermark recovery process are briefly reviewed in [3]. They fall into two broad classes: Correlation-based recovery and Data-model-based optimum recovery.

2.3.1 Correlation-based Recovery

Although correlation-based recovery is the most common solution in the watermark detection problem, it does not lead to optimum performance, unless the embedding rule is additive and the host features are normally distributed [3]. The correlator is not optimal for non-Gaussian data, especially those of a more impulsive nature, as high-magnitude data values cause its performance to deteriorate significantly [24]. The correlation detectors are optimal only in the case of data that follow the Gaussian statistics. But, the important coefficients of an image, which correspond to the low and mid frequencies, do not follow a Gaussian distribution [12]. Following such a consideration, some optimum recovery schemes have been proposed in the last couple of years, leading to a considerable improvement of performance. Nevertheless, motivations exist that make correlation-based recovery worth attention.

First, correlation-based recovery is usually much simpler in implementation than optimum recovery [21], [18], and it is sometimes preferred when fast decoding is a crucial requirement. In addition, correlation decoding makes it feasible the

exhaustive search of the watermark in presence of some kinds of geometrical distortions. Let us consider, for example, the case of a watermark embedded in the spatial domain, and let us suppose that the image has been shifted. To recover the watermark one should consider all possible horizontal and vertical shifts, which is a very time-consuming procedure. By noting that such a process corresponds to the correlation between the host image and the watermark, a faster algorithm is obtained by operating in the frequency domain, where correlation corresponds to coefficient wise multiplication.

Another reason not to abandon correlation-based recovery, is that the structure of optimum decoders is usually derived under a set of assumptions that only rarely are satisfied, e.g. absence of attacks and exact knowledge of the pdf of host features. It is necessary, then, that the real effectiveness of optimum techniques be tested experimentally. As in this thesis, the primary concern is watermark detection, not extraction, it focuses on the detection only in this section.

In general, watermark detection is a typical binary hypothesis testing problem. Given an observation variable r, a decision rule is defined to decide whether the watermark is present (hypothesis H_1) or not (hypothesis H_0). In correlation-based detection the observation variable is the correlation ρ between the watermark and the host features:

$$\rho = \frac{1}{n}\sum_{i=1}^{n} m_i y_i \tag{2.3}$$

To decide whether the watermark is present or not, ρ is compared to a threshold T_ρ. Several approaches exist to set T_ρ. A possibility consists in choosing T_ρ in such a way that the probability of error P_e is minimised, under the assumption that ρ follows a Gaussian pdf.

A drawback with the choice of T_ρ is that it does not take into account possible attacks, whose main effect is to lower ρ, thus increasing the probability of missing the watermark (P_M). On the contrary, the false alarm probability (P_F) is not affected by attacks.

A solution leading to a considerable improvement in term of robustness consists in minimising P_M subject to a fixed false detection rate, i.e. to use as low a threshold as possible constrained to a maximum P_F (Neyman-Pearson criterion) [25].

Another advantage of choosing T_ρ according to the Neyman-Pearson criterion is that in this way the decoder does not need to know the watermark strength, only the statistics conditioned to hypothesis H_0 are needed, which can be estimated directly on the image under analysis, without any knowledge about the watermark energy [22], [25], [26].

2.3.2 Data-model-based Optimum Recovery

Driven by the need to improve the reliability of watermark recovery, some optimum algorithms have been proposed recently [10], [27], [11], [28], [29]. The benefits achievable through optimum decoding are more evident in cases where the deviation form the AWGN assumption is stronger, e.g. when the embedding rule is not additive and the host features are not Gaussian [28]. Though recovery algorithm comprises both detection and extraction of watermark, due to the same reason as stated before, here only the optimum detection is reviewed.

Optimum detection techniques may differ from one to another depending upon a number of factors such as the embedding rule, the pdf of host features, and the optimality criterion. Here also, we need to look for a criterion that permits to distinguish between H_0 and H_1. In [28], De Rosa et al. derive the optimum decoder for a multiplicative/additive watermark embedded in the magnitude of DFT coefficients according to the rule

$$y_i = x_i + \gamma m_i x_i \tag{2.4}$$

where, the watermark m_i is uniformly distributed in [-1,1]. Two major deviations from the AWGN assumptions are present here: the watermark is not additive, and the pdf of host features is not Gaussian.

In [28], the authors assume that the magnitude of DFT coefficients is characterized by a Weibull distribution. By following Bayes theory of detection, it first demonstrated that the likelihood ratio,

$$l(\mathrm{y}) = \frac{f(\mathrm{y}|H_1)}{f(\mathrm{y}|H_0)} \tag{2.5}$$

is the optimum decision function, in that it permits to minimize the Bayes risk associated to the decision.

A drawback with the optimum detection strategy proposed by De Rosa et al. is that the watermark strength γ must be known in advance. This forces the

encoder to always use the same γ, thus preventing the possibility of adapting it to the image at hand.

Hernandez in [10] proposed the design of a statistical watermark detector that models the DCT coefficients by the commonly used Generalized Gaussian (GG) distribution [1], [34]. Here, optimum detection is applied to an additive watermark embedded in the block-DCT domain. The Bayes detection theory is applied here to obtain the optimum decision rule. The resulting detector structure based on this model led to considerable improvements when compared to the correlation receiver. The reason behind the improvement obtained by modeling DCT coefficients through the generalized Gaussian instead of the standard Gaussian pdf (which would lead to correlation detection)is the fact that, the generalized Gaussian distribution provides a better model for the low and mid-frequency DCT coefficients [10], [12], [30], as its tails decay at a slower rate.

The blind watermark detector proposed by Briassouli *et. al.* in [1], is specially designed for α-stable pdf. Actually, the detector in [1] is based on Cauchy distribution which is a closed form expression of the symmetric α-stable (SαS) family of distributions. Cauchy-based detectors and estimators were shown to be particularly robust in heavy-tailed environments even under signal mismatch, in contrary to traditional detectors [15], [16]. The likelihood ratio is used here as the decision function.

Although the α-stable pdf, proposed in [1], proves to be more appropriate model for the DCT coefficients than the others (Laplacian, generalized Gaussian), it does not have a closed-form expression, making the parameter estimation complicated especially from noisy data [17]. In fact, in [1], the authors use the Cauchy PDF, a special case of the α-stable PDF in developing the watermarking system. Obviously, a more desirable approach would be to employ a generalized PDF with a closed-form expression in developing an image processing system.

In [31], Laplacian model has been used for watermark detection for image in DWT domain. Here, the detection is performed by maximum-likelihood algorithm whereby the decision threshold is obtained using the Neyman-Pearson criterion. The Laplacian model exhibits better performance than that of the Gaussian-based detector.

Though not used particularly for watermark detection, some other data mod-

els have been used in literature for different purposes related to watermarking system, such as, denoising the attack on image watermarking. In [32], Bessel K Form prior is used for the development of a maximum a posterior (MAP) Bayesian denoiser in wavelet-domain, which resulted in improved visual quality of the attacked image and a better PSNR.

An approach proposed by Oostveen et al. [29] does not use the likelihood ratio as decision function. Given the additive/multiplicative embedding rule in (2.2), and under the assumption that the watermark is a known, binary valued sequence, an ML estimation of the watermark strength γ is performed. The estimate is compared to a threshold computed according to the Neyman-Pearson optimality criterion. However, this approach leads to sub-optimum detection.

2.4 Conclusion

This chapter provides an overview of different watermark detection schemes, and different evaluation criteria used for designing these detectors. First, watermark embedding rule is overviewed. Of different watermark recovery schemes, data model based detection techniques generally performs better than correlation based detector. Several data model based detectors are reviewed and their scopes and limitations are investigated.

Chapter 3

Development of SNIG-based Watermark Detector

3.1 Introduction

Due to huge application in information security and data encryption, watermarking has been the benchmark protective technique used in images over last decade. As presented in Chapter 2, data model based detector performs better than correlation based detectors for blind image processing system. This chapter presents a robust SNIG based blind watermark detector for still images. From the state of art data models it has been observed that, SNIG model provides fairly satisfying goodness of fit for most images. Before the employment of SNIG prior for detection, the estimation of the SNIG parameters by minimizing the Kullback-Leibler (KL) divergence are achieved [17].

In this chapter, at first image data modeling using different priors is presented. This is done with an aim to verify the superiority of SNIG prior to other ones in image data modeling. After that, an embedding process of DCT-based image watermarking is provided. The detector using SNIG prior is developed in the later section. Last of all, an analysis of the performance of the proposed watermark detector in terms of the associated probabilities of detection and false alarm are presented and then the performance of the proposed scheme is compared with that of other state of art watermark detectors.

3.2 DCT-domain Image Data Models For Optimum Detection

In order to verify the existence of a watermark using a optimum recovery scheme, based on the statistical properties of the given data, one must design a binary hypothesis test where the two hypotheses concern the existence or not of a known signal iu a given image. Obviously, such a structure will lead to reliable detection results if the data, i.e., the low and mid frequency DCT coefficients, are modeled as accurately as possible [1]. It is well known from the relevant literature that the low and mid-frequency image DCT coefficients, which carry most of the image informatiou, are not adequately modeled by the Gaussian distribution [12], [33], [34]. The pdfs of these coefficients bear a similarity to the Gaussian model as they remain bell-shaped, but their tails are significantly heavier [30].

A number of pdfs have been proposed in the literature for modeling the DCT coefficients that include the Laplacian, generalized Gaussian (GG), alpha-stable and generalized gamma pdfs [1], [30], [34], [35], [36]. In this section, an overview of some models used in literature for DCT-domain image data is provided. For modeling of the DCT coefficients of digital images, each image can be considered as a 2-D sequence. The DCT of a 2-D data $F(x, y)$ of size $N \times N$ is given by

$$G(u,v) = B_u B_v \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] \tag{3.1}$$

where, B_u is $\sqrt{1/N}$ and $\sqrt{2/N}$, for $u = 0$ and $u > 0$, respectively. Similar couditions hold for B_v. In this thesis, both full frame and blocks of size 8×8 are used. The block-DCT coefficients with index (u, v) are denoted as $C_{u,v}$.

3.2.1 Laplacian Modeling of DCT Coefficients

The Laplacian pdf is giveu by

$$f_X(x) = \frac{\beta}{2} exp(-\beta|x-\mu|) \tag{3.2}$$

where, $\mu = \text{mean}(x)$, $\beta^2 = 2/\text{var}(x)$. The drawback of the Laplacian PDF is its inability to capture the tail information. As shown in [13], the Laplacian distribution is inadequate for the heavier tailed samples, because its tails decay at a fast exponential rate [1].

3.2.2 Generalized Gaussian Modeling of DCT Coefficients

In [34], a generalized Gaussian (GG) pdf is shown to be a better model than the Laplacian one. The generalized Gaussian distribution, characterized by the parameter c and the standard deviation of the data σ, has the following PDF:

$$f_X(x) = Aexp(-\beta|x-\mu|^c) \tag{3.3}$$

The parameters A and β can be expressed in terms of c and σ respectively as the following:

$$\beta = \frac{1}{\sigma}(\frac{\Gamma(\frac{3}{c})}{\Gamma(\frac{1}{c})})(1/2), \tag{3.4}$$

$$A = \frac{\beta c}{2\Gamma(\frac{1}{c})}. \tag{3.5}$$

Coefficients at high frequencies are better approximated by a Gaussian distribution and sometimes by a Laplacian distribution [31]. Note that the Gaussian and Laplacian pdfs are two special cases of the GG pdf. The suitability of the GG pdf in modeling the DCT coefficients is further illustrated in [35] through a detailed mathematical analysis.

3.2.3 Alpha-stable Modeling of DCT Coefficients

In [1], a symmetric alpha stable (SαS) family of distributions is proposed for the modeling of the heavy-tailed DCT coefficients. It reports alpha stable model has been successful in modeling heavy-tailed data in various applications [37], such as underwater acoustic signals, clutter returns in radar, financial data, internet traffic, as well as transform domain image or audio signals [38], [14].

The SαS distribution can be best described by its characteristic function,

$$\varphi(\omega) = exp(j\delta\omega - \gamma\omega^\alpha) \tag{3.6}$$

which is parameterized by the location parameter δ, the scale parameter γ, known as the dispersion, and the characteristic exponent α.

Closed-form expressions exist for the pdf of random variables only for $\alpha = 2$ and $\alpha = 1$, which correspond to the Gaussian and Cauchy distributions, respectively. The density function of the Cauchy distribution is given in closed form by

the expression;

$$f_X(x) = \frac{1}{\pi}\frac{\gamma}{\gamma^2 + (x-\delta)^2} \tag{3.7}$$

where, γ is the data dispersion and δ is the location parameter.

3.2.4 Symmetric Normal Inverse Gaussian (SNIG) Modeling of DCT Coefficients

In [17], another model using the SNIG pdf is proposed as a highly suitable prior for modeling the DCT coefficients of natural images. The SNIG pdf is expressed as,

$$P_X(x) = \frac{A(\delta,\alpha)K_1(\alpha\sqrt{\delta^2+x^2})}{\sqrt{\delta^2+x^2}} \tag{3.8}$$

where,

$$K_\lambda(\xi) = \frac{1}{2}\int_0^\infty z^{\lambda-1}exp(-\frac{1}{2}\xi(z+z^{-1}))dz \tag{3.9}$$

and

$$A(\delta,\alpha) = \frac{\delta\alpha}{\pi}exp(\delta\alpha) \tag{3.10}$$

$K_\lambda(\xi)$ is the modified Bessel function of order λ. The α parameter controls the steepness of the distribution in that the larger the values of α, the higher the peak of the pdf. The increase in the value of α has also implications for the tails, since with a sharper peak, the tails would become lighter. The other parameter, δ, defines the scale of the pdf and is similar to the variance parameter of a Gaussian pdf. Fig. 3.1 shows the variation in the shape of the SNIG distribution for various values of α.

In order to employ the SNIG pdf for modeling, it is essential that the SNIG parameters are estimated from the data being modeled. In this paper, a technique, based on minimizing the KL (Kullback-Leibler) divergence between the SNIG pdf and the empirical pdf corresponding to the data, is introduced to estimate the SNIG parameters. The KL divergence, also known as the relative entropy, is given by

$$KL(P_{emp}, P) = \int P_{emp}(x)\log_2\left(\frac{P_{emp}(x)}{P(x)}\right)dx \tag{3.11}$$

where, P and P_{emp} represent the SNIG and empirical pdfs, respectively [39].

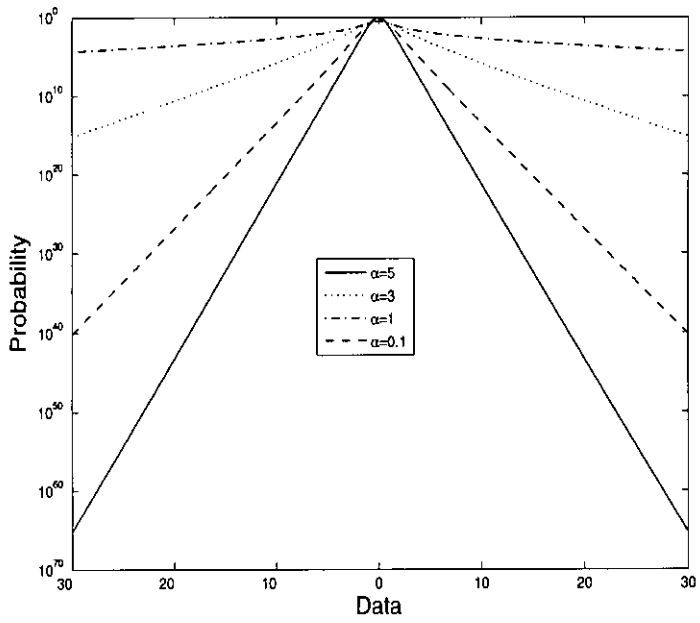


Fig. 3.1: The effect of changing α on the shape of the SNIG pdf. The value of δ is set to 1. The vertical axis is log-normalized.

SNIG Parameter Estimation

The parameters of the SNIG pdf are estimated from the DCT coefficients by minimizing the KL divergence between the SNIG pdf and the empirical PDF corresponding to the data. The KL divergence, also known as the relative entropy, is given by

$$KL(P_{emp}, P) = \int P_{emp}(x) \log_2 \frac{P_{emp}(x)}{P(x)} dx \tag{3.12}$$

where, P and P_{emp} represent the SNIG and empirical pdfs, respectively [39]. Minimizing the KL divergence is equivalent to maximizing the log-likelihood, since the latter is a negative of the sum of the KL divergence and the data entropy [39], and thus can be expected to provide unbiased estimation of the parameters asymptotically. The parameters of the SNIG pdf are obtained as

$$\widehat{\alpha}, \widehat{\delta} = \arg\min_{\widehat{\alpha},\widehat{\delta}} \sum_{i=1}^{N_h} P_{emp}(x_i) \log_2 \frac{P_{emp}(x_i)}{P(x_i)} \tag{3.13}$$

where, x_i denotes the center values of the bins of a N_h-point histogram corresponding to the data, the minimization being carried out using the Nelder-Mead direct search technique.

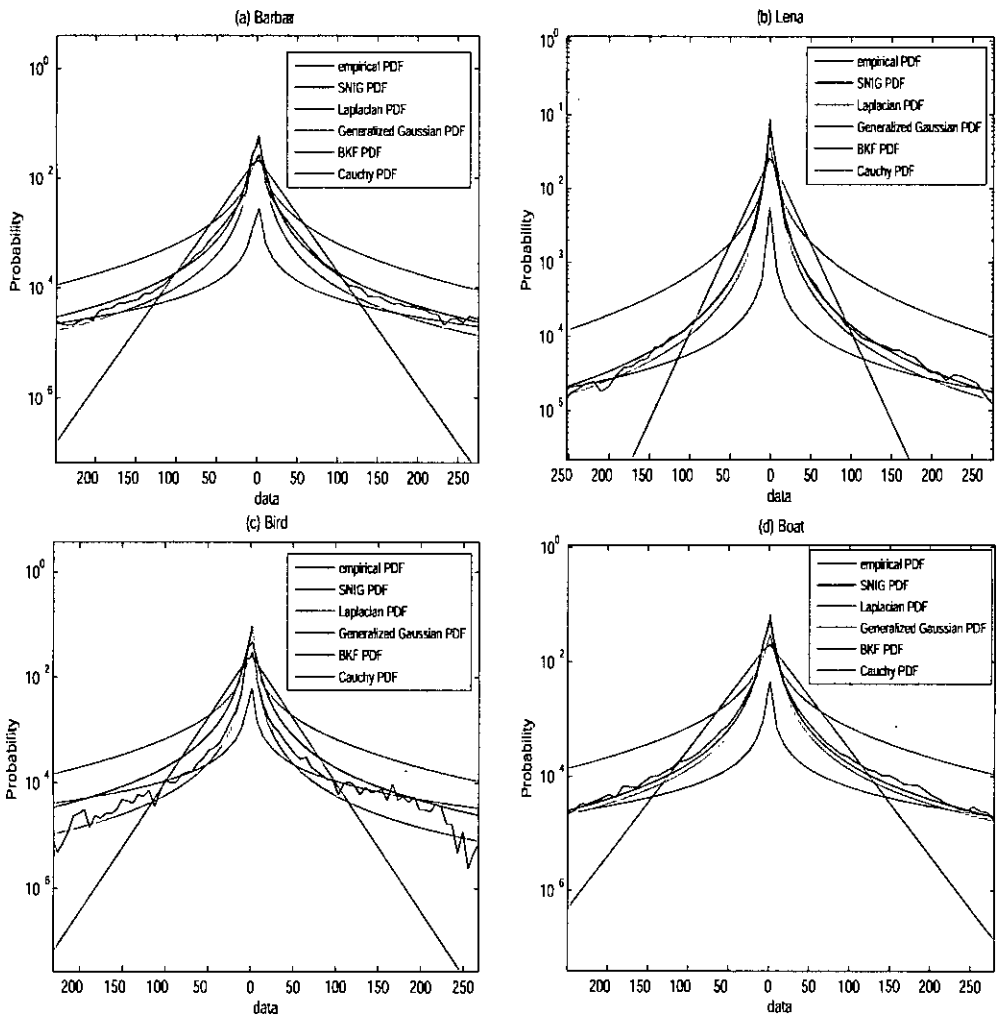


Fig. 3.2: Plot of the empirical, SNIG, GG, Cauchy, Laplacian and BKF pdfs corresponding to full-frame DCT coefficients.

The SNIG pdf, proposed in [17], shows better characterization of the DCT coefficients of some natural image data, when compared to Laplacian, Bessel-K form (BKF), generalized Gaussian (GG), and alpha-stable (Cauchy) models. This is demonstrated in Fig. 3.2.

From the amplitude probability distribution (APD) curves (Fig. 3.2), it has been shown that the SNIG pdf is a better model in comparison to the GG, α-stable and Laplacian pdfs for modeling the full-frame DCT coefficients of natural images. As for modeling the block-DCT coefficients, the SNIG pdf has been shown to be more effective than the GG, BKF and Laplacian pdfs, and as good as the α-stable pdf, while incurring much less computational cost for parameter

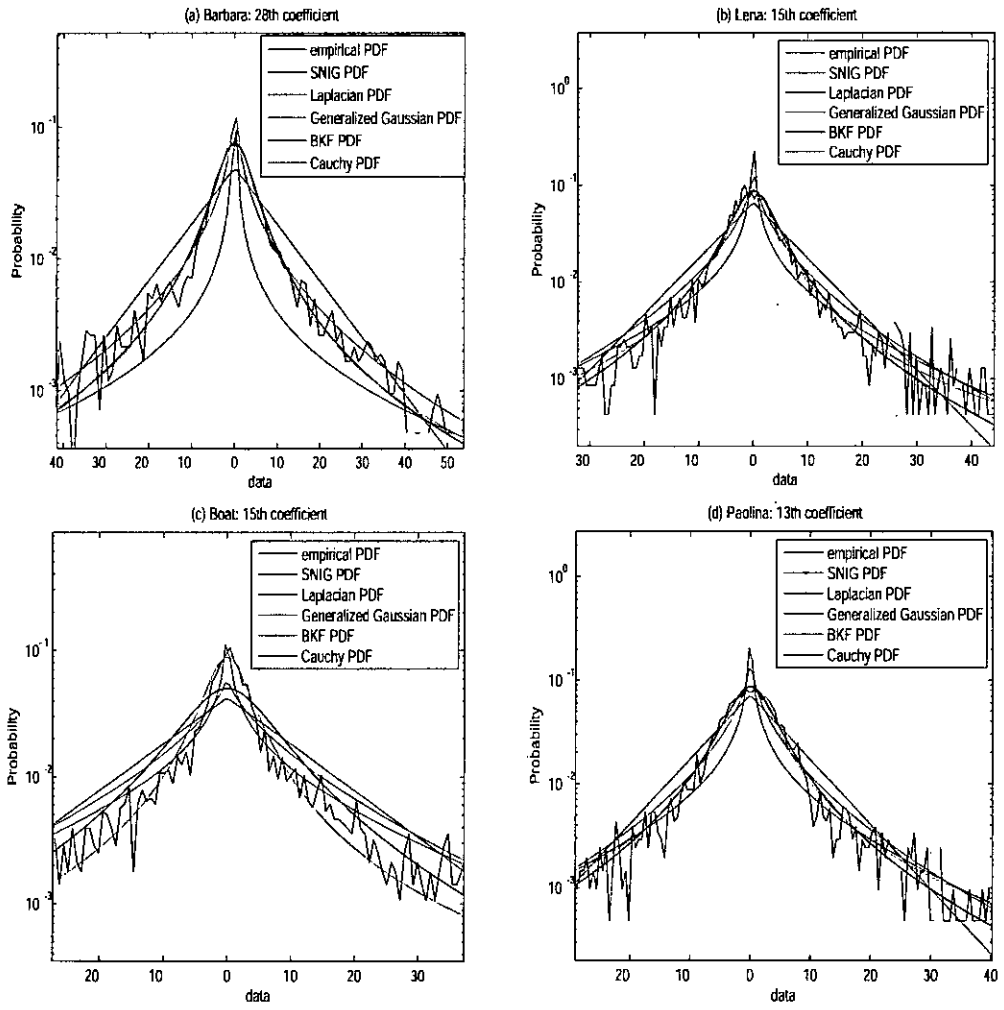


Fig. 3.3: Plot of the empirical, SNIG, GG, Cauchy, Laplacian and BKF pdfs corresponding to DCT coefficients of 8×8 blocks.

estimation.

As SNIG pdf fits as a better model for DCT coefficients of digital images, it bears lots of promises to yield a better optimal detector. In this thesis work, SNIG modeling for DCT coeeficients is used to develop the watermark detector. The performance of the SNIG-based detector and its comparison with other detectors is elaborately demonstrated in the following sections.

3.3 Watermark Generation for Still Images

In this section, a brief description of spread spectrum (SS) watermarking in the DCT domain for still images similar to one in [10] is presented. Many watermarking systems are based on additive spread spectrum (SS) ideas [40], [41], which are inspired by the spread spectrum modulation schemes used in digital communications in jamming environments [18], [42]. The role of the jammer in the watermarking problem is assumed by the cover signal (additive noise) and by an attacker who may try to destroy or extract the embedded watermark [43], while the watermark is the hidden information signal [1]. An advantage of SS techniques which has made them attractive for information hiding is the ability to reliably transmit signals at low power, which results in a low probability of intercept (LPI) [44], [33]. During watermark embedding, we have considered the properties of the human visual system (HVS) to ensure imperceptibility of the hidden signal.

3.3.1 Watermark Embedding

Fig. 3.4 shows general DCT based model for watermark embedding. An image in the spatial domain with $N_1 \times N_2$ pixels is represented here as a discrete 2-D sequence $x[\mathbf{n}]$ and its DCT transform as $X[\mathbf{k}]$, where the indices in boldface typesetting is used to represent the corresponding two-dimensional (2-D) indices, i.e., $\mathbf{n} = [n1, n2]$ for the spatial domain and $\mathbf{k} = [k1, k2]$ for the DCT domain. The watermark can be considered as a 2-D DCT signal $W[\mathbf{k}]$, which is added to the DCT coefficients giving the watermarked image $Y[\mathbf{k}]$.

The discrete cosine transform can be applied either to the entire image or in blocks as in the JPEG standard [45], [46]. Block-wise DCT is faster in application than the full-image DCT. Specifically, the application of the DCT in 8×8 blocks

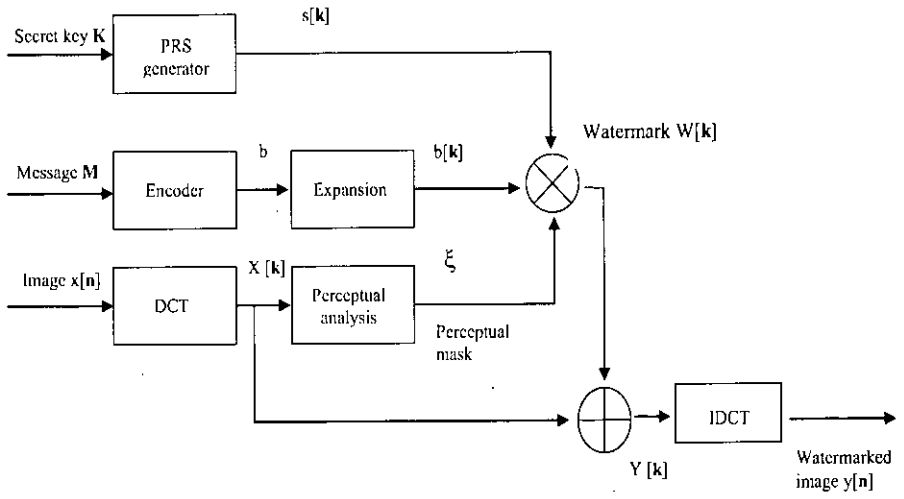


Fig. 3.4: Block diagram for DCT-based watermark embedding

of the image leads to 64 DCT coefficients which can be zigzag scanned and thus arranged in order of decreasing importance. The first coefficients are of the main interest as they correspond to the low and mid frequencies that carry the most information about the image. By applying the blockwise DCT, these coefficients can be extracted from each block and then their statistical distribntion can be estimated, which is essential in the design of the detection system [1]. In this thesis, simulated results for both full frame image and blockwise DCT application are incorporated.

The hidden message M can be mapped by an encoder to a N-dimensional codeword vector b. It results in an expansion process during which every element of the codeword vector b_i is repeated in a different set S_i of DCT coefficients, covering the entire image. This repetition introduces a certain degree of redundancy in the watermark, which increases its robustness. As this thesis concerns with watermark detection, there is no hidden message M, so for this case, $b[\mathbf{k}] = b = 1$.

In order to generate a direct SS modulated watermark, the signal ($b = 1$) resulting from the above expansion process is multiplied with an appropriate 2-D pseudorandom sequence (PRS) $s[\mathbf{k}]$, which depends on a secret key K. This key corresponds to the legal owner of the watermarked document and without it the generation of the watermark at the receiver is impossible. In order to

increase the robustness, the PRS should have a white-noise like properties. It takes values (+1,-1), whose mean is zero and the autocorrelation approximately equal to Kronecker delta function.

In order that the watermark signal can have maximum strength (for providing a robust system) at the same time ensuring the invisibility of the alteration introduced to the image, the spread signal is multiplied by a visual mask which takes into account the properties of the human visual system (HVS). In this work, ξ has been used as the visual mask to obtain the watermark signal as $W[\mathbf{k}] = \xi s[\mathbf{k}]$.

Following the method depicted in [47], the parameter ξ has been selected in such a way that each coefficient has the same level of watermark-to-document ratio (WDR) defined as,

$$WDR = 10\log\left(\frac{\sigma_W^2}{\sigma_X^2}\right) = 10\log\left(\frac{\xi^2}{\sigma_X^2}\right) \tag{3.14}$$

where, σ_W^2 is the variance of the embedded watermark. Last of all, the resulting watermark $W[\mathbf{k}]$ is added to the original DCT coefficients $X[\mathbf{k}]$, giving the watermarked signal $Y[\mathbf{k}] = X[\mathbf{k}] + W[\mathbf{k}]$. The watermark can be retrieved only if one uses a copy of the pseudorandom sequence s[k] that can be reproduced only if one knows the entire procedure through which it is generated and the cryptographic key that was used as its seed. As a result, an attacker will not be able to extract the watermark without knowledge of the secret key, even if the entire watermark generation and embedding procedure is known.

A number of test images have been used in this thesis to embed with watermark of different strengths. Lower values of WDR corresponds to weaker and more invisible watermark.

This thesis does not take into account of any geometric attacks. Although this watermark has not been specifically designed to resist geometric attacks, the high degree of redundancy, that it has achieved through the spreading of information over the entire image, enhances its chances of survival from such attacks.

3.4 Watermark Detection

3.4.1 Detection Based on Hypothesis Testing

Watermark detection are often looked at as a communications problem related to the reliable transmission and detection of a weak signal through a noisy channel

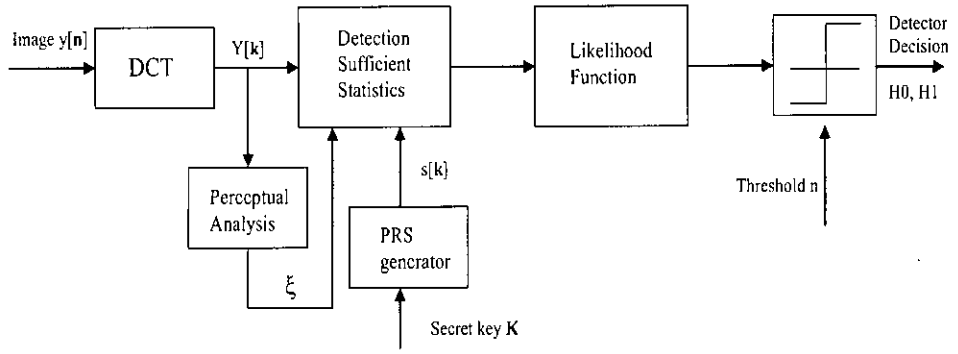


Fig. 3.5: Block diagram of DCT-based watermark detection

[10], [18], where the signal and the noise, in our case, are represented by the watermark and the host data, respectively. Fig. 3.5 shows the block diagram of DCT based watermark detection scheme used in this thesis. Thus, the watermark detection problem, i.e, the verification of the existence of $W[\mathbf{k}]$ in the given signal $Y[\mathbf{k}]$ can be formulated as a binary hypothesis test where the two hypotheses concern the existence of a watermark. This technique is blind since the detection is performed without knowledge of the original, unwatermarked data $X[\mathbf{k}]$. The two hypotheses for the test can be written as follows:

$$H_0 : Y[\mathbf{k}] = X[\mathbf{k}] \tag{3.15}$$

$$H_1 : Y[\mathbf{k}] = X[\mathbf{k}] + W[\mathbf{k}] \tag{3.16}$$

An optimal watermark detector aims at finding whether or not there is a watermark in the received image $Y[\mathbf{k}]$, based on the statistical properties of the image $X[\mathbf{k}]$ and its watermark $W[\mathbf{k}]$. Generally, it is assumed that the pdf of the original coefficients does not change with the embedding of the watermark [1], because, the watermarked image coefficients should have a distribution similar to that of the host in order to keep perceptual similarity with it.

The pdfs of the image and its watermark can be accurately approximated from the given data, if the data has been modeled by an appropriate statistical distribution. The watermark detector bases its decision on a ratio test, that can be formulated as follows:

$$\Lambda(Y) \gtrless_{H_0}^{H_1} \eta' \tag{3.17}$$

Here, the likelihood ratio $\Lambda(Y)$ and the threshold η' are defined as [47],

$$\Lambda(Y) = \frac{f(Y|H_1)}{f(Y|H_0)} \tag{3.18}$$

and

$$\eta' = \frac{C_{fa}Pr(H_0)}{C_m Pr(H_1)} \tag{3.19}$$

where C_{fa} and C_m are the costs of false alarm and missdetection, respectively, and $Pr(H_0)$ and $Pr(H_1)$ are the probabilities of null and alternative hypotheses, respectively.

In practice, the log-likelihood ratio is usually preferred to perform hypothesis testing using N DCT coefficients which can be treated as independent and identically distributed (i.i.d.) random variables, since the DCT approximates the Karhunen-Love (KL) transform [24]. The Bayesian log-likelihood ratio is simply defined as the natural logarithm of the likelihood ratio, $l(Y) = \ln(\Lambda(Y))$, so the decision rule can be rewritten as,

$$\begin{aligned} l(Y) &= \ln\left(\frac{f(Y|H_1)}{f(Y|H_0)}\right) && (3.20)\\ &= \ln\left(\frac{\prod_k f(Y[\mathbf{k}]|H_1)}{\prod_k f(Y[\mathbf{k}]|H_0)}\right) \\ &= \sum_k \ln\left(\frac{f(Y[\mathbf{k}]|H_1)}{f(Y[\mathbf{k}]|H_0)}\right) \\ &= \sum_k \ln\left(\frac{f_X(Y[\mathbf{k}]-W[\mathbf{k}])}{f_X(Y[\mathbf{k}])}\right) \gtrless_{H_0}^{H_1} \eta. && (3.21) \end{aligned}$$

The threshold η can be determined by the Neyman Pearson (NP) criterion, which minimizes the probability of missing a watermark for a bounded false alarm probability P_{fa}. The resulting test guarantees that the power of the test, i.e., the probability of detection, will be maximized for a predetermined false alarm [24], [33].

3.4.2 The Proposed SNIG Watermark Detector

It is evident from the previous section that, a statistical watermark detector based on binary hypothesis test can result in authentic detection only if the DCT coefficients of the image data are modeled accurately. The greater the accuracy of the pdf of the image data incorporated in the detector, the higher the reliability of detection of the watermark at a predefined false alarm rate.

Being inspired by the performance of SNIG pdf in modeling data, a blind watermark detector using this pdf is devised in this section. As mentioned in the previous section, the SNIG pdf is expressed as,

$$f_X(x) = \frac{A(\delta,\alpha)K_1(\alpha\sqrt{\delta^2+x^2})}{\sqrt{\delta^2+x^2}} \tag{3.22}$$

where,

$$K_\lambda(\xi) = \frac{1}{2}\int_0^\infty z^{\lambda-1}\exp(-\frac{1}{2}\xi(z+z^{-1}))dz$$

and

$$A(\delta,\alpha) = \frac{\delta\alpha}{\pi}\exp(\delta\alpha)$$

Here, α the steepness controlling parameter, and δ scaling parameter of the pdf.

Therefore, for the SNIG watermark detector, the log-likelihood ratio given in (3.20) can be expressed as,

$$\begin{aligned} l(Y) &= \sum_k \ln\left(\frac{\frac{K_1(\alpha\sqrt{\delta^2+(Y-W)^2})}{\sqrt{\delta^2+(Y-W)^2}}}{\frac{K_1(\alpha\sqrt{\delta^2+Y^2})}{\sqrt{\delta^2+Y^2}}}\right) \\ &= \sum_k \left(\ln\frac{K_1(\alpha\sqrt{\delta^2+(Y-W)^2})}{\sqrt{\delta^2+(Y-W)^2}} - \ln\frac{K_1(\alpha\sqrt{\delta^2+Y^2})}{\sqrt{\delta^2+Y^2}}\right) \end{aligned} \tag{3.23}$$

3.4.3 Performance Analysis of SNIG Watermark Detector

The performance of the conventional gaussian correlator can be measured in terms of the detection and error probabilities, both for the maximum likelihood (ML) and the Neyman-Pearson (NP) detectors [33]. The goal of an ML detector is to maximize the detection probability by minimizing the error probability. The error probability incorporates both the probabilities of missdetection and false alarm by the following relation,

$$\begin{aligned} P_{err} &= P_{miss}Pr(H_1) + P_{fa}Pr(H_0) \\ &= \frac{1}{2}P_{miss} + \frac{1}{2}P_{fa} \end{aligned} \tag{3.24}$$

As in (3.24) it is generally held that, missdetection and false alarm are equiprobable, i.e., $Pr(H_0) = Pr(H_1) = 1/2$.

This model has adopted the N-P criterion for the detection of watermark, where the detection probability is maximized for a given false alarm probability. Now, it is possible to analyze the performance of the detector from the receiver operating characteristic (ROC) curves which plots $P_{det} vs. P_{fa}$. Simulation results are included for different levels of watermark strength (WDR).

Evaluation of ROC requires estimation of the mean and the variance of the log-likelihood ratio under H_0 and H_1 conditions. Let us denote the mean and the variance under hypothesis H_0 as m_0 and σ_0^2 respectively, and the same under hypothesis H_1 as m_1 and σ_1^2 respectively.

The pseudorandom sequence (PRS) $s[\mathbf{k}]$ that we have considered in our design can take the values (+1,-1) equiprobably, so the watermark added to the image coefficients can either be $+\xi$ or $-\xi$ having a equal probability of 1/2. Therefore, using (3.23) the mean of $l(Y)$ under H_0 condition can be written as,

$$\begin{aligned}
m_0 &= E_W[l(Y)|H_0] \\
&= \frac{1}{2}\sum_k [\ln f_X(X[\mathbf{k}]-\xi) - \ln f_X(X[\mathbf{k}])] + \frac{1}{2}\sum_k [\ln f_X(X[\mathbf{k}]+\xi) - \ln f_X(X[\mathbf{k}])] \\
&= \frac{1}{2}\sum_k [\ln f_X(X[\mathbf{k}]-\xi) + \ln f_X(X[\mathbf{k}]+\xi)] - \sum_k \ln f_X(X[\mathbf{k}]) \\
&= \frac{1}{2}\sum_k \left[\ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2}} + \ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]+\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]+\xi)^2}}\right] \\
&- \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+X^2[\mathbf{k}]})}{\sqrt{\delta^2+X^2[\mathbf{k}]}}
\end{aligned} \tag{3.25}$$

Here, $E_W[.]$ is the expectation operator on $W[\mathbf{k}]$. The variance of $l(Y)$ under H_0 condition can be obtained as,

$$\sigma_0^2 = E_W[l(Y)|H_0]^2 - m_0^2 \tag{3.26}$$

Here,

$$
\begin{aligned}
E_W[l(Y)|H_0]^2 &= \frac{1}{2}\left[\sum_k \ln f_X(X[\mathbf{k}]-\xi) - \sum_k \ln f_X(X[\mathbf{k}])\right]^2 \\
&+ \frac{1}{2}\left[\sum_k \ln f_X(X[\mathbf{k}]+\xi) - \sum_k \ln f_X(X[\mathbf{k}])\right]^2 \\
&= \frac{1}{2}\left[\sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2}} - \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+X^2[\mathbf{k}]})}{\sqrt{\delta^2+X^2[\mathbf{k}]}}\right]^2 \\
&+ \frac{1}{2}\left[\sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]+\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]+\xi)^2}} - \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+X^2[\mathbf{k}]})}{\sqrt{\delta^2+X^2[\mathbf{k}]}}\right]^2
\end{aligned}
\tag{3.27}
$$

So, from (3.26) and (3.27), it follows that,

$$
\begin{aligned}
\sigma_0^2 &= \frac{1}{2}\left[\sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2}} - \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+X^2[\mathbf{k}]})}{\sqrt{\delta^2+X^2[\mathbf{k}]}}\right]^2 \\
&+ \frac{1}{2}\left[\sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]+\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]+\xi)^2}} - \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+X^2[\mathbf{k}]})}{\sqrt{\delta^2+X^2[\mathbf{k}]}}\right]^2 - m_0^2
\end{aligned}
\tag{3.28}
$$

After replacing the expression of m_0 from (3.25), and a little calculation, finally it can be written that,

$$
\sigma_0^2 = \frac{1}{4}\left[\sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2}} - \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]+\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2}}\right]^2 \tag{3.29}
$$

In the similar way, the mean of the log-likelihood function, $l(Y)$, under H_1 condition can be obtained as,

$$
\begin{aligned}
m_1 &= E_W[l(Y)|H_1] \\
&= \frac{1}{2}\sum_k [\ln f_X(X[\mathbf{k}]) - \ln f_X(X[\mathbf{k}]+\xi)] + \frac{1}{2}\sum_k [\ln f_X(X[\mathbf{k}]) - \ln f_X(X[\mathbf{k}]-\xi)] \\
&= \frac{1}{2}\sum_k \left[-\ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]-\xi)^2}} - \ln \frac{K_1(\alpha\sqrt{\delta^2+(X[\mathbf{k}]+\xi)^2})}{\sqrt{\delta^2+(X[\mathbf{k}]+\xi)^2}}\right] \\
&+ \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2+X^2[\mathbf{k}]})}{\sqrt{\delta^2+X^2[\mathbf{k}]}} \\
&= -m_0,
\end{aligned}
\tag{3.30}
$$

and

$$\begin{aligned}
\sigma_1^2 &= E_W[l(Y)|H_1]^2 - m_1^2 \\
&= \frac{1}{2}\left[\sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2 + X^2[\mathbf{k}]})}{\sqrt{\delta^2 + X^2[\mathbf{k}]}} - \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2 + (X[\mathbf{k}] + \xi)^2})}{\sqrt{\delta^2 + (X[\mathbf{k}] + \xi)^2}}\right]^2 \\
&+ \frac{1}{2}\left[\sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2 + X^2[\mathbf{k}]})}{\sqrt{\delta^2 + X^2[\mathbf{k}]}} - \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2 + (X[\mathbf{k}] - \xi)^2})}{\sqrt{\delta^2 + (X[\mathbf{k}] - \xi)^2}}\right]^2 - m_1^2 \\
&= \frac{1}{4}\left[\sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2 + (X[\mathbf{k}] - \xi)^2})}{\sqrt{\delta^2 + (X[\mathbf{k}] - \xi)^2}} - \sum_k \ln \frac{K_1(\alpha\sqrt{\delta^2 + (X[\mathbf{k}] + \xi)^2})}{\sqrt{\delta^2 + (X[\mathbf{k}] - \xi)^2}}\right]^2 \\
&= \sigma_0^2
\end{aligned} \tag{3.31}$$

As long as blind watermark detection is concerned, one can consider the two occurrences, H_0 and H_1, equally probable, i.e., $Pr(H_0) = Pr(H_1)$. In that case, from the estimated values of the mean and variance of the conditional $l(Y)$, the probabilities of false alarm and detection can be calculated as,

$$\begin{aligned}
P_{fa} &= Q\left(\frac{\eta - m_0}{\sigma_0}\right), \\
P_{det} &= Q\left(\frac{\eta - m_1}{\sigma_1}\right)
\end{aligned} \tag{3.32}$$

where, $Q(u) = \frac{1}{2}erfc(u/\sqrt{2})$. For a predetermined P_{fa}, the threshold for the detector output decision can be calculated as,

$$\eta = m_0 + \sigma_0 Q^{-1}(P_{fa}) \tag{3.33}$$

and the corresponding detection probability as,

$$P_{det} = Q\left(Q^{-1}(P_{fa}) - \frac{m_1 - m_0}{\sigma_1}\right) \tag{3.34}$$

By predefining this threshold, one can find the relation between P_{fa} and P_{det}, which leads to the receiver operating characteristic (ROC). For a certain value of P_{fa}, the higher the value of P_{det}, the better is the performance of the watermark detector.

For a blind watermark detector, the mean and the variance of the conditional log-likelihood function are estimated from the received image. From (3.25)-(3.31) one can see that, the mean and the variance of $l(Y)$ on both the conditions (H_0 and H_1) depend on parameters of the SNIG pdf, namely, α and δ. Since, in case

of blind detection, while estimating the parameters we have no idea whether the received image contains a watermark or not, it is necessary that the watermark embedding does not change these parameters significantly [47].

During data modeling and watermark embedding, it requires to determine the values of the SNIG pdf parameters, α and δ, for both the marked and unmarked images. These values have been for a number of 512×512 and some 256×256 grayscale images varying the watermark strength to a considerable range, which are shown in Table 3.1. It is verified from the data in the table that, the deviation between the parameters of the SNIG pdf for marked and unmarked images are negligible. So, one can say that, it is justified to use the SNIG pdf for estimating the values of m_0, σ_0^2, m_1, and σ_1^2 of the watermark detector from any received image, without considering whether it is watermarked or not.

3.5 Experimental Results

For a reliable measurement of the performance of the proposed watermark detector, simulations are performed on a large number of images. The performance of the proposed SNIG detector with that of other detectors , based on different pdfs, i.e., Laplacian [30], BKF [48], generalized Gaussian [34], and alpha-stable [1] distributions are compared. First, results of the detector performance in terms of the receiver operating characteristics (ROC) and then the detection probability of each detector for varying strength of invisible watermark are presented.

Here in this section, simulation results of nine grayscale images, namely, *Barbara*, *Lena*, *Boat*, *Paolina*, *Bird*, *Cameraman*, *House*, *Goldhill* and *Mandrill* are given. Some of them are shown in Fig. 3.6. The simulation results here testifies SNIG detector as a better one than the other state of art detectors.

Table 3.1: Parameters of the SNIG pdf estimated from the DCT coefficients of the marked and unmarked images.

Barbara					
Unmarked		*Marked (WDR=-40dB)*		*Marked (WDR=-50dB)*	
α	δ	α	δ	α	δ
0.0010	6.0728	0.0010	6.0737	0.0010	6.0729
Lena					
Unmarked		*Marked (WDR=-40dB)*		*Marked (WDR=-50dB)*	
α	δ	α	δ	α	δ
0.0010	4.4585	0.0010	4.4592	0.0010	4.4586
Boat					
Unmarked		*Marked (WDR=-40dB)*		*Marked (WDR=-50dB)*	
α	δ	α	δ	α	δ
0.0009	5.2396	0.0009	5.2402	0.0009	5.2397
Paolina					
Unmarked		*Marked (WDR=-40dB)*		*Marked (WDR=-50dB)*	
α	δ	α	δ	α	δ
0.0009	6.2984	0.0009	6.2994	0.0009	6.2985
Bird					
Unmarked		*Marked (WDR=-40dB)*		*Marked (WDR=-50dB)*	
α	δ	α	δ	α	δ
0.0014	6.2983	0.0014	6.2993	0.0014	6.2984
Cameraman					
Unmarked		*Marked (WDR=-40dB)*		*Marked (WDR=-50dB)*	
α	δ	α	δ	α	δ
0.0013	9.2012	0.0013	9.2020	0.0013	9.2010
Goldhill					
Unmarked		*Marked (WDR=-40dB)*		*Marked (WDR=-50dB)*	
α	δ	α	δ	α	δ
0.0010	6.1326	0.0010	6.1335	0.0010	6.1327
House					
Unmarked		*Marked (WDR=-40dB)*		*Marked (WDR=-50dB)*	
α	δ	α	δ	α	δ
0.0013	6.9805	0.0013	6.9816	0.0013	6.9806
Mandrill					
Unmarked		*Marked (WDR=-40dB)*		*Marked (WDR=-50dB)*	
α	δ	α	δ	α	δ
0.0007	14.7782	0.0007	14.7806	0.0007	14.7784

3.5.1 Detector Performance in Terms of Receiver Operating Characteristic (ROC) Curves

The theoretical ROC curves are derived for the Laplacian, generalized Gaussian, BKF, Cauchy and the proposed SNIG detector using (3.25), (3.29), (3.30), (3.31) and (3.34), respectively. The probability of false alarm P_{fa} is set to the range 10^{-3} to 1. As the watermark has been embedded both in full frame and in 8×8 blocks, the ROC curves are obtained for both the cases. For full frame images, the ROC curves are drawn keeping the WDR at as -40dB and -50dB. For 8×8 block images, the ROC curves are shown for different coefficients with WDR $= -40$dB.

In Figs. (3.7-3.14), it is clear that for most of the full frame images the SNIG detector gives higher P_{det} for a given P_{fa} compared to other detectors. In

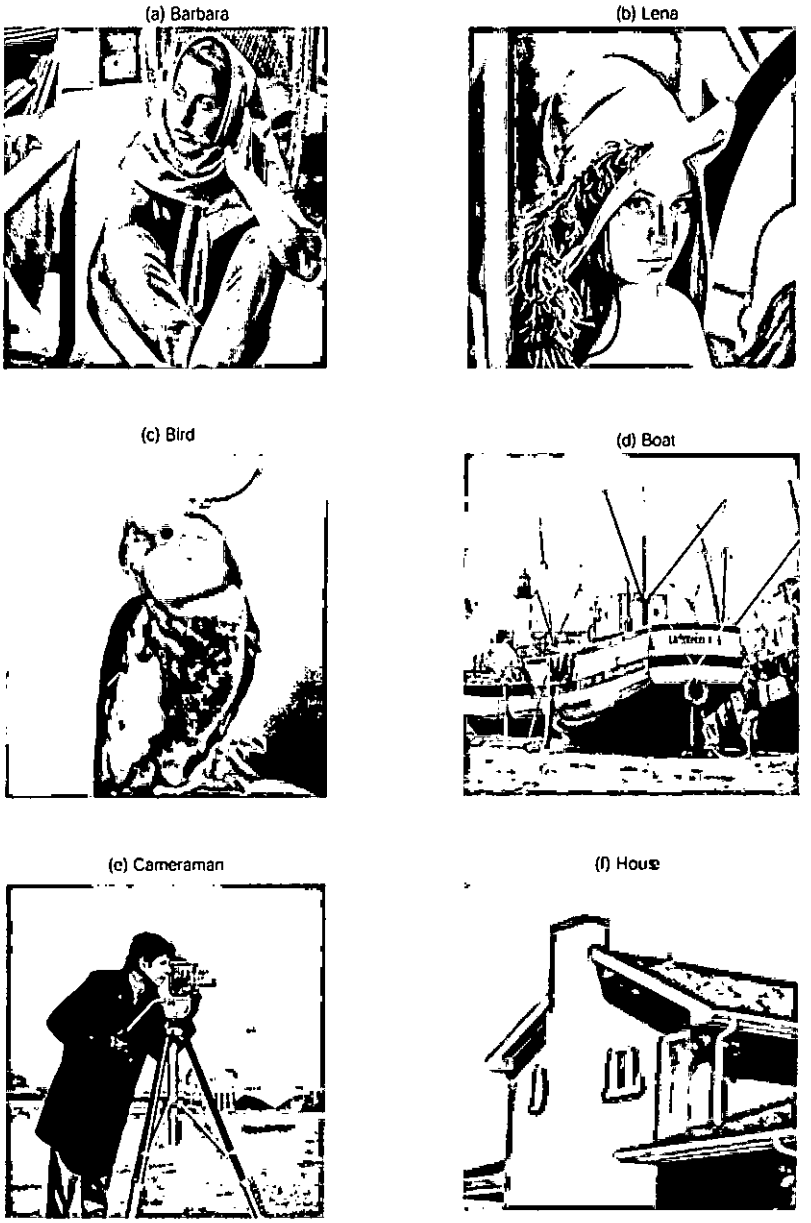


Fig. 3.6: Some of the test images used for watermarking.

case of *Barbara*, *Lena* and *Paolina*, the P_{det} values of the proposed detector is significantly better than the others.

In Figs. (3.15- 3.18), different methods are compared for four test images watermarked in 8×8 blocks. Here, it is also evident that the SNIG detector performs better. Especially for *Barbara* and *Bird*, the differences in P_{det} values are clearly distinguishable.

3.5.2 Detector Performance in Terms of Varying Strength of Watermark

The performance of the SNIG detection scheme is also compared with others when watermarks of varying strength are embedded in a given set of DCT coefficients. For this purpose, WDR is measured using (3.14). Watermarks of varying strength $W[\mathbf{k}]$ are embedded in the DCT coefficients, leading to different values of σ_W^2 and corresponding WDR. As the value of WDR is increased it results in stronger watermark and also becomes more visible (Fig. 3.19). While the watermark strength is increased the properties of the HVS is taken into account, in order to ensure invisibility. However, its power can be decreased to the point where it is still detectable.

The detector performance is studied for images watermarked both in full frame and blocks. It is clear from Figs. (3.20-3.28) that in almost all the images, the SNIG detector exhibits better performance than the others as it shows higher value of detection probability for a wide range of WDR. The probability of false alarm is kept at 0.01 while WDR is varied between -30 dB to -60 dB.

It should be noted that, among the full frame watermarked images, SNIG shows significant better performance specially in case of *Barbara* and *Paolina*. But in case of *Goldhill*, the P_{det} value of SNIG detector falls for higher values of WDR, which indicates that, for strong watermark the performance of SNIG detector degrades. However, it performs better for low WDR, i.e. weaker and more invisible watermark which is the more desired condition.

3.6 Conclusion

In this chapter, the proposed watermark detector is developed based on SNIG prior. Before developing the detector, a brief overview of the statistical models

used in literature for image data modeling is provided. Then the watermark embedding and detection algorithm is discussed with detailed mathematical framework.

After development of the detector, its performance is evaluated and compared with other state of art detectors in terms of ROC and for different watermark strength. The better performance of SNIG detector is verified through the simulation results.

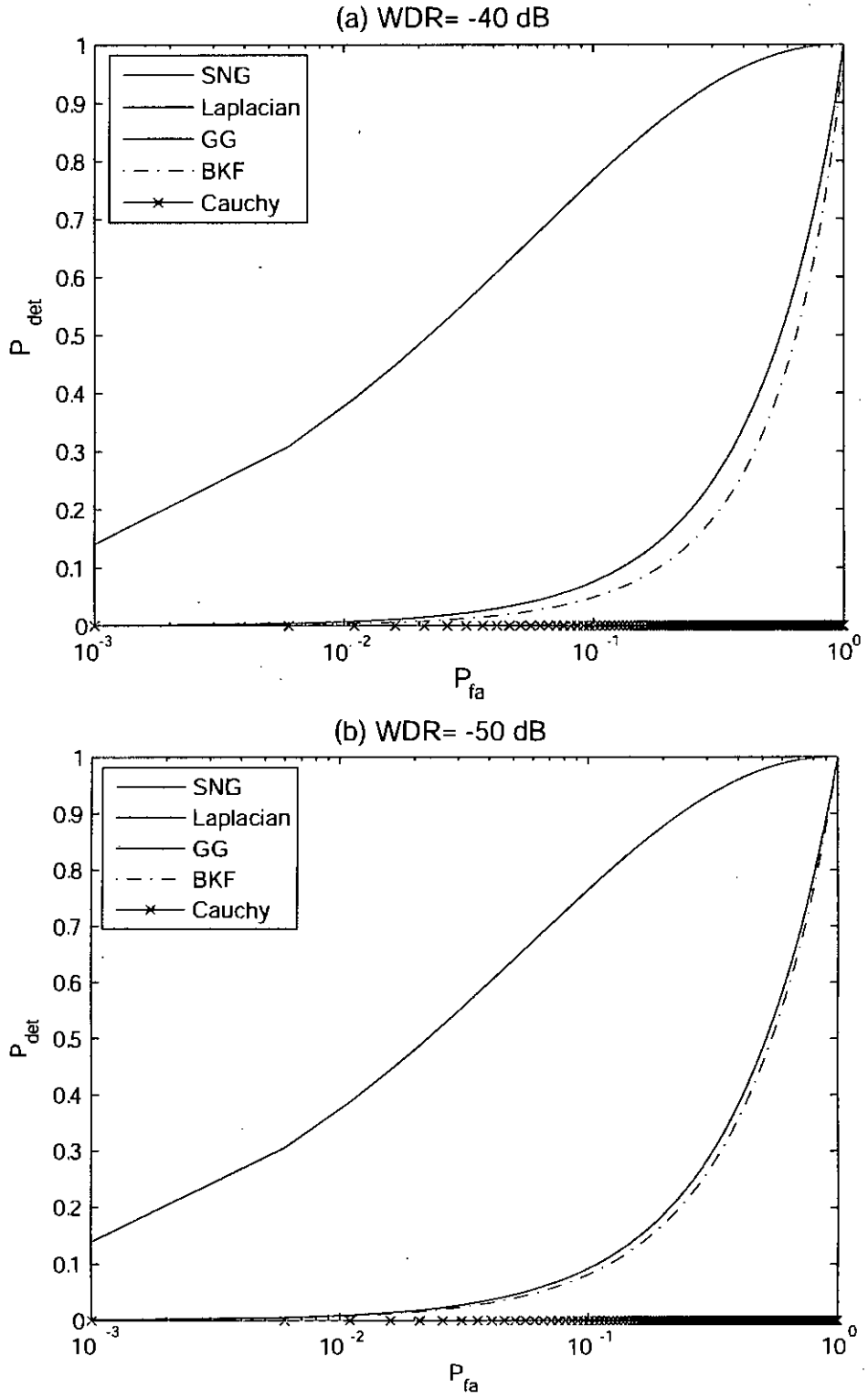


Fig. 3.7: Receiver Operating Characteristic curve for 'Barbara' (watermarked in full-frame) with (a) WDR= -40 dB, (b) WDR= -50 dB

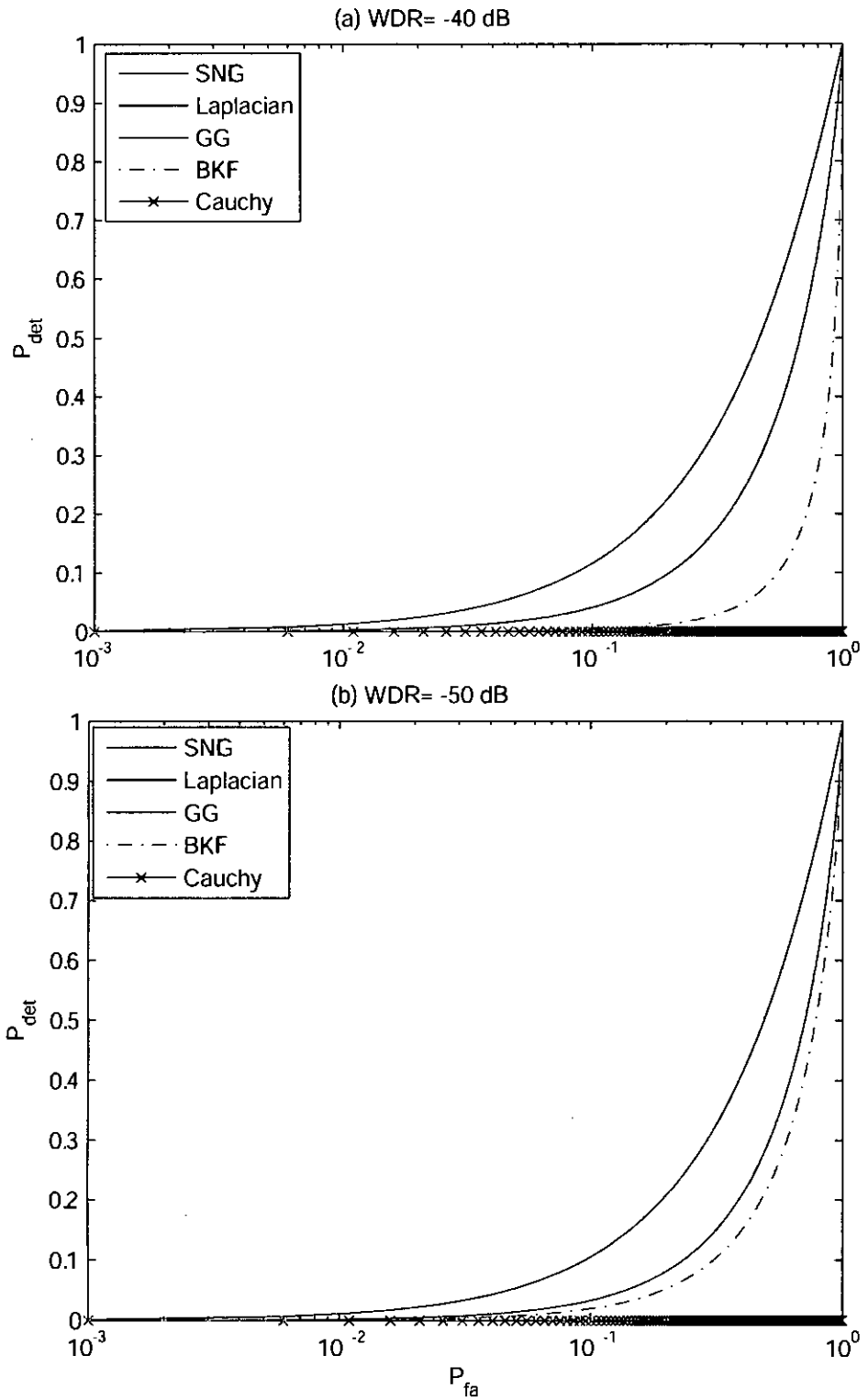


Fig. 3.8: Receiver Operating Characteristic curve for 'Lena' (watermarked in full-frame) with (a) WDR= -40 dB, (b) WDR= -50 dB

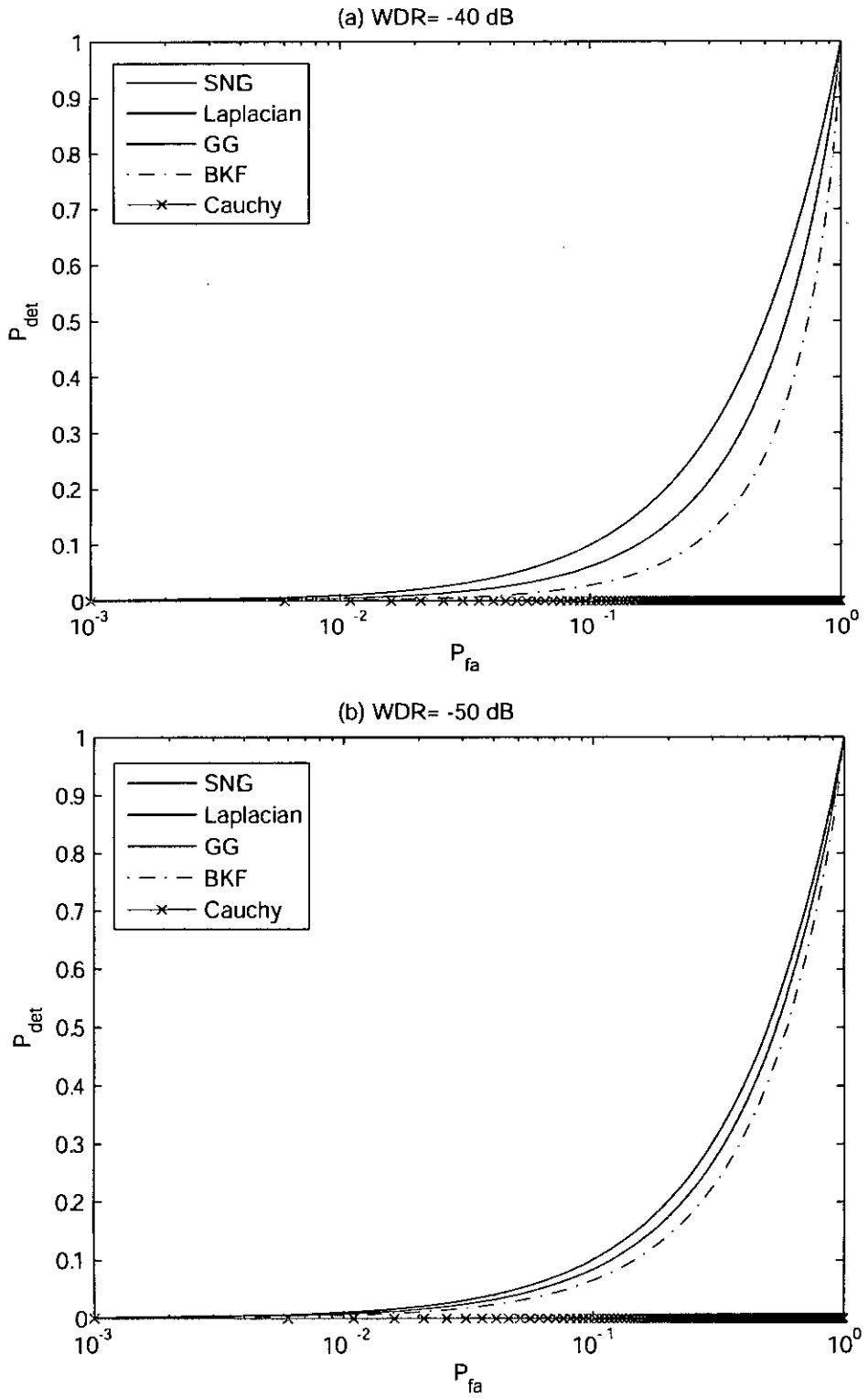


Fig. 3.9: Receiver Operating Characteristic curve for 'Bird' (watermarked in full-frame) with (a) WDR= -40 dB, (b) WDR= -50 dB

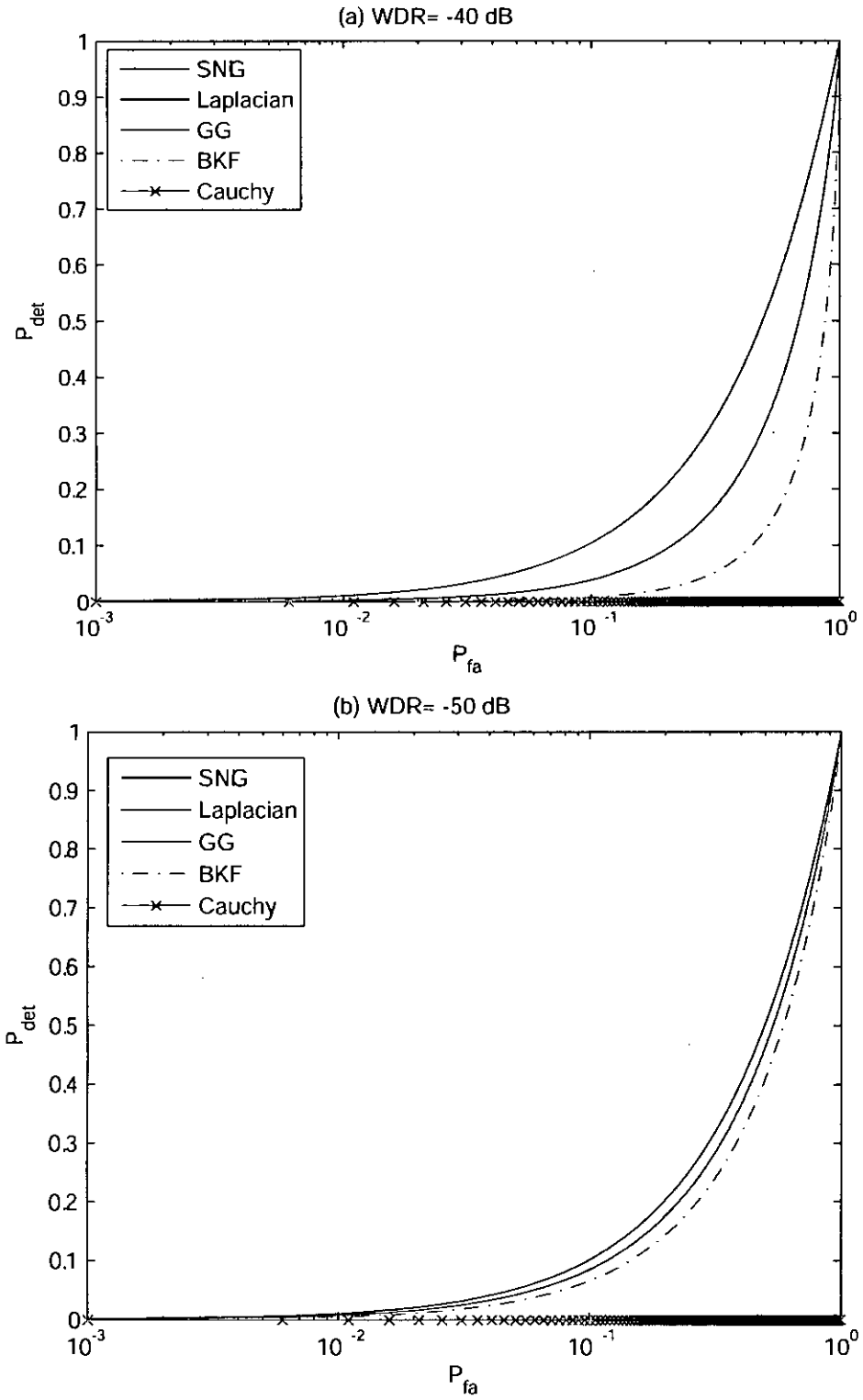


Fig. 3.10: Receiver Operating Characteristic curve for 'Boat' (watermarked in full-frame) with (a) WDR= -40 dB, (b) WDR= -50 dB

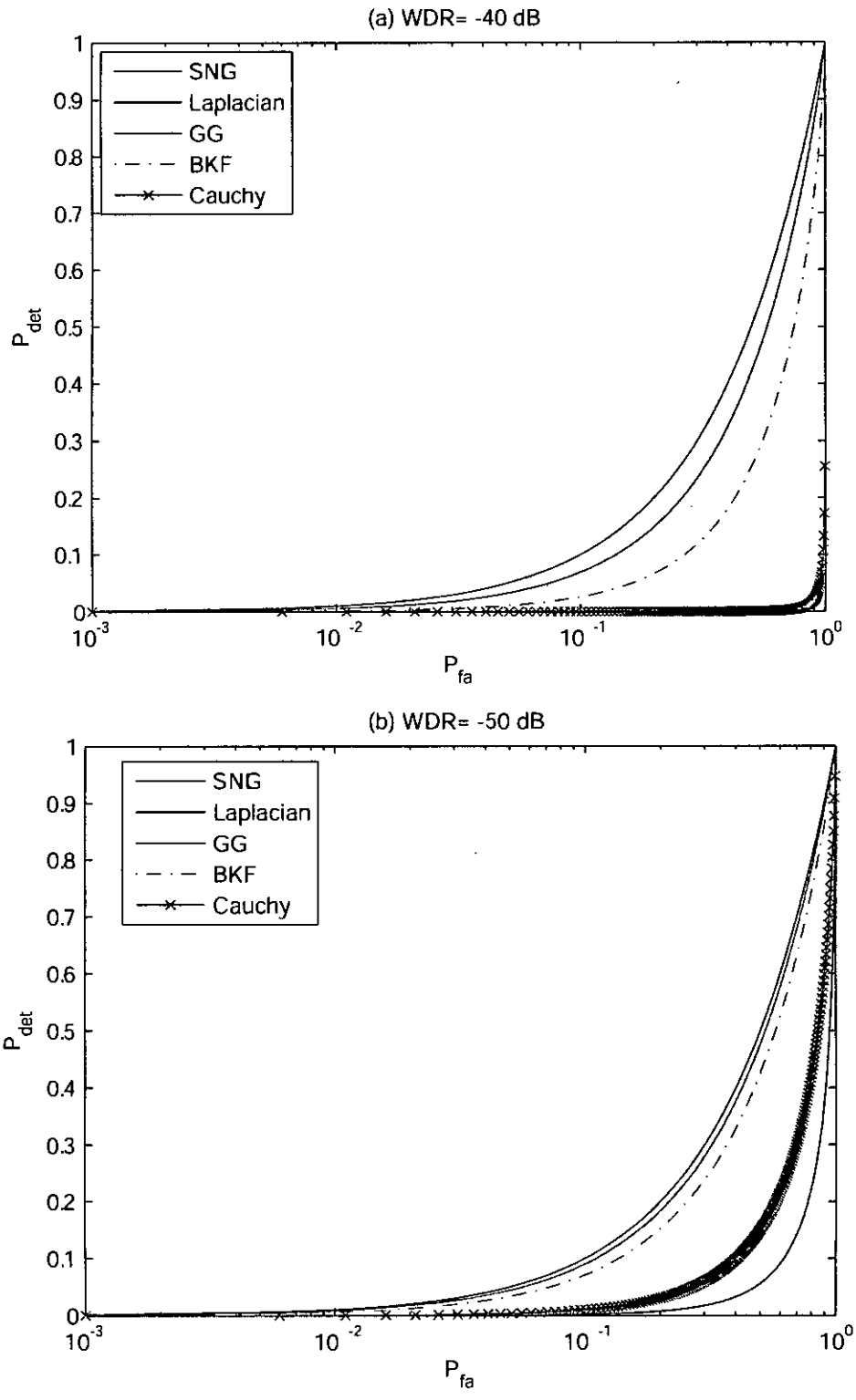


Fig. 3.11: Receiver Operating Characteristic curve for 'Cameraman' (watermarked in full-frame) with (a) WDR= -40 dB, (b) WDR= -50 dB

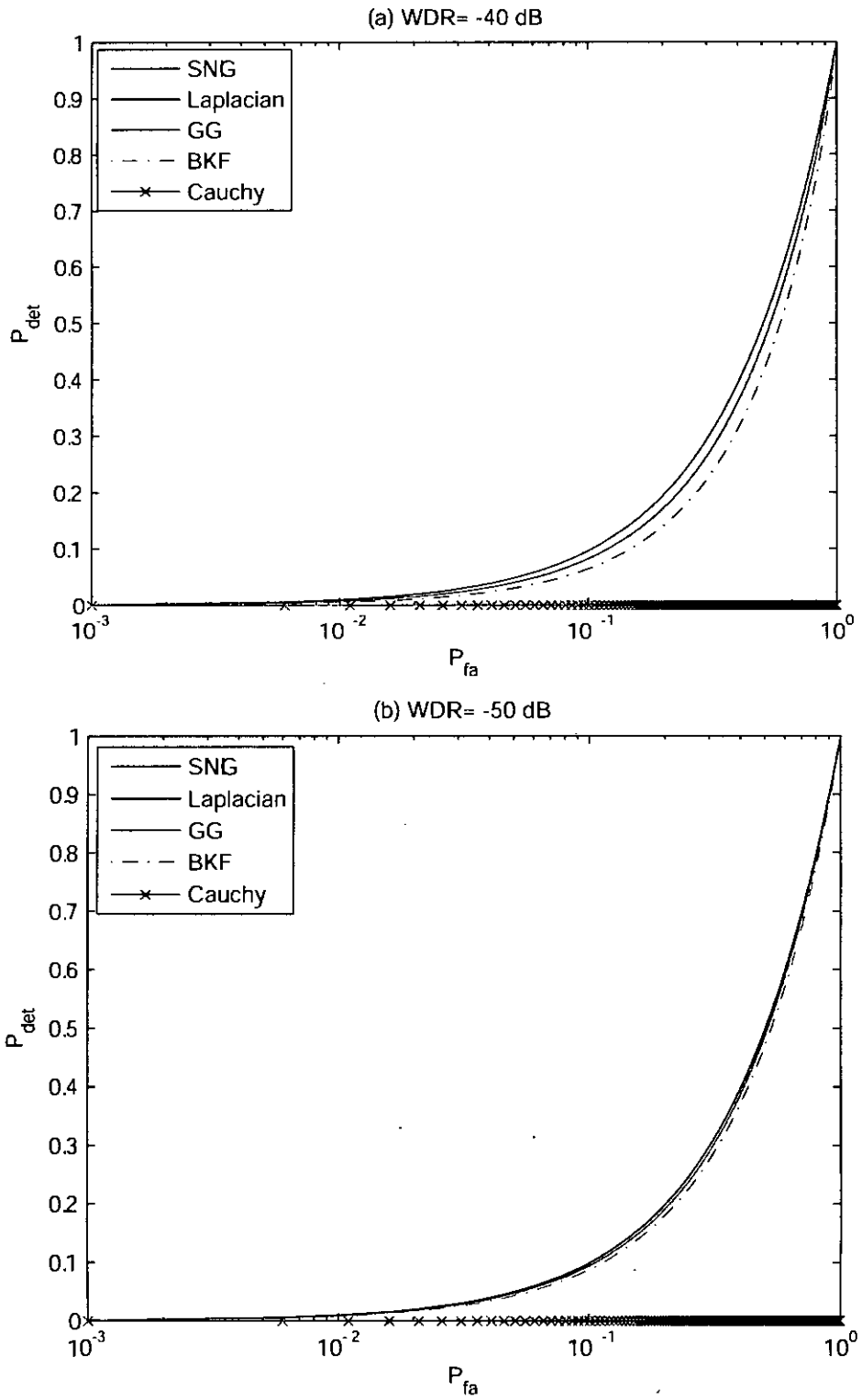


Fig. 3.12: Receiver Operating Characteristic curve for 'House' (watermarked in full-frame) with (a) WDR= -40 dB, (b) WDR= -50 dB

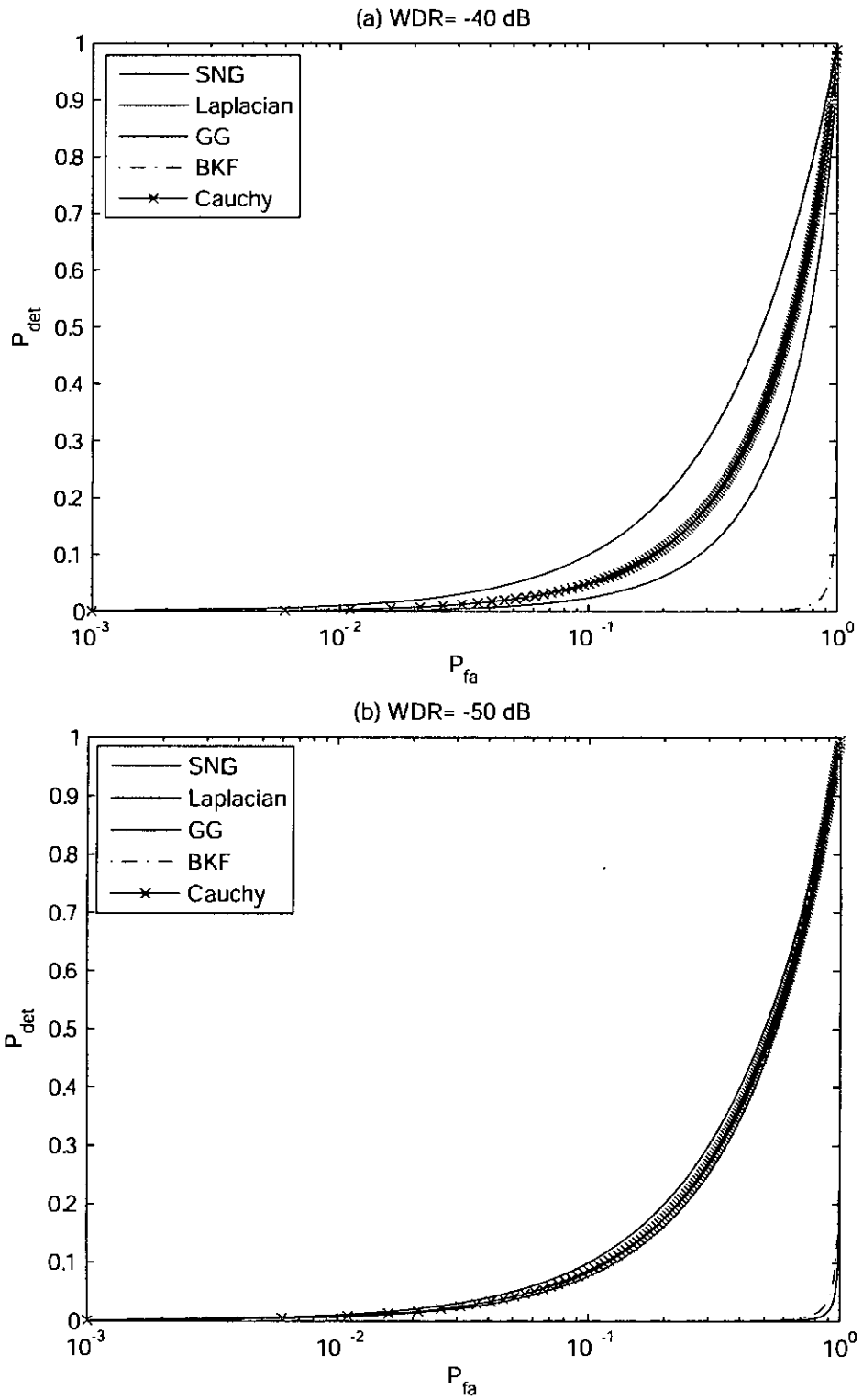


Fig. 3.13: Receiver Operating Characteristic curve for 'Mandrill' (watermarked in full-frame) with (a) WDR= -40 dB, (b) WDR= -50 dB

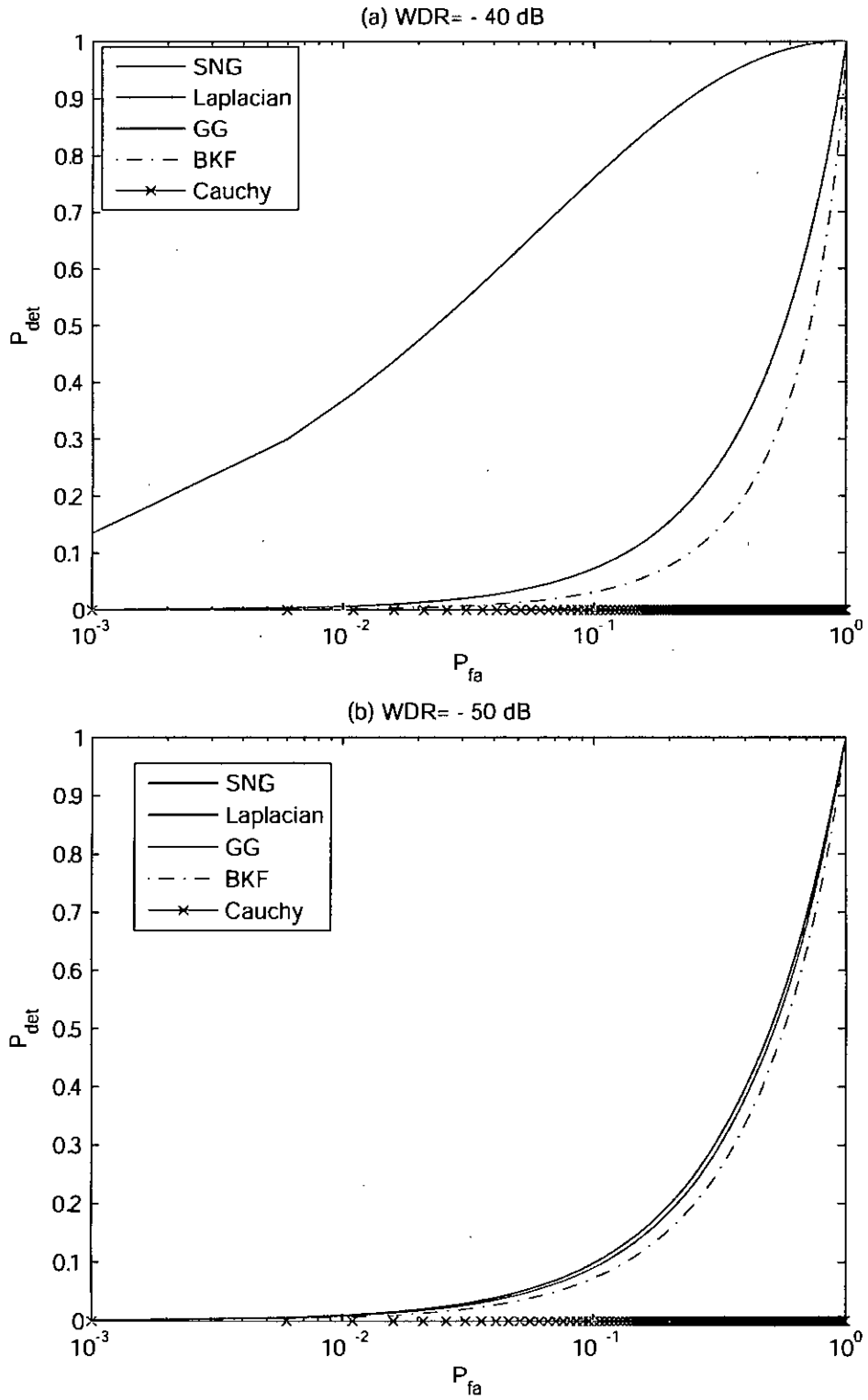


Fig. 3.14: Receiver Operating Characteristic curve for 'Paolina' (watermarked in full-frame) with (a) WDR= -40 dB, (b) WDR= -50 dB

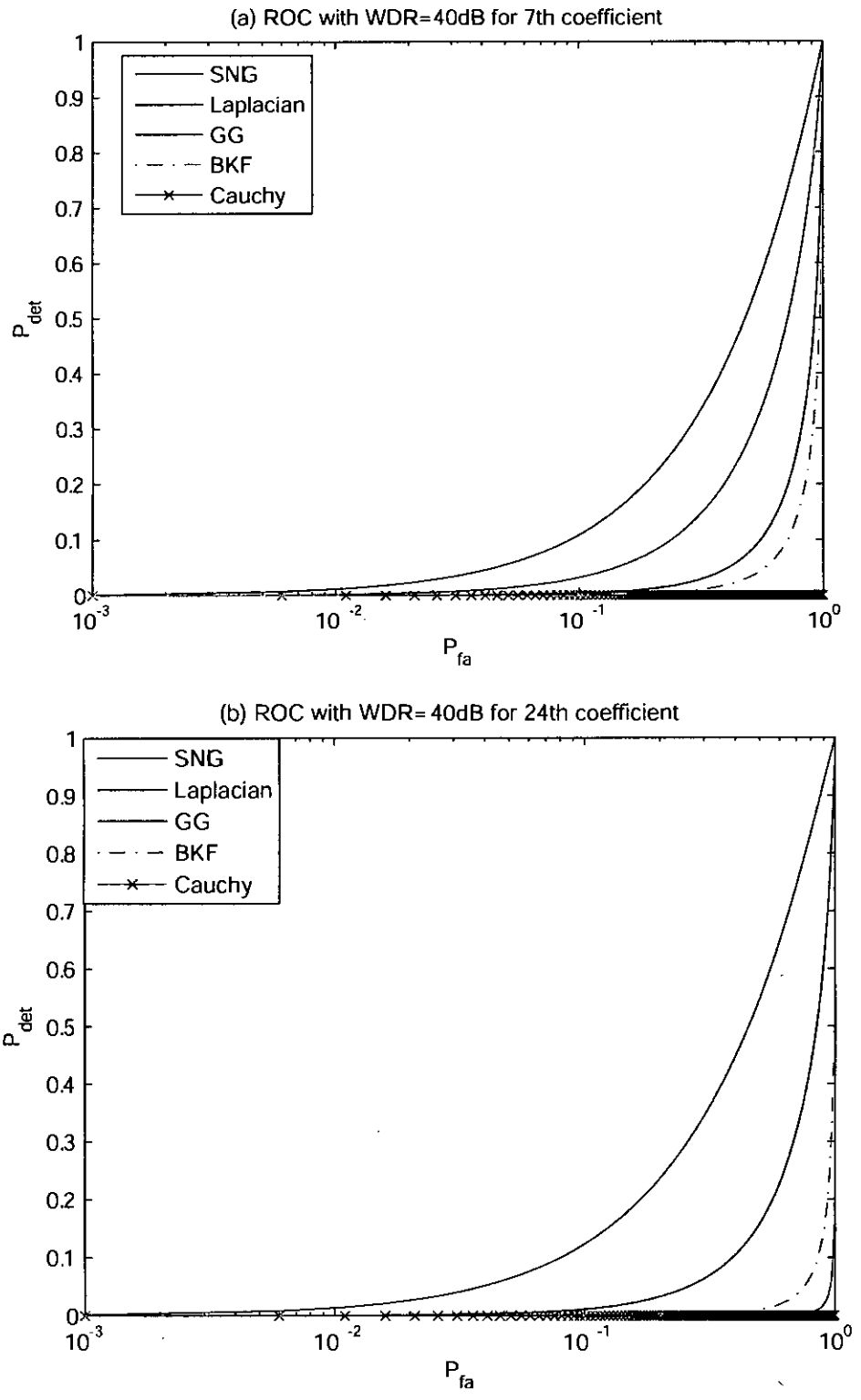


Fig. 3.15: Receiver Operating Characteristic curve for 'Barbara' (watermarked in 8×8 blocks) with WDR= -40 dB for (a) 7th and (b) 24th coefficients

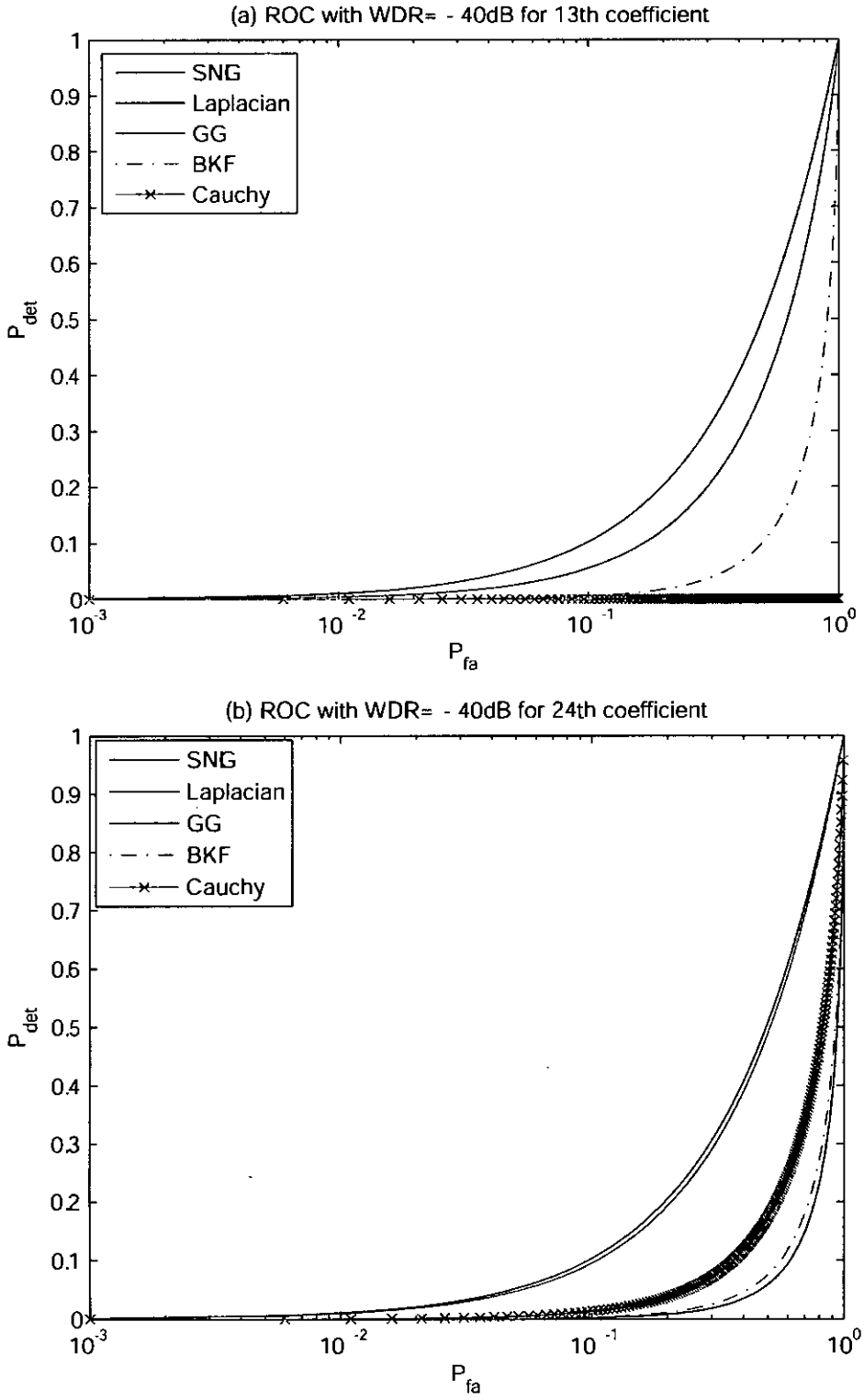


Fig. 3.16: Receiver Operating Characteristic curve for 'Lena' (watermarked in 8×8 blocks) with WDR= -40 dB for (a) 13th and (b) 24th coefficients

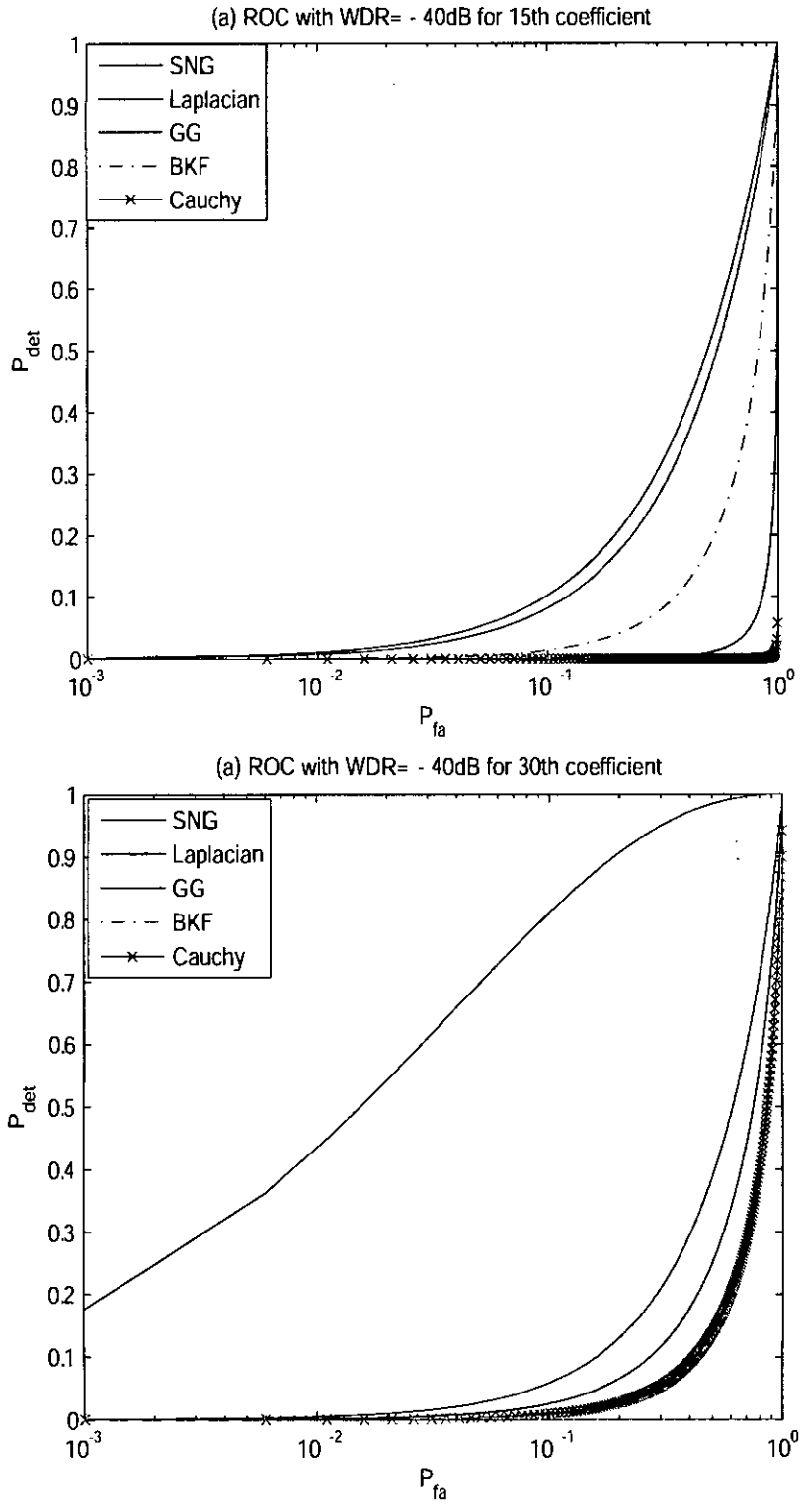


Fig. 3.17: Receiver Operating Characteristic curve for 'Bird' (watermarked in 8×8 blocks) with WDR= -40 dB for (a) 15th and (b) 30th coefficients

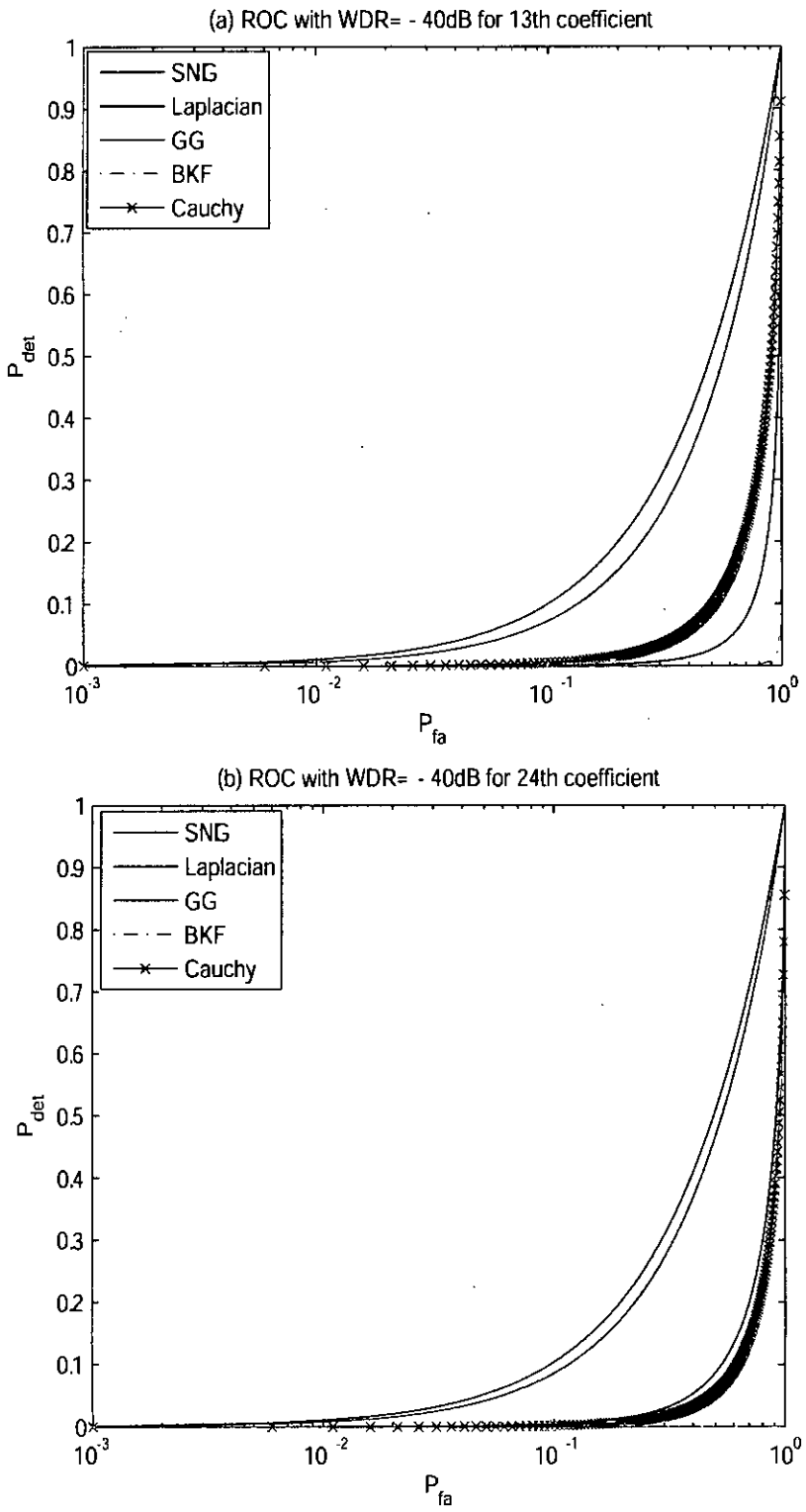


Fig. 3.18: Receiver Operating Characteristic curve for 'Boat' (watermarked in 8×8 blocks) with WDR= -40 dB for (a) 13th and (b) 24th coefficients

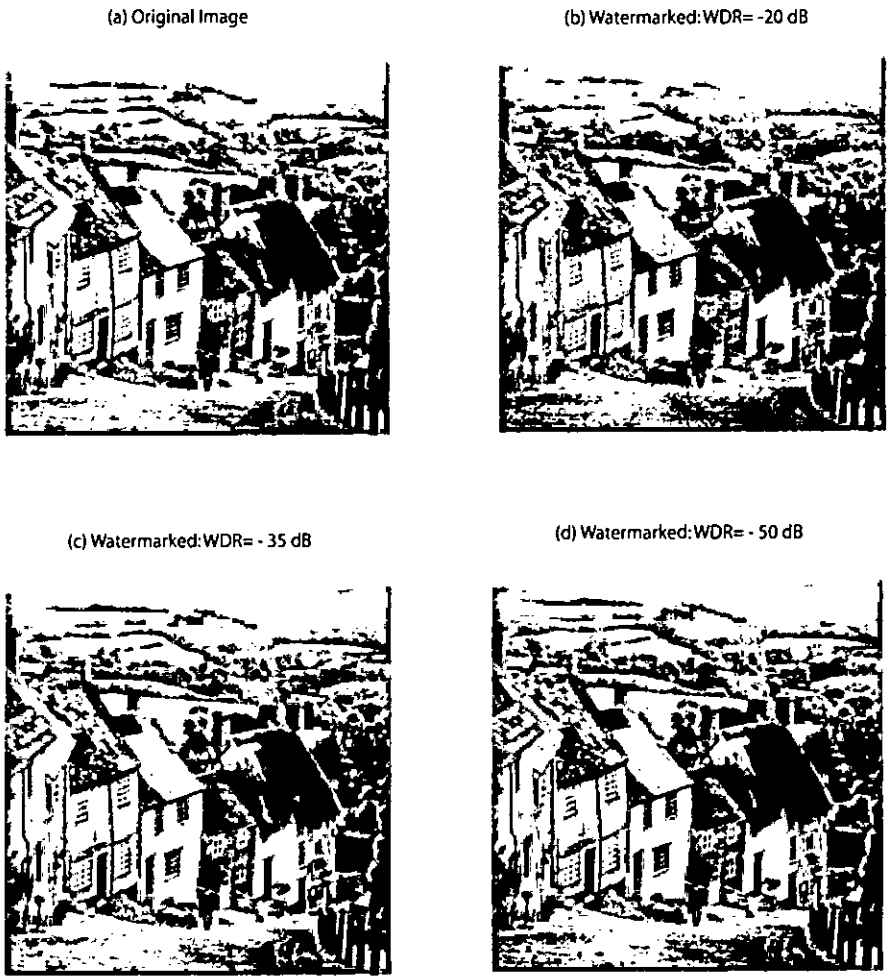


Fig. 3.19: The test image *Goldhill* in original and watermarked form. Watermark strength is varied with (b) WDR=-20dB, (c) WDR=-35dB, and (d) WDR=-50dB.

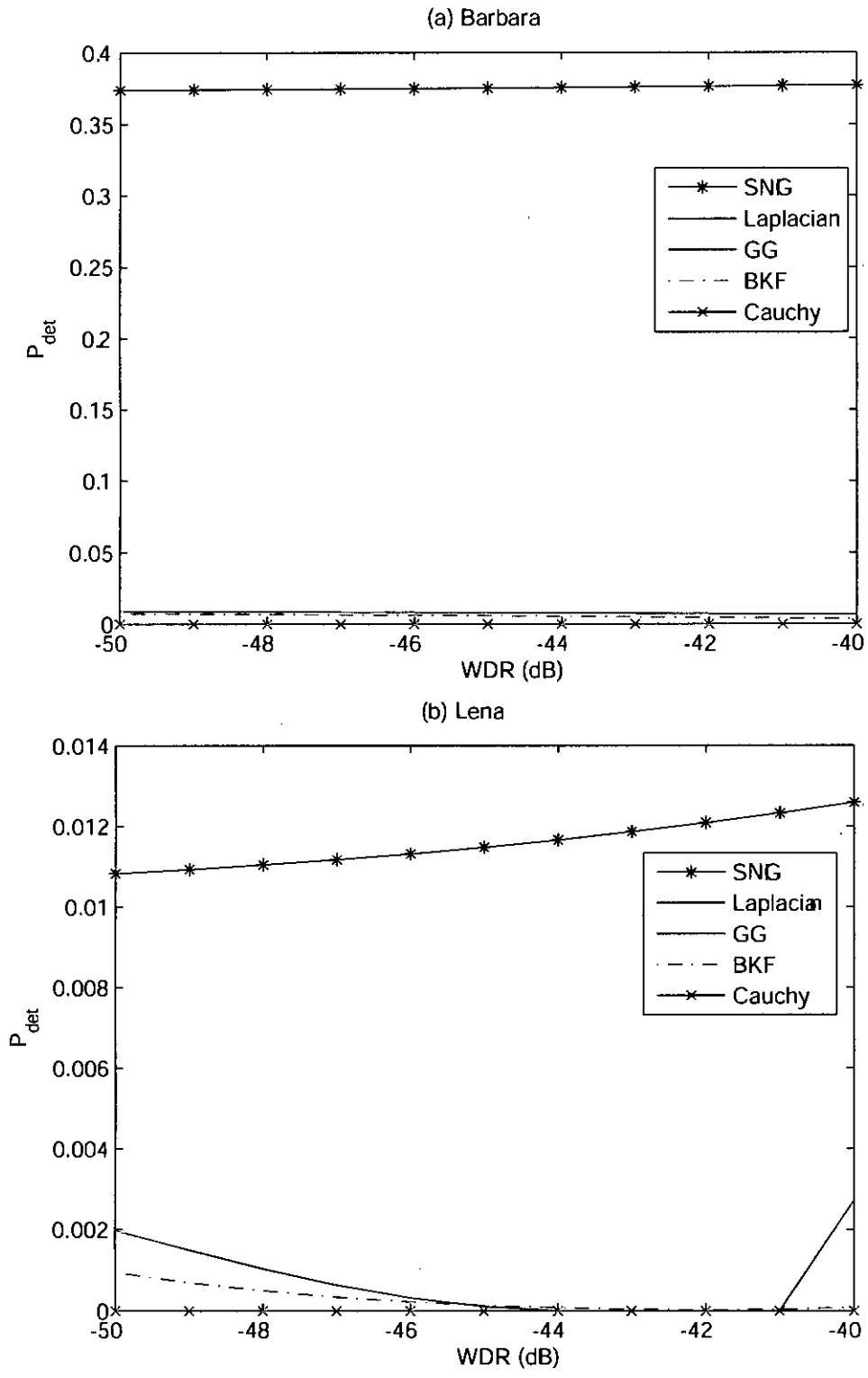


Fig. 3.20: Probability of detection for varying strength of watermark (embedded in fullframe) with the false alarm probability set to $P_{fa} = 10^{-2}$ for test images (a) *Barbara*, (b) *Lena*.

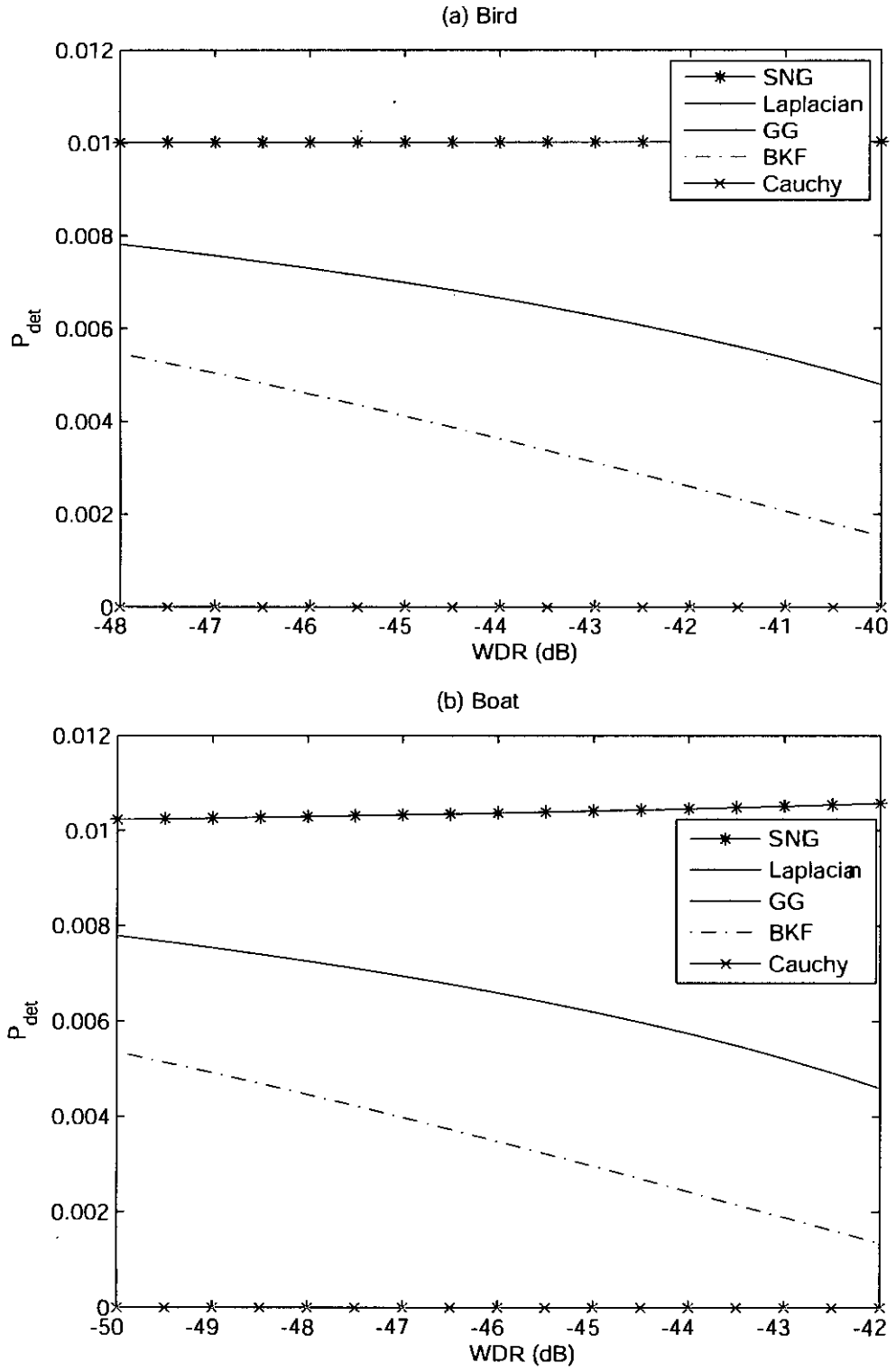


Fig. 3.21: Probability of detection for varying strength of watermark (embedded in fullframe) with the false alarm probability set to $P_{fa} = 10^{-2}$ for test images (a) *Bird*, (b) *Boat*.

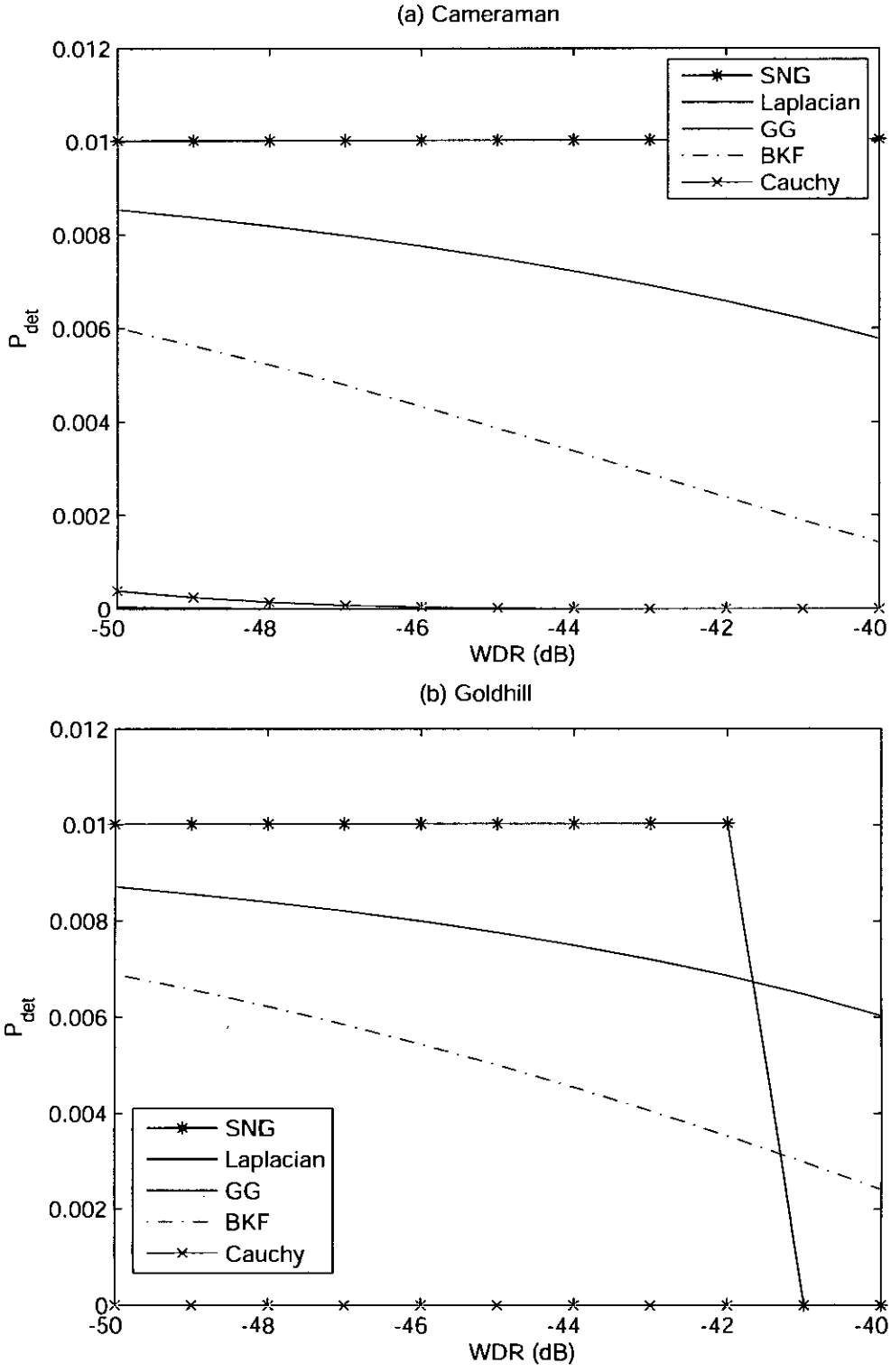


Fig. 3.22: Probability of detection for varying strength of watermark (embedded in fullframe) with the false alarm probability set to $P_{fa} = 10^{-2}$ for test images (a) *Cameraman*, (b) *Goldhill*.

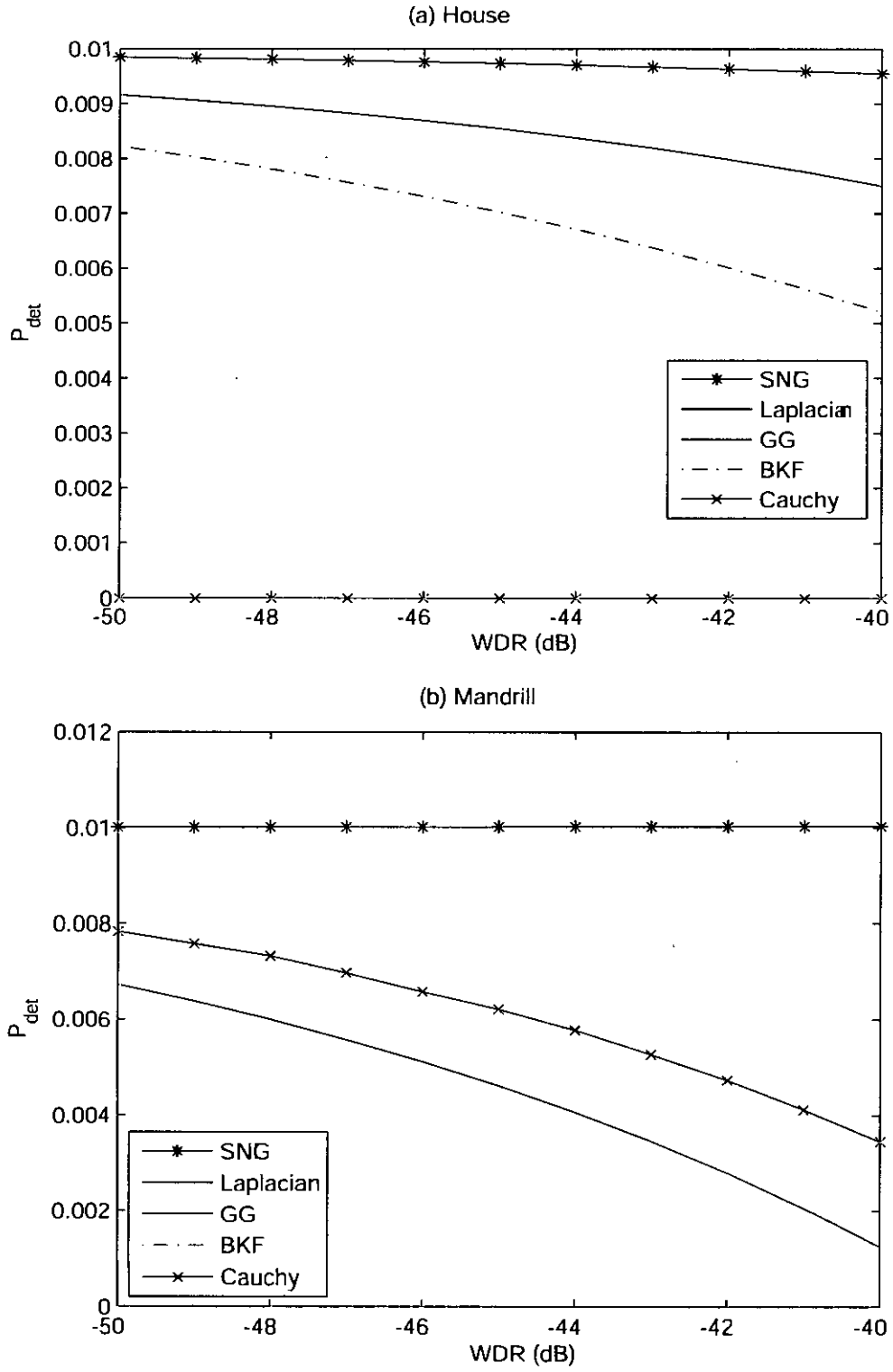


Fig. 3.23: Probability of detection for varying strength of watermark (embedded in fullframe) with the false alarm probability set to $P_{fa} = 10^{-2}$ for test images (a) *House*, (b) *Mandrill*.

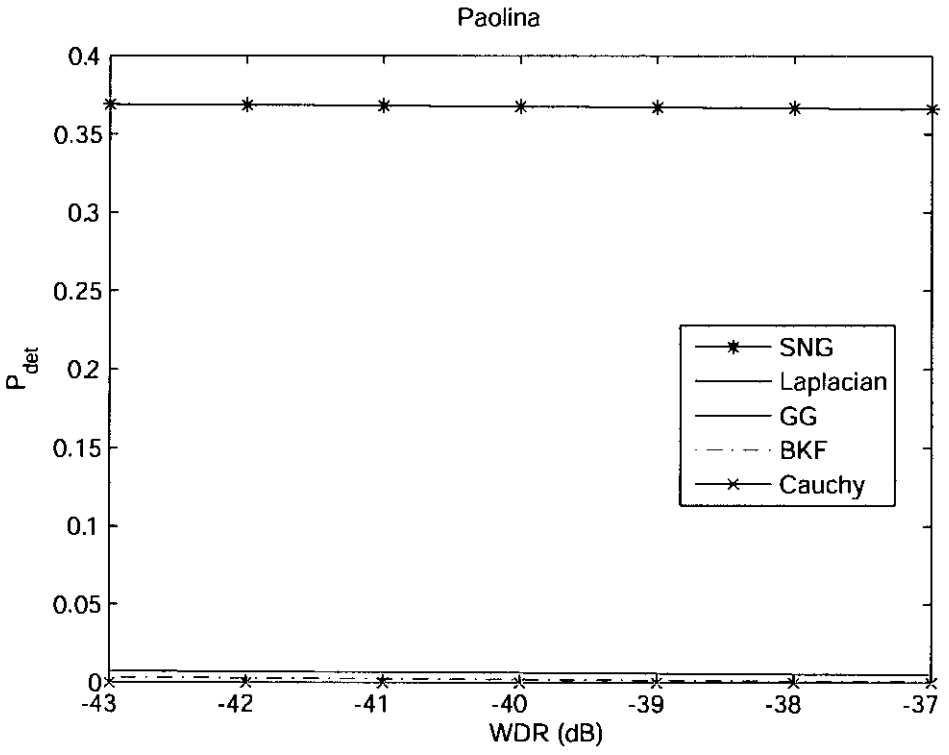


Fig. 3.24: Probability of detection for varying strength of watermark (embedded in fullframe) with the false alarm probability set to $P_{fa} = 10^{-2}$ for test image *Paolina*

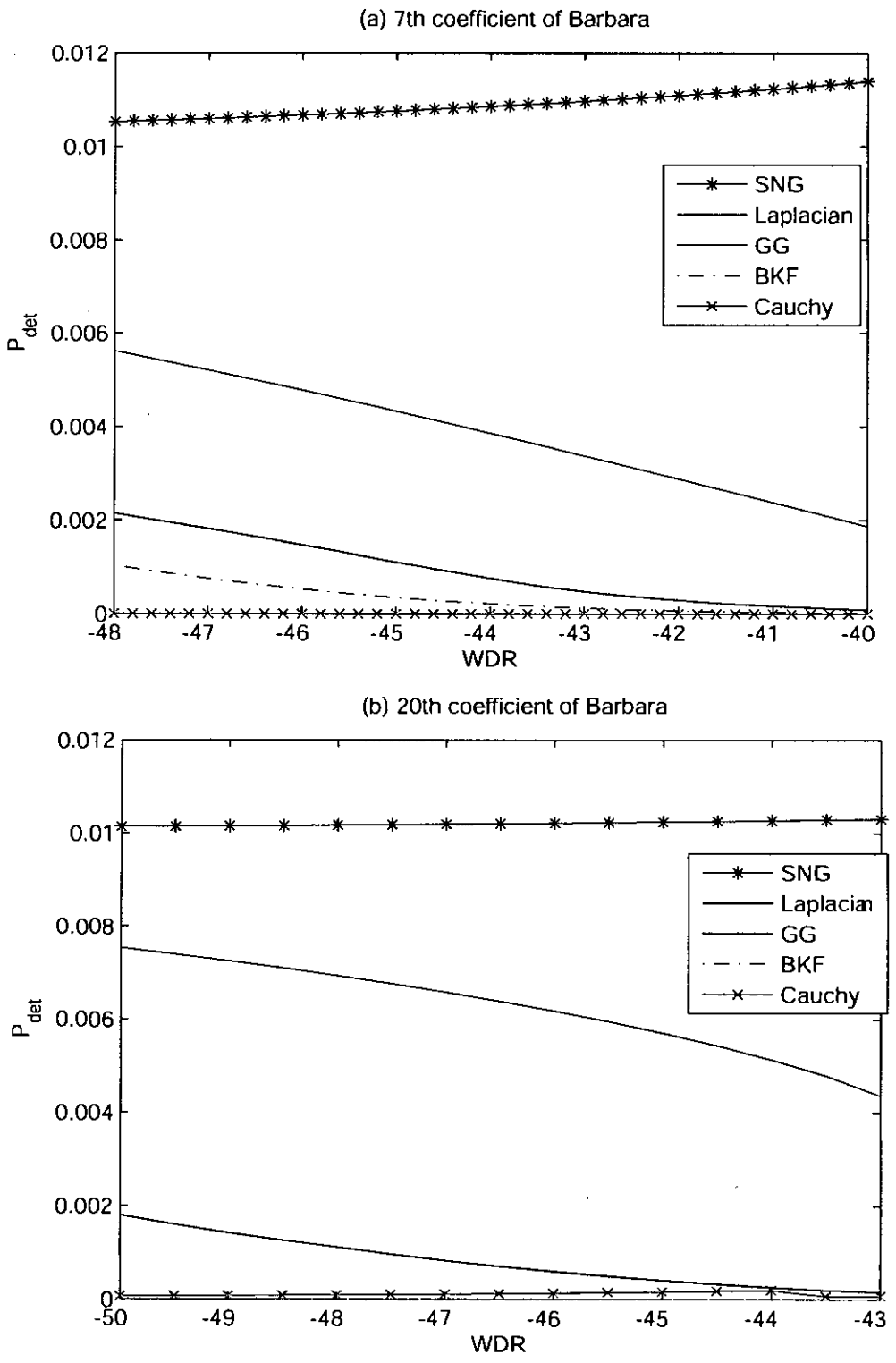


Fig. 3.25: Probability of detection for varying strength of watermark (embedded in 8X8 blocks) for (a) 7th and (b) 20th coefficients of *Barbara*. The false alarm probability set to $P_{fa} = 10^{-2}$

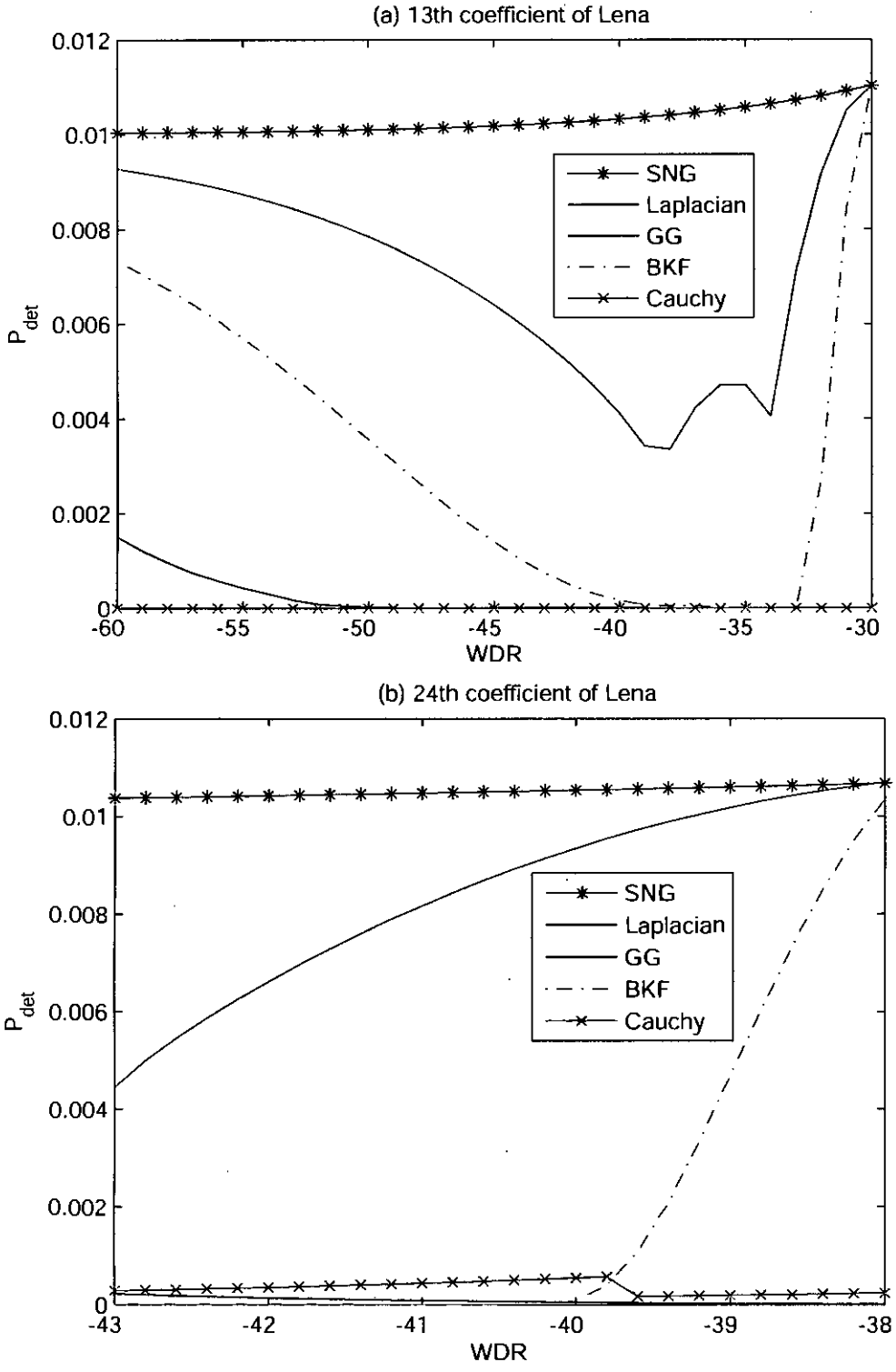


Fig. 3.26: Probability of detection for varying strength of watermark (embedded in 8×8 blocks) for (a) 13th and (b) 24th coefficients of *Lena*. The false alarm probability set to $P_{fa} = 10^{-2}$

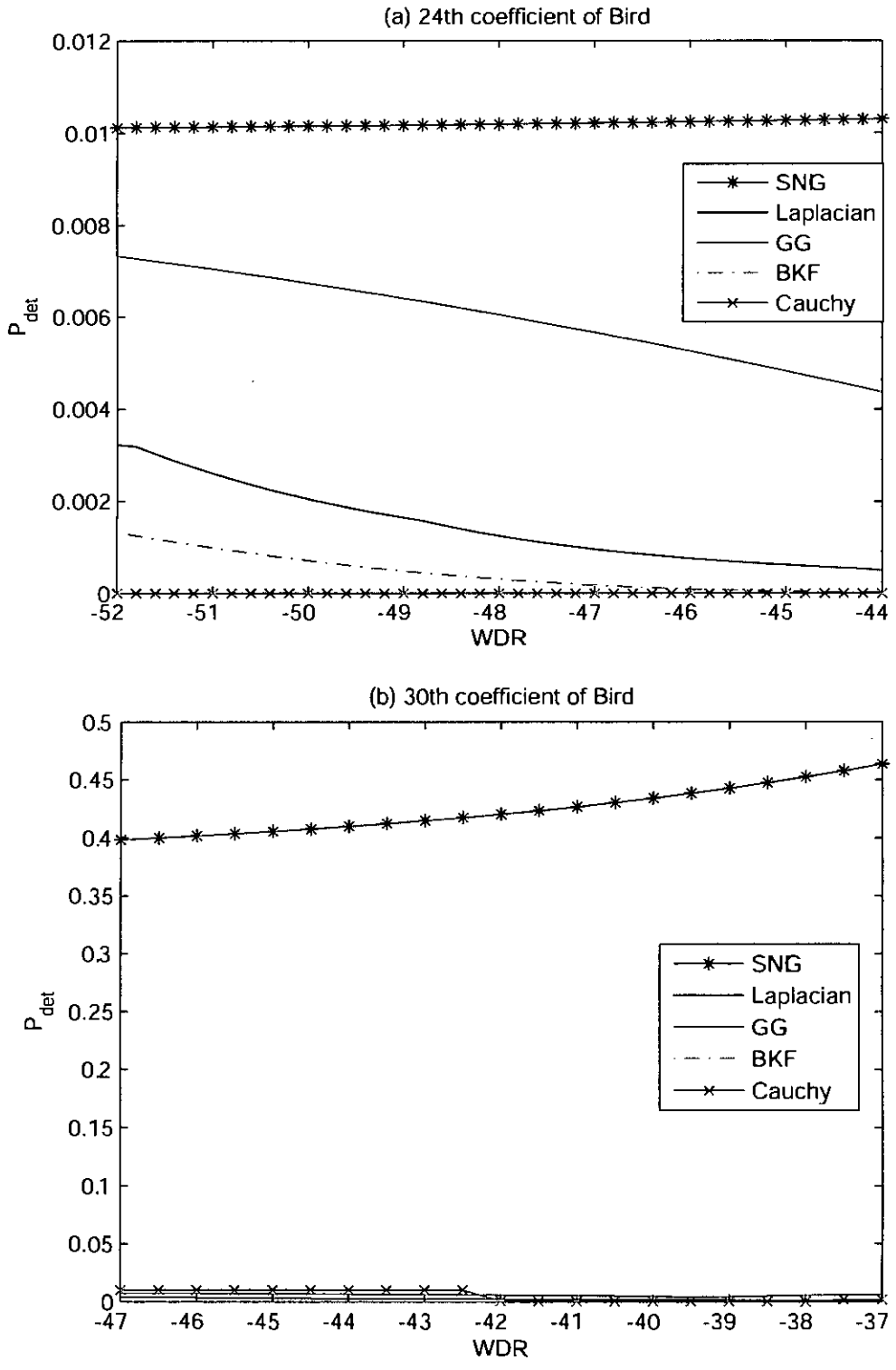


Fig. 3.27: Probability of detection for varying strength of watermark (embedded in 8×8 blocks) for (a) 24th and (b) 30th coefficients of *Bird*. The false alarm probability set to $P_{fa} = 10^{-2}$

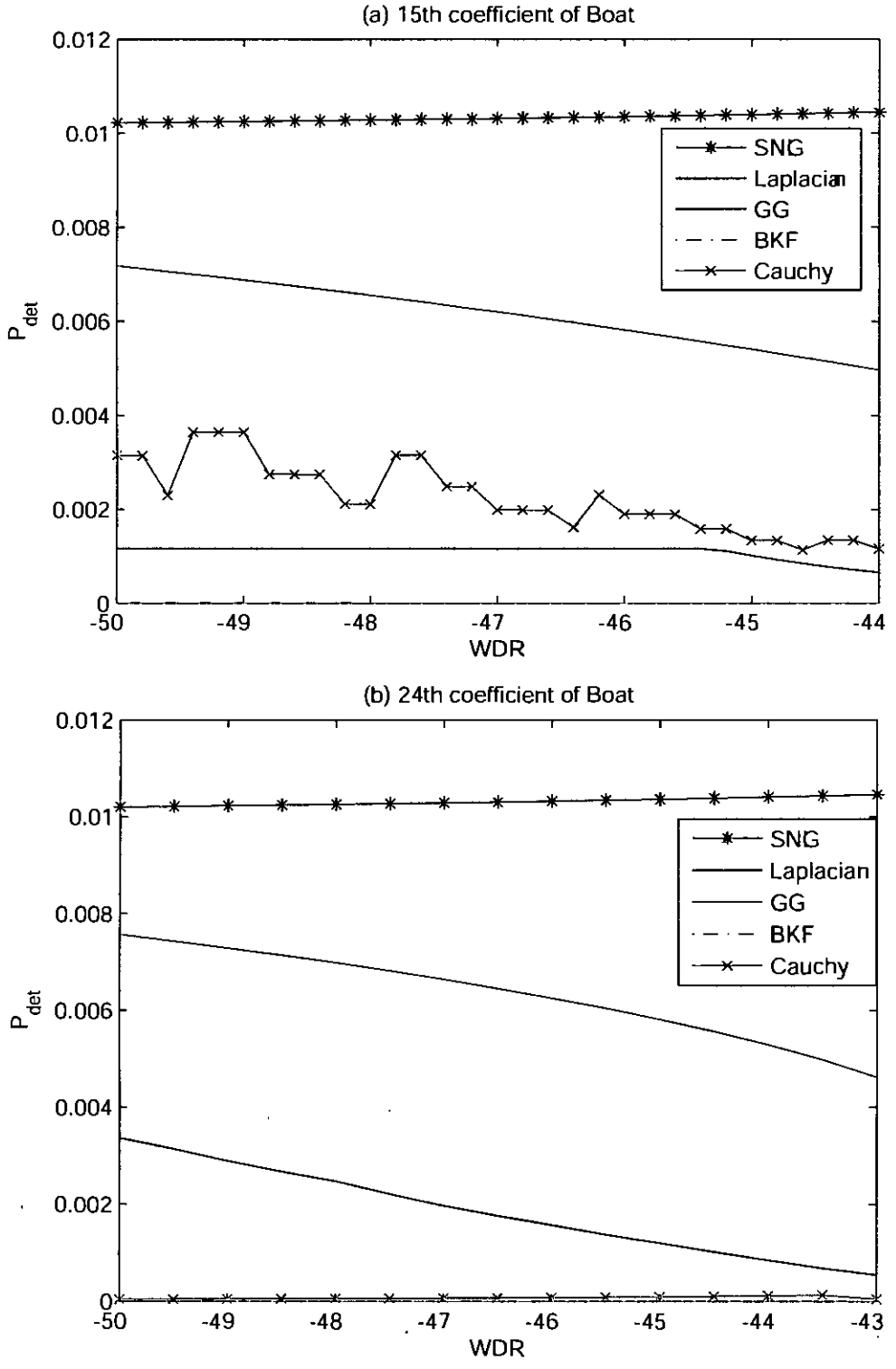


Fig. 3.28: Probability of detection for varying strength of watermark (embedded in 8×8 blocks) for (a) 15th and (b) 24th coefficients of *Boat*. The false alarm probability set to $P_{fa} = 10^{-2}$

Chapter 4

SNIG-based Model for Video DCT Coefficients

4.1 Introduction

The use of digital video is widespread now-a-days ranging from entertainment to medical applications. Various algorithms have been developed in recent times for the storage, transmission and analysis of digital video. Practical video processing techniques often use the discrete cosine transform (DCT) due to its excellent signal decorrelation property, thus enabling the representation of the signal information in terms of as few coefficients as possible, and availability of fast DCT algorithms for real time implementations [49]. For example, in MPEG-2, one of the most commonly used video coding standard, the DCT is employed for intra-frame compression. Each video frame is divided into 8×8 blocks and subsequently the blocks are subjected to the DCT. Since, the DCT has the ability to compact the signal energy into a few coefficients, most of the DCT coefficients of an image block are small and can be quantized to zero. Thus, the intra-frame signal information can be stored by using a small number of coefficients. The inter-frame information can also be decomposed using the DCT and the corresponding coefficients subsequently compressed as the intra-frame coefficients [50]. However, for efficient quantization of the DCT coefficients, it is necessary to know about the statistics of these coefficients. More specifically, the quantization step size and the corresponding decision levels can be efficiently designed by incorporating the probability distribution of these coefficients in the integrals for obtaining these values. For this purpose, it is essential to assume a certain pdf to model the DCT coefficients. Therefore, as it was in the case of image watermarking, the

knowledge about the distribution of the DCT coefficients might also be useful for designing video watermarking, since each frame can be considered as an individual image and one can exploit it to spread the hidden message in a robust and efficient manner in the frames [27].

In this chapter, the SNIG pdf is employed for modeling the DCT coefficients corresponding to the digital video frames. The parameters of the SNIG pdf are obtained by minimizing the Kullback-Leibler (KL) divergence [39] between the SNIG PDF and that corresponding to the DCT coefficients. Monte Carlo simulations are carried out to study the efficiency of the parameter estimation technique. The effectiveness of the SNIG pdf in modeling the DCT coefficients of video frames is investigated through extensive simulations using various standard digital videos. Both block- and full-frame DCT coefficients are utilized in the simulations. The description of SNIG pdf is given in Chapter 3, so not repeated here.

4.2 Modeling of the DCT Coefficients

In this section, the modeling of the DCT coefficients of digital video is discussed [51]. Experiments are conducted using the DCT coefficients of various standard video sequences to study the goodness-of-fit of the SNIG pdf. To make sure that the findings of the experiments are general enough, video sequences with different characteristics such as high motion and low motion are used. The video sequences are collected from the website of the Center for Image Processing Research, Rensselaer Polytechnic Institute.
(http://www.cipr.rpi.edu/resource/sequences/index.html).

Fig. 4.1 shows sample frames of some of the video sequences used in the experiments. For a particular video sequence, the distributions of the block-DCT coefficients of the corresponding frames are fitted with the SNIG, Laplacian, GG and Bessel K form (BKF) [48] pdfs. The parameters of the GG and BKF pdfs are obtained using the methods described in [52] and [48], respectively. The method in [52] is used for estimating the GG parameters due to its ability to provide estimates that are about as good as the maximum-likelihood ones, while incurring a considerably less computational complexity [52]. For a particular frame of a video sequence, the goodness-of-fit of the various pdfs are compared

of the *Tennis* video sequence. It is seen that the SNIG pdf matches the empirical ones more closely than the other pdfs.

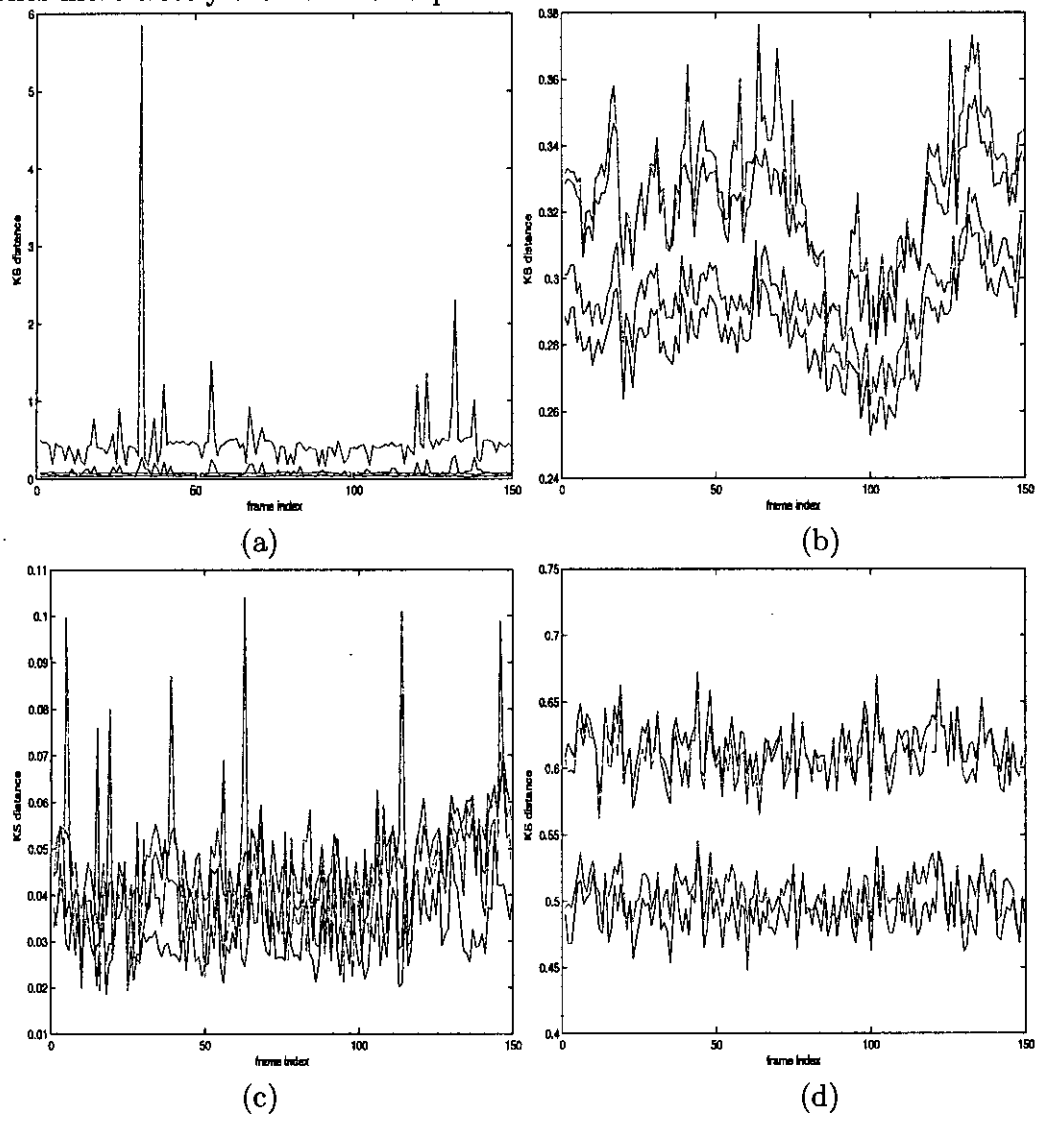


Fig. 4.2: Plot of the values of the K-S distance for various block-DCT coefficients of the *Miss America* video sequence: (a) C_{01}, (b) C_{10}, (c) C_{22}, and (d) C_{50}. Plots of the Laplacian, SNIG, GG and BKF PDFs are shown using red, green, blue and magenta colored lines.

Experiments have also been carried out using the full-frame DCT coefficients of various video sequences. Figs. 4.6 and 4.7 show the plots of K-S distances for various pdfs for the *Miss America*, *Salesman*, *Tennis*, *Football*, *Garden* and *Susie* video sequences. It is observed from these figures that the values of the K-S distance corresponding to the SNIG pdf is smaller than those of the other pdfs for different frames, thus indicating its superiority in modeling the full-frame DCT

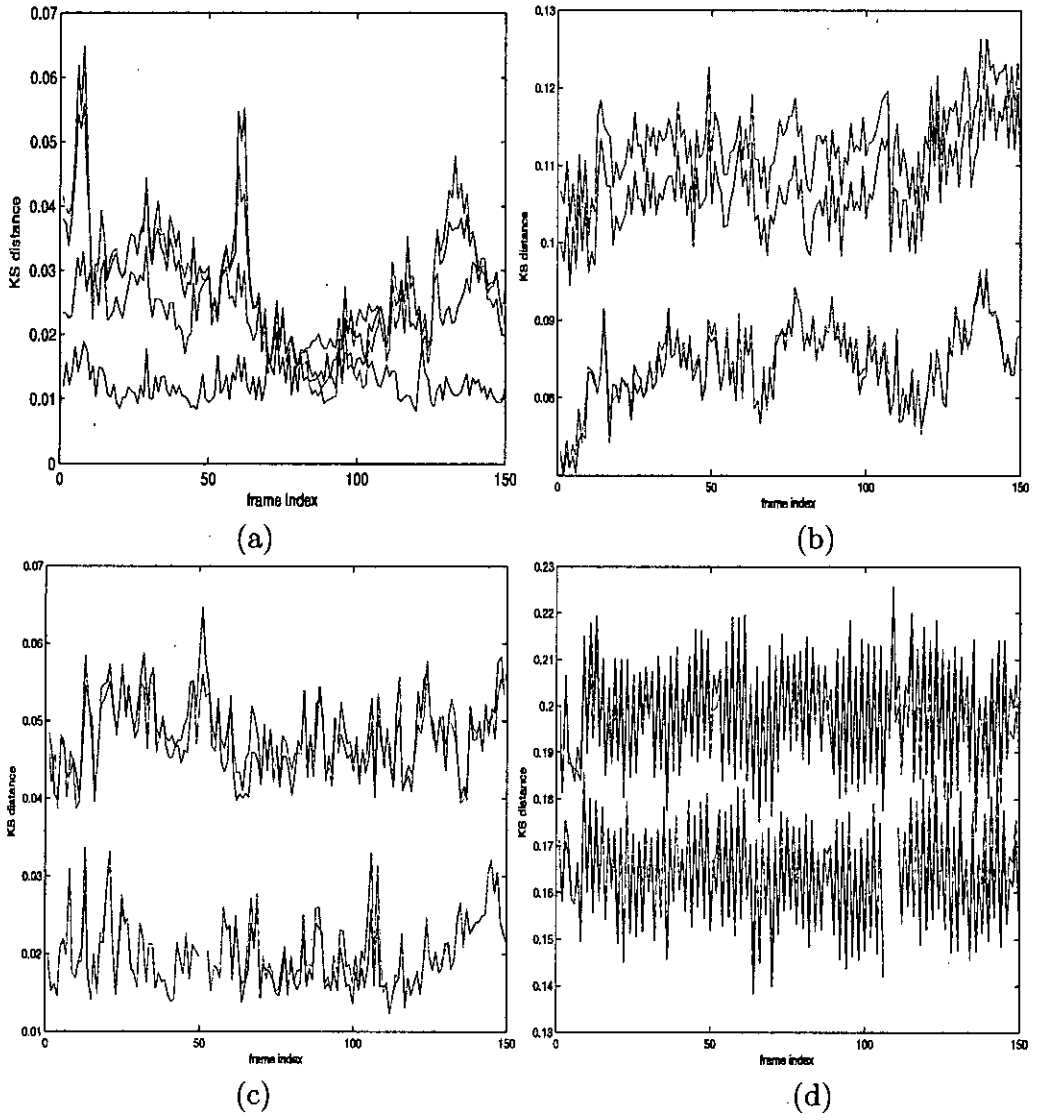


Fig. 4.3: Plot of the values of the K-S distance for various block-DCT coefficients of the *Salesman*: (a) C_{01}, (b) C_{10}, (c) C_{22} and (d) C_{50}. Plots of the Laplacian, SNIG, GG and BKF PDFs are shown using red, green, blue and magenta colored lines.

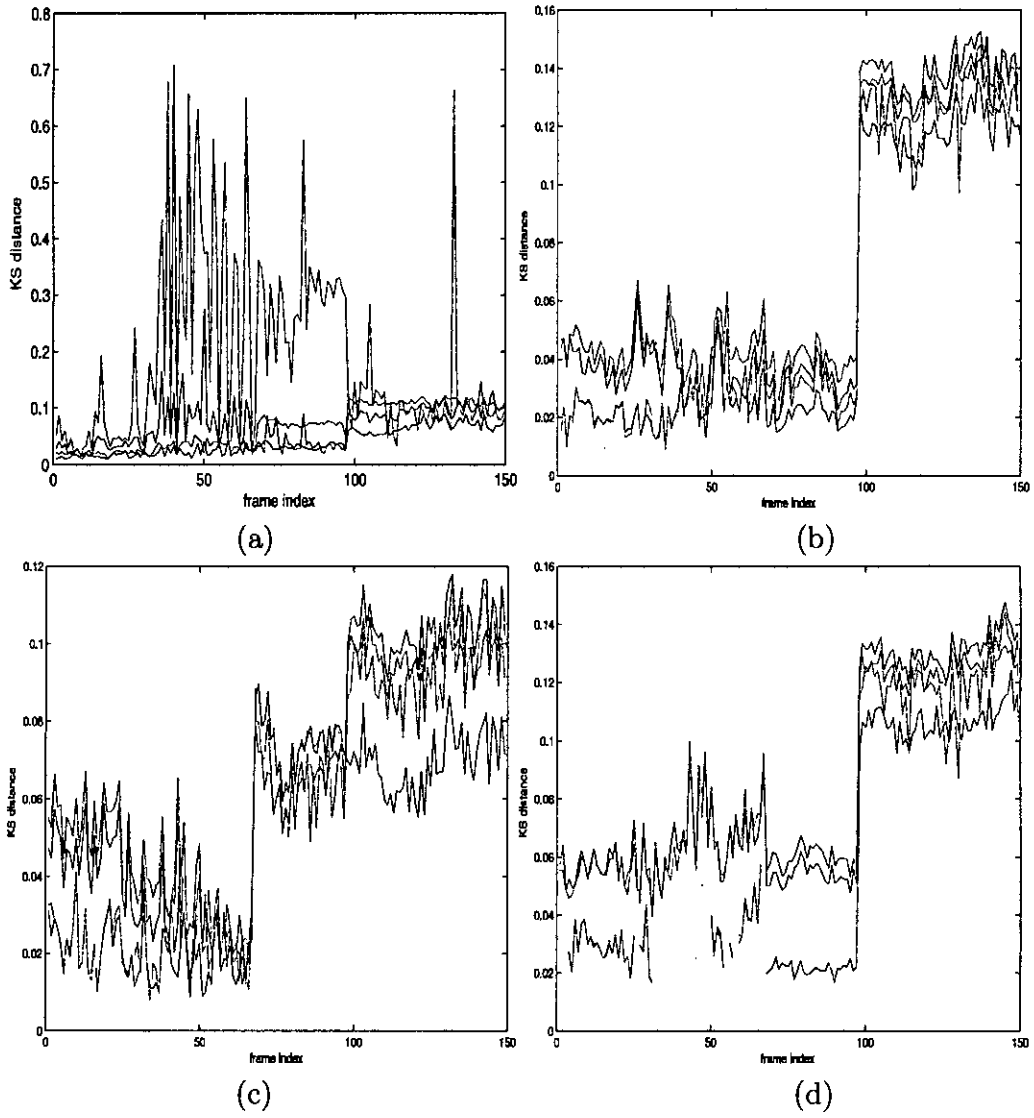


Fig. 4.4: Plot of the values of the K-S distance for various block-DCT coefficients of the *Tennis*: (a) C_{01}, (b) C_{10}, (c) C_{22} and (d) C_{50}. Plots of the Laplacian, SNIG, GG and BKF pdfs are shown using red, green, blue and magenta colored lines.

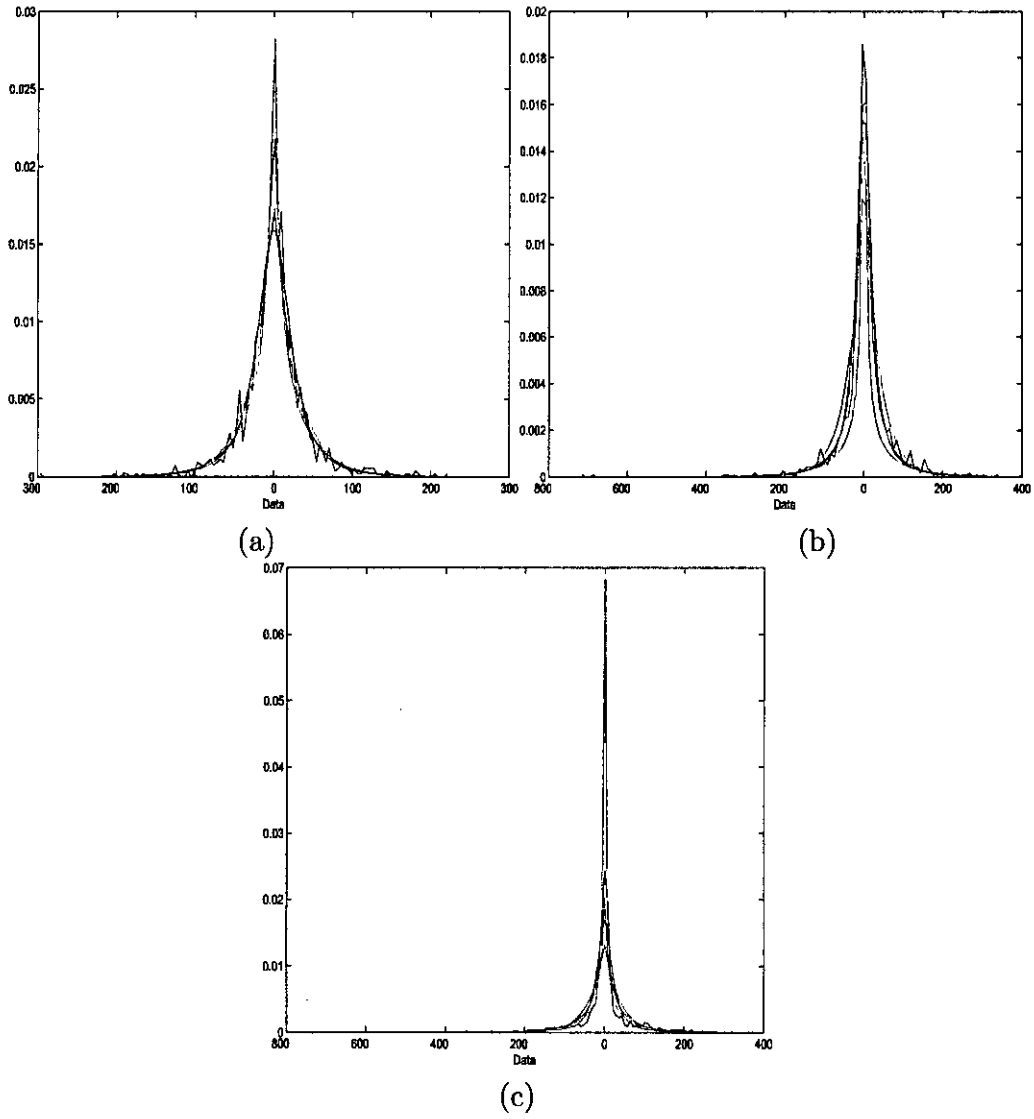


Fig. 4.5: Plots of the empirical, SNIG, Laplacian, GG and BKF pdfs for the C_{01} block-DCT coefficients of the *Tennis* video sequence. (a) 25^{th} frame, (b) 85^{th} frame and (c) 105^{th} frame. Plots of the Laplacian, SNIG, GG and BKF pdfs are shown using red, green, blue and magenta colored lines.

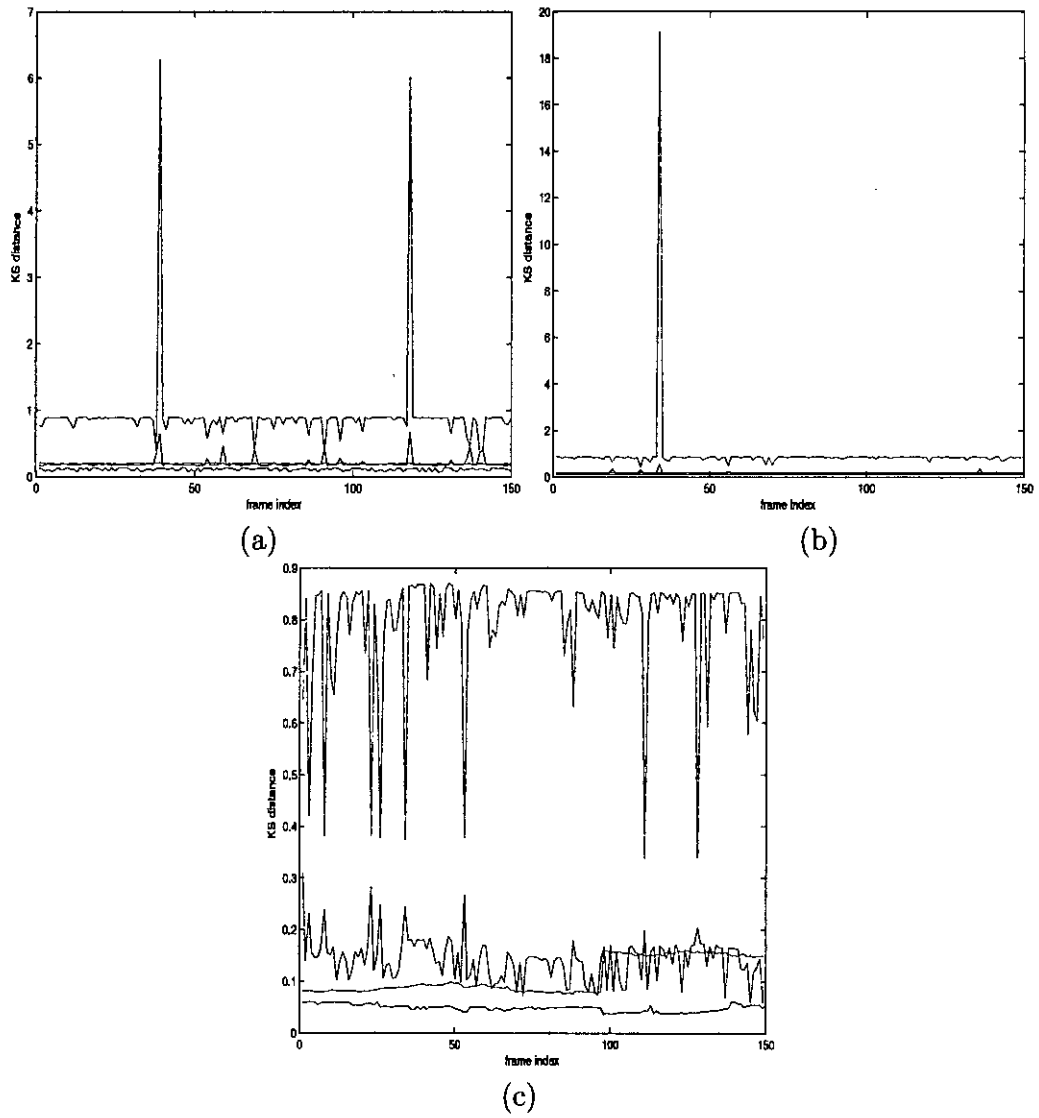


Fig. 4.6: Plot of the values of the K-S distance for the full-frame DCT coefficients of different video sequences : (a) *Miss America*, (b) *Salesman* and (c) *Tennis*. Plots of the Laplacian, SNIG, GG and BKF pdfs are shown using red, green, blue and magenta colored lines.

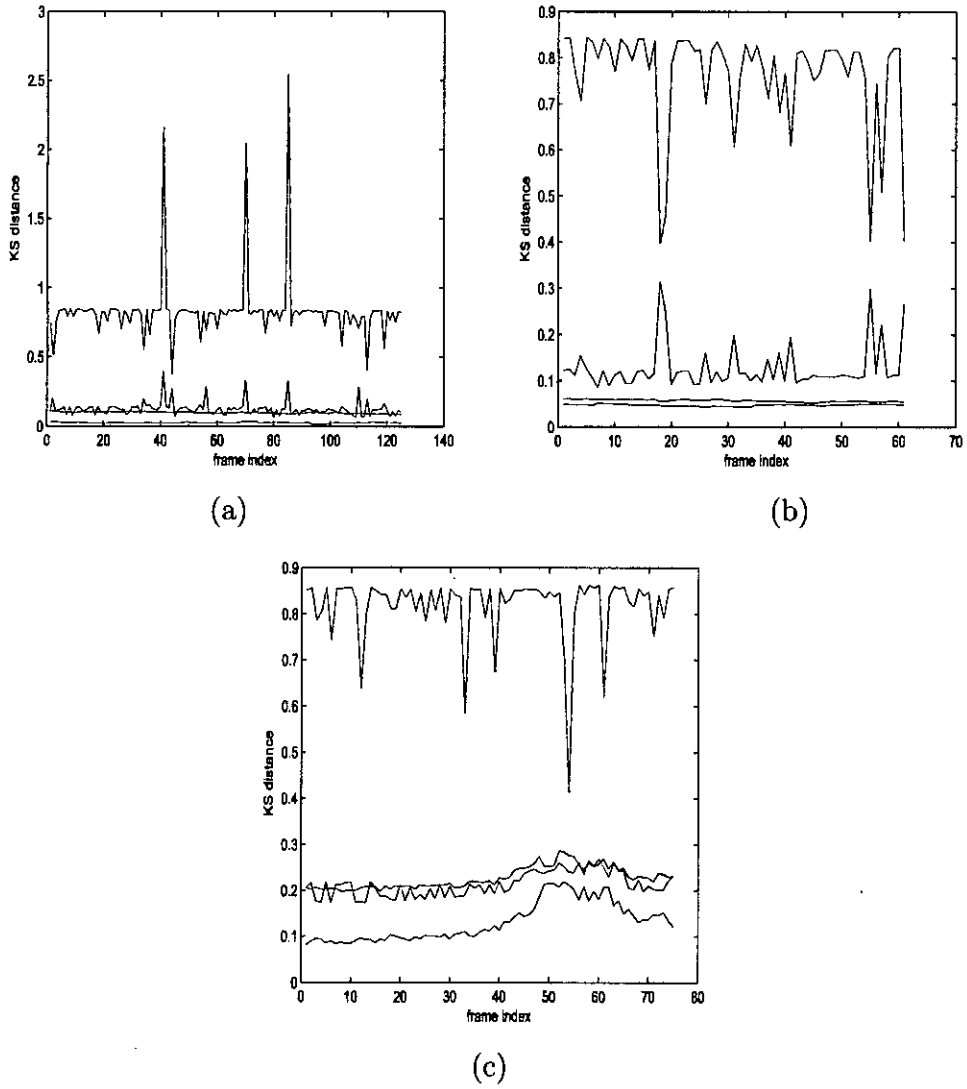


Fig. 4.7: Plot of the values of the K-S distance for the full-frame DCT coefficients of different video sequences : (a) *Football*, (b) *Garden* and (c) *Susie*. Plots of the Laplacian, SNIG, GG and BKF pdfs are shown using red, green, blue and magenta colored lines.

Chapter 5

Conclusions

5.1 Summary

Watermarking is one of the most prominent technique of today in data protection schemes. Continuous research is going on for the development of more robust watermark generator and more effective watermark detector. As the performance of a watermark detector depends on the accuracy of the data model used in detector design, experiments are also going on in this regard. In this thesis, a novel watermark detector has been developed for digital images using SNIG model.

Different types of watermark detectors have been proposed so far in literature. Frequency domain detectors is the most popular and common among the existing detectors. Considering the wide range of commercial application, DCT domain is chosen for the detector developed in this thesis.

The development SNIG watermark detector has been presented in Chapter 3. First the accuracy of the SNIG model is verified through experimental modeling of the data of some natural images. The result demonstrates that this model describes the image data with more perfection than the other statistical models (Laplacian, generalized Gaussian, Bessel-K and Cauchy).Therefore, it is evident that the SNIG model more accurately describes the DCT coefficients of interest.

After data modeling, a mathematical structure for development of the SNIG detector has been presented. The blind detector design is based on binary hypothesis test. After developing the detector, its performance is analyzed with that of other detectors. The images that have been used for test are embedded with watermark both in full frame and in blocks. The detector performance is

first compared in terms of the corresponding ROC curves. For most of the natural images, SNIG shows higher detection probability for a given value of false alarm probability, which indicates better performance. Then, the performance is evaluated for a wide range of watermark strength variation. The watermark power is controlled by varying the value of WDR. The lower value of WDR corresponds to weaker and more invisible watermarks. Here also, the SNIG detector proves to be better detector even in case of weaker watermarks. The overall result verifies the improved performance of the SNIG detector than the others.

In Chapter 4, the application of the SNIG model has been demonstrated for digital video. The results prove SNIG as a highly suitable prior for modeling the intra-frame DCT coefficients. Here, the performance of video data modeling of the SNIG prior is compared with that of the Laplacian, GG and BKF pdfs. The lower values of the K-S distance corresponding to the SNIG PDF compared to those of the other pdfs for different frames suggests SNIG as more suitable prior for modeling the DCT coefficients of digital video sequences.

5.2 Suggestions for Future Work

From the work presented in Chapter 4 it is evident that, the SNIG distribution exhibits superiority in data modeling not only for still images, but also in case of video sequences. Since the performance a certain pdf in data coefficient modeling directly relates to the performance of the watermark detector based on that pdf, it can be suggested that, SNIG will work as a better watermark detector for digital video also. Besides, this dissertation did not include quantization attack after watermarking the images. The performance of the SNIG detector can be further analyzed with several kinds of attacks taken into account.

Last of all, research can be continued for the design of a watermark decoder based on the SNIG modeling of the DCT coefficients. This decoder could be incorporated as the second part of a watermark verification and extraction system that also includes a watermark detector. Taking the improved performance of the proposed SNIG detector into consideration, such a decoder is also expected to give good results. This may consequently lead to the design of an integrated watermark verification and extraction system with better performance than the existing schemes of today.

References

[1] A. Briassouli, P. Tsakalides, and T. Stouraitis, "Hidden messages in heavy-tails: DCT-domain watermark detection using alpha-stable models," *IEEE Trans. on Multimedia*, vol. 7, no. 4, pp. 700–715, 2005.

[2] M. B. A. Piva, F. Bartolini, and V. Cappellini, "Application-driven requirements for digital watermarking technology," in *Proc. of Europ. Multimedia Microproc. System and Electronic Commerce Conf. and Exhibition*, vol. 9, Bordeaux, France, pp. 54–58, 2002.

[3] M. Barni, F. Bartolini, and A. Piva, "Digital watermarking of visual data: state of the art and new trends," in *Proc. of European Signal Processing Conference*, pp. 1657–1664, 2000.

[4] C. T. Hsu and J. L. Wu, "DCT-based watermarking for video," *IEEE Trans. on Consumer Electronics*, vol. 44, no. 1, pp. 206–216, 1998.

[5] H. Berghel and L. O'Gorman, "Protecting ownership rights through digital watermarking," *Computer Magazine*, pp. 101–103, July 1996.

[6] A. M. Bruckstein and T. J. Richardson, "A holographic transform domain image watermarking method," *Circuits, Systems, and Signal Processing*, vol. 17, no. 3, pp. 361–389, 1998.

[7] R. Chandramouli and N. D. Memon, "On sequential watermark detection," *IEEE Trans. on Signal Processing*, vol. 51, no. 4, pp. 1034–1044, 2003.

[8] R. Chandramouli, N. D. Memon, and M. Rabbani, "Digital watermarking," *Encyclopedia of Imaging Science and Technology*, 2002.

[9] Q. Cheng and T. S. Huang, "An image watermarking technique using pyramid transform," in *Proc. of ACM international conference on Multimedia*, pp. 319–328, 2001.

[10] J. R. Hernandez, M. Amado, and F. Perez-Gonzales, "DCT domain watermarking techniques for still images: detector performance analysis and a new structure," *IEEE Trans. on Image Processing*, vol. 9, no. 1, pp. 55–68, 2000.

[11] G. F. Elmasry and Y. Q. Shi, "Maximum likelihood sequence decoding of digital image watermarks," in *Proc. of SPIE*, vol. 3657, San Jose, CA, pp. 425-436, 1999.

[12] K. A. Birney and T. R. Fischer, "On the modeling of DCT and subband image data for compression," *IEEE Trans. on Image Processing*, vol. 4, no. 2, pp. 186-193, 1995.

[13] R. J. Clarke, *Transform Coding of Images.* New York, USA: Academic, 1985.

[14] P. Georgiou, P. Tsakalides, and C. Kyriakakis, "Alpha-stable modeling of noise and robust time-delay estimation in the presence of impulsive noise," *IEEE Trans. on Multimedia*, vol. 1, no. 3, pp. 291–301, 1999.

[15] G. A. Tsihrintzis and C. L. Nikias, "Performance of optimum and suboptimum receivers in the presence of impulsive noise modeled as an alpha-stable process," *IEEE Trans. on Communications*, vol. 43, no. 3, pp. 904–914, 1995.

[16] P. Tsakalides, *Array Signal Processing with Alpha-Stable Distributions.* Los Angeles, CA: Ph.D. dissertation, Univ. Southern California, 1995.

[17] M. I. H. Bhuiyan, M. O. Ahmad, and M. N. S. Swamy, "Modeling of the DCT coefficients of images," in *Proc. of IEEE International Symposium on Circuits and Systems*, pp. 272 – 275, 2008.

[18] I. J. Cox, M. L. Miller, and A. McKellips, "Watermarking as communications with side information," in *Proc. of IEEE*, vol. 87, no. 7, pp. 1127–1141, 1999.

[19] I. J. Cox, M. L. Miller, and J. Bloom, "Informed embedding: Exploiting image and detection information during watermark insertion," in *Proc. of IEEE Int. Conf. Image Processing*, no. 7, Vancouver, Canada, 2000.

[20] J. R. Hernandez, F. Perez-Gonzales, J. M. Rodriguez, and G. Nieto, "Performance analysis of a 2-D-multipulse amplitude modulation scheme for data hiding and watermarking of still images," *IEEE Journal on Selected Areas of Communications*, vol. 4, no. 16, pp. 510-524, 1998.

[21] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," in *Proc. of IEEE*, vol. 87, no. 7, pp. 1108-1126, 1999.

[22] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, and A. Piva, "DWT-based technique for spatio-frequency masking of digital signatures, in security and watermarking of multimedia contents," in *Proc. of SPIE*, San Jose, CA, pp. 31–39, 1999.

[23] F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask building for perceptually hiding frequency embedded watermarks," in *Proc. of IEEE Int. Conf. Image Processing*, vol. 1, Chicago, IL, 1998.

[24] H. V. Poor, *An Introduction to Signal Detection and Estimation.* New York, USA: Springer-Verlag, 1994.

[25] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "Threshold selection for correlation-based watermark detection," in *Proc. of COST254 Workshop*, Laquila, Italy, April 1998.

[26] ——, "Exploiting the cross-correlation of RGB-channels for robust watermarking of color images," in *Proc. of IEEE Int. Conf. Image Processing*, vol. 1, Kobe, Japan, pp. 306–310, 1998.

[27] M. Barni, F. Bartolini, V. Cappellini, A. Piva, and F. Rigacci, "A MAP identification criterion for DCT-based watermarking," in *Proc. of European Signal Processing Conference*, Rodos, Greece, pp. 17–20, 1998.

[28] A. D. Rosa, M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "Optimum decoding of non-additive full frame DFT watermarks," in *Proc. of Information Hiding Workshop*, Dresden, Germany, pp. 159-171, 1999.

[29] J. Oostveen, T. Kalker, and J. P. Linnartz, "Optimal detection of multiplicative watermarks," in *Proc. of European Signal Processing Conference*, Tampere, Finland, pp. 17–20, 2000.

[30] R. C. Reininger and J. D. Gibson, "Distributions of the two-dimensional DCT coefficients for images," *IEEE Trans. on Communications*, vol. 31, no. 6, pp. 835–839, 1983.

[31] T. M. Ng and H. K. Garg, "Maximum-likelihood detection in DWT domain image watermarking using laplacian modeling," *IEEE Signal Processing Letters*, vol. 12, no. 4, pp. 285–288, 2005.

[32] L. Boubchir and J. M. Fadili, "Bayesian denoising based on the MAP estimation in wavelet-domain using Bessel k form prior," *Proc. of IEEE International Conference on Image Processing*, vol. 1, pp. 113–116, 2005.

[33] A. Briassouli and M. G. Strintzis, "Locally optimum nonlinearities for DCT watermark detection," *IEEE Trans. on Image Processing*, vol. 13, no. 12, pp. 1604–1617, 2004.

[34] F. Muller, "Distribution shape of two-dimensional DCT coefficients of natural images," *Electron. Lett.*, vol. 29, pp. 1935–1936, 1993.

[35] E. Y. Lam and J. W. Goodman, "A mathematical analysis of the DCT coefficient distributions for images," *IEEE Trans. on Image Processing*, vol. 9, pp. 1661–1666, 2000.

[36] J. C. et. al., "Image probability distribution based on generalized gamma function," *IEEE Signal Processing Letters*, vol. 12, pp. 325–328, 2005.

[37] R. Adler, R. Feldman, and M. S. Taqqu, *A Guide to Heavy Tails: Statistical Techniques and Applications*. Boston, MA, USA: Birkhauser, 1998.

[38] A. Achim, A. Bezerianos, and P. Tsakalides, "Novel bayesian multiscale method for speckle removal in medical ultrasound images," *IEEE Trans. on Medical Imaging*, vol. 20, no. 8, pp. 772–783, 2001.

[39] J. Cardoso, "Infomax and maximum likelihood for blind source separation," *IEEE Signal Processing Letters*, vol. 4, no. 4, pp. 112–114, 1997.

[40] V. Capellini, M. Barni, F. Bartolini, and A. Piva, "A DCT-domain system for robust watermarking," *Signal Processing*, vol. 66, pp. 357–372, 1998.

[41] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust data hiding for images," in *Proc. of IEEE Digital Signal Processing Workshop*, Loen, Norway, pp. 37–40, 1996.

[42] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum perceptual watermarking for images, audio and video," *IEEE Trans. on Image Processing*, vol. 6, no. 4, pp. 1673–1687, 1997.

[43] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," in *Proc. of IEEE*, vol. 87, no. 7, pp. 1197–1207, 1999.

[44] J. G. Proakis, *Digital Communications.* New York: McGraw-Hill, 1995.

[45] G. K. Wallace, "The JPEG still picture compression standard," *IEEE Trans. on Consumer Electronics*, vol. 38, no. 1, pp. 18–34, 1992.

[46] M. Nelson, *The Data Compression Book.* San Mateo, CA: M&T Books, 1992.

[47] S. M. M. Rahman, M. O. Ahmad, and M. N. S. Swamy, "Statistical detector for wavelet-based image watermarking using modified GG PDF," in *Proc. of IEEE International Symposium on Circuits and Systems*, pp. 18–34, 2008.

[48] J. Fadili and L. Boubchir, "Analytical form for a Bayesian wavelet estimator of images using the Bessel k form densities," *IEEE Trans. Image processing*, vol. 14, pp. 231–240, 2005.

[49] T. Sikora, *Digital video coding standards and their role in video communications.* IOS Press, 1999.

[50] Y. Wang, J. Ostermann, and Y. Zhang, *Video Processing and Communication.* USA: Prentice Hall Ltd., 2002.

[51] M. I. H. Bhuiyan and R. Rahman, "Modeling of the video DCT coefficients," in *Proc. of IEEE ICECE*, Dhaka, Bangladesh, pp. 417–421, 2008.

[52] R. L. Joshi and T. R. Fisher, "Comparison of generalized gaussian and laplacian modeling in DCT image coding," *IEEE Signal Processing Letters*, vol. 2, pp. 81–82, 1995.

[53] S. Bossi, F. Mapelli, and R. Lancini, "Semi-fragile watermarking for video quality evaluation in broadcast scenario," in *Proc. of IEEE International Conference of Image Processing*, 2005.