

WATERMARKING IN BAND-LIMITED CHANNELS

APPROVED BY SUPERVISORY COMMITTEE:

Dr. Aria Nosratinia, Chair

Dr. John P. Fonseka

Dr. Philip Loizou

Copyright 2002

Vimal Thilak

All Rights Reserved

To my parents

WATERMARKING IN BAND-LIMITED CHANNELS

by

VIMAL THILAK, B.E.

THESIS

Presented to the Faculty of the Graduate School of

The University of Texas at Dallas

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

THE UNIVERSITY OF TEXAS AT DALLAS

December 2002

ACKNOWLEDGEMENTS

I thank my advisor Dr. Aria Nosratinia for providing me with the opportunity to work as graduate student with him over the past two years. I express my gratitude to Dr. Nosratinia for his guidance, support and confidence he has shown in my work. I also thank him for instilling a sense of curiosity to learn new things in me.

I would like to thank Dr. John Fonseka and Dr. Philip Loizou for serving on my supervisory committee. I express my gratitude for their helpful suggestions and comments that assisted me in improving the presentation of this thesis.

I would like to thank Ahmad Hedayat for sharing his computer programs and his expertise on trellis coded modulation with me.

I would also like to thank my colleagues of the Multimedia Communications Laboratory, Todd, Ahmad, Mohammad, Ramky, Hong Bo, Nikhil and Shahab, for their timely help and support.

I would like to thank my family for their constant encouragement and support.
December, 2002.

WATERMARKING IN BAND-LIMITED CHANNELS

Publication No. _____

Vimal Thilak, M.S.E.E.

The University of Texas at Dallas, 2002

Supervising Professor: Aria Nosratinia

Watermarking consists of embedding an information bearing signal ,called a watermark, within another signal such as an image or a video signal. The embedding process should not degrade the perceptual quality of the host signal. The watermarked signal may be subjected to either malicious or unintentional interference, which distorts the watermark. The embedded information must be extracted despite the presence of this interference.

The watermarking communication channel is both power limited and band-limited . The power limit arises due to the requirement for imperceptible watermark. The bandwidth limit arises due to the low-pass nature of multimedia signals such as images, audio and video. While the power limit has clear implications in watermark design, the bandwidth limitation has not been fully considered in existing watermarking algorithms. This thesis proposes techniques that, by appropriately addressing the band-limited nature of watermarking, achieve improvements in performance.

This thesis has three main contributions. The first part addresses the issue of error control in watermarking. We propose coded-modulation techniques for watermarking that achieve high reliability without loss of information rate. It is shown that the proposed method provides a better rate-performance trade off compared to existing methods.

The second part addresses intersymbol interference (ISI) in watermarking. We present a method to design ISI-free signals and show that the proposed method outperforms existing methods that are not ISI-aware.

The final part of this thesis investigates equalization in watermarking systems. We design a linear equalizer to reduce the effects of ISI for watermarking systems.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	v
ABSTRACT.....	vi
LIST OF FIGURES.....	x
CHAPTER 1. INTRODUCTION.....	1
1.1 Motivation.....	1
1.2 Watermarking Requirements.....	3
1.3 Classes of Embedding Methods.....	6
1.3.1 Modulation based Watermarking Algorithms.....	6
1.3.2 Watermarking with side information.....	7
1.3.3 Game theoretic watermarking.....	9
1.4 Thesis Outline.....	9
CHAPTER 2. EFFICIENT ERROR CONTROL FOR DIGITAL WATERMARK- ING WITH TRELLIS CODED MODULATION.....	12
2.1 Introduction.....	12
2.2 Watermarking by TCM.....	13
2.2.1 Baseline System.....	14
2.2.2 TCM Scheme.....	15
2.3 Experimental Results.....	18
CHAPTER 3. SIGNAL DESIGN FOR ROBUST WATERMARKING ON ISI CHANNELS.....	26
3.1 Introduction.....	26
3.2 Signal Design via the Nyquist criterion.....	29
3.2.1 Review of Eigenfilter Design.....	31
3.3 Watermarking with Nyquist Pulses.....	34
3.4 Experiments.....	36

CHAPTER 4. TWO METHODS TO IMPROVE THE ROBUSTNESS OF WATERMARKING IN BAND-LIMITED CHANNELS	42
4.1 Error Control for Band-Limited Watermark Signals	42
4.2 Watermarking in Unknown Band-Limited Channels	43
CHAPTER 5. CONCLUSIONS	50
REFERENCES	52
VITA	

LIST OF FIGURES

1.1	Figure illustrating the relationship between imperceptibility, robustness and payload. it is clear that there is a tradeoff between the three basic requirements.	4
1.2	Block diagram of a typical modulation based watermarking system.	6
1.3	Block diagram of a watermarking system that utilizes side information during the embedding process.	8
1.4	An example quantization index modulation (QIM) system.	9
2.1	Block diagram of a watermarking system with TCM.	14
2.2	Block diagram of the TCM transmitter	15
2.3	Set partitioning of 4-PAM signal set.	16
2.4	Block diagram of the four-state TCM transmitter	17
2.5	Trellis for the four-state encoder.	17
2.6	Block diagram of the eight-state TCM transmitter	18
2.7	Trellis for the eight-state encoder.	19
2.8	Block diagram of blind extraction scheme	19
2.9	Block diagram of informed extraction scheme	20
2.10	BER performance of TCM and coding followed by expanded modulation in a 512×512 host (Lena).	21
2.11	BER performance of TCM versus baseline system with a payload of 484 bits in a 512×512 host (Lena).	21
2.12	BER performance with blind and informed receivers in a 512×512 host (Lena).	22
2.13	BER performance with 4-state and 8-state TCM codes in a 512×512 host (Lena).	23
2.14	BER performance of TCM and baseline system in a 1024×1024 host (Stream).	23
2.15	BER performance of TCM and baseline system in a 512×512 host (Tiffany).	24
2.16	MMSE estimated decision boundaries versus perfect knowledge of the same.	24

2.17	Decision boundaries estimated from demodulated data.	25
3.1	Periodograms illustrating the high interference around the DC regions of typical images.	27
3.2	Periodograms illustrating the insignificant energy regions of typical images	28
3.3	Plot of the watermark spectrum and the image spectrum.	30
3.4	Magnitude spectrum of the watermarking pulse.	30
3.5	Transmitter of the proposed scheme.	34
3.6	Block diagram of blind extraction scheme.	37
3.7	Block diagram of informed extraction scheme.	37
3.8	Performance comparison in the informed receiver case with a 1024 x 1024 host.	38
3.9	Performance comparison in the blind receiver case with a 1024 x 1024 host (Man).	39
3.10	Performance comparison in the blind receiver case with a 1024 x 1024 host (Stream).	39
3.11	Performance comparison in the informed receiver case with a 512 x 512 host.	40
3.12	Performance comparison in the blind receiver case with a 512 x 512 host (Peppers).	41
3.13	Performance comparison in the blind receiver case with a 512 x 512 host (Tiffany).	41
4.1	Block Diagram of a watermarking system with TCM	42
4.2	Trellis of our TCM encoder	43
4.3	BER performance of TCM and uncoded system in a 1024 x 1024 host. (Man).....	44
4.4	BER performance of TCM and uncoded system in a 1024 x 1024 host. (Stream)	44
4.5	Principle of inverse filtering.	45
4.6	Block diagram of a watermarking system employing a equalizer	46
4.7	Performance comparison with and without equalizers in a 1024 x 1024 host. (Man)	47
4.8	Performance comparison with and without equalizers in a 1024 x 1024 host. (Stream)	48

4.9	Block diagram of a watermarking system with equalizer and error control	48
4.10	Performance comparison illustrating the coding gain due to TCM in a 1024 x 1024 host. (Man)	49
4.11	Performance comparison illustrating the coding gain due to TCM in a 1024 x 1024 host. (Stream)	49

CHAPTER 1

INTRODUCTION

Watermarking consists of embedding an information bearing signal within data signals such as images and video [17, 36, 26]. The embedding must not overly distort the host signal. At the same time, the embedded signal must be robust to unintentional or malicious operations. We review the need for watermarking and also some of its important requirements and applications.

1.1 Motivation

The use of digital data has become popular due to the availability of inexpensive resources including computers, software and the Internet. It is now possible to store and transmit digital media with high reliability. It is also possible effortlessly to modify and replicate digital media with modern signal processing tools. Digital multimedia data processing is preferred over its analog counterpart in most applications.

Digital watermarking has been used in a number of applications [11, 17, 36, 26]. Some important applications are:

1. **Copyright Protection:** The owner of multimedia data may embed a watermark that conveys copyright and ownership information. The watermark can prove ownership in court.

Watermarking can be used in conjunction with encryption [24, 25] to provide efficient copyright protection. Encryption ensures that the digital data is avail-

able to only the authorized users, i.e, users who have access to the decryption key. Since the data must be decrypted to be used, it is vulnerable at some point in the system. Watermarking can complement digital encryption, thereby ensuring that the owners always have some form of control over their multimedia data.

2. **Copy Control:** A watermark can be used in a copy control system to enable or disable copying. The recording device may decide to allow or inhibit recording depending on the information conveyed by the watermark. Such a system has been proposed for allowing a copy once feature in digital video disc recorders [3]. A similar feature can be incorporated into playback devices [31].
3. **Fingerprinting:** The owner of multimedia data embeds a watermark that is unique to a particular copy (user) of the work. The watermark acts as a digital fingerprint since it is associated with a unique copy of the work. This can be a useful tool in tracing the source of illegal copies of the work. The paper by Cox et. al [11] provides further applications of fingerprinting.
4. **Broadcast Monitoring:** In these applications, a watermark is embedded in advertisements that are aired by broadcasting television stations. An automated monitoring system can then track the number of times the advertisement is aired on television. This information can be used by the advertisers for book keeping purposes.
5. **Authentication:** We may need to ensure the authenticity or integrity of multimedia signals in certain applications such as legal cases and medical imaging. Fragile watermarks [50] are used to indicate whether the data has been altered. These watermarks can also provide information about the locations of the host

that has undergone alterations. Algorithms that are robust to compression such as JPEG but not to intentional tampering have been proposed [29, 28].

6. Meta-data Tagging: Meta-data convey auxiliary information about the host multimedia signal. Embedding information related to a patient in medical images or a time stamp in photographs are typical applications of meta-data embedding. Existing methods include embedding the information in the header of the data file and in the perceptually unimportant regions of signals like images and video. However, these methods are vulnerable to simple operations such as changing of the file format and image cropping.

Watermarking is a natural and effective way to transmit meta-data. By designing a robust algorithm, we may guarantee that the embedded data is available even after the host signal has undergone alterations.

7. Error Concealment in Images and Video: Data hiding for error concealment has been proposed by Robie and Mersereau [39]. The data required for error correction is embedded as a watermark and transmitted to the video decoder. The decoder uses this data in conjunction with error concealment techniques to recover from channel errors.

1.2 Watermarking Requirements

A watermark must be robust, secure and imperceptible. The design of a watermarking algorithm usually involves a tradeoff among the above requirements. The requirements of a algorithm are described below.

1. Imperceptibility: Many applications involving multimedia hosts such as audio, images and video require unobtrusive watermarks. We require that the watermarked host and the original host be perceptually indistinguishable. This

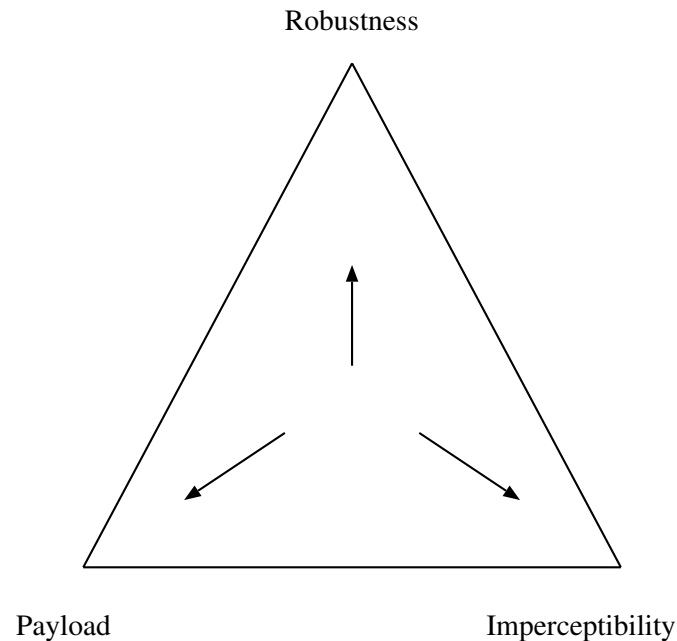


Figure 1.1. Figure illustrating the relationship between imperceptibility, robustness and payload. it is clear that there is a tradeoff between the three basic requirements.

requirement arises due to need to preserve the perceptual quality and consequently the commercial value of the multimedia host.

Podilchuk and Zeng [37] have developed a method that exploits the properties of the Human Visual System (HVS). The idea [37] is to limit the changes in this host due to embedding to just below the threshold of perception to render the watermark invisible. Podilchuk and Zeng calculated the threshold of visual perception by computing the Just Noticeable Differences (JND). The paper by Vleschouwer et. al [47] overviews research in perceptual watermarking.

2. **Robustness:** Robustness refers to the ability of the watermark to be resilient to interference. The information must be extracted reliably from a corrupted watermark. The interference may be either malicious or unintentional. The unintentional interference may arise from content processing such as compression, filtering, re-sampling, digital-to-analog (D/A) and analog-to-digital (A/D) con-

versions. On the other hand, a knowledgeable attacker may intentionally try to distort or completely destroy the watermark. Examples of intentional attacks include collusion and averaging attacks wherein an unwatermarked host is constructed from several copies of the watermarked host [41, 48].

Attack modeling for digital watermarking is an active research area. We refer the reader to the paper by Voloshynovskiy et. al [48] for a tutorial on attack modeling and countermeasures.

3. **Payload:** The amount of information to be conveyed by a watermark depends on intended application. Applications such as data authentication and fingerprinting require only one bit of embedded information since it is required only to verify whether a given watermark is present or not. Applications such as copyright protection and meta-data tagging require more than one bit of information to be embedded in the host. Some have suggested that at least 128 bits of information are needed for efficient copyright protection [26].
4. **Oblivious and Non-Oblivious Watermarking:** In some applications such as broadcast monitoring, it is possible for the watermark extraction algorithm to have a copy of the original (unwatermarked) signal. This scenario is referred to as informed or non-blind watermarking. Oblivious or blind watermarking refers to the case wherein the information is extracted without the knowledge of the original host signal.

Figure 1.1 illustrates the relationship between robustness, imperceptibility and payload requirements of a watermarking system. It is difficult to simultaneously meet these conflicting requirements in a watermarking system, the design of a watermarking algorithm involves a tradeoff between these requirements.

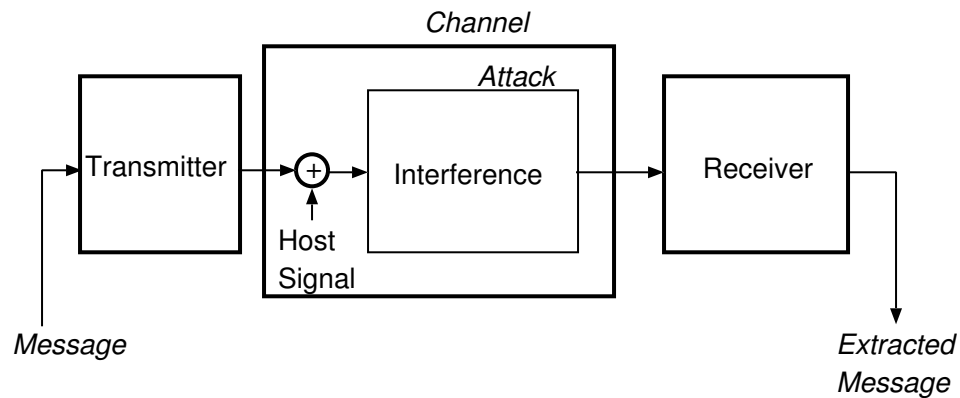


Figure 1.2. Block diagram of a typical modulation based watermarking system.

1.3 Classes of Embedding Methods

A number of embedding methods have been proposed in the literature [17, 36, 26]. We describe the general approaches adopted to design watermarking algorithms in the following. The interested reader is referred to [17, 36, 26] for a detailed description of the individual algorithms.

1.3.1 Modulation based Watermarking Algorithms

These popular algorithms are sometimes referred to as spread spectrum methods [10]. Figure 1.2 illustrates the block diagram of a typical modulation based watermarking algorithm. The watermark information is modulated with a predefined signal to form the watermark. The modulating signal is usually generated using a secret key. The watermark is then added to the host signal. The image and the attacks form an equivalent channel. The information must be extracted from the signal received at the output of this channel.

The secret key has two functions. First, to separate potential users by assigning a unique key to each user. Second, the secrecy required for watermarking applications is supplied via cryptographically secure keys.

This method works as follows:

$$I' = W + I \quad (1.1)$$

where I is the host (unwatermarked) signal, W is the watermark and I' is the watermarked signal. The algorithms proposed by Cox et. al [10], Tirkel et. al [42], Bender et al. [2] and Smith and Comiskey [40] belong to the additive class of embedding functions.

A number of variations of the modulation based methods have been proposed in the literature. Cox et.al propose a non-oblivious image watermarking algorithm [10]. A number of authors including Hernandez et al [19] and Honsinger and Rabbani [21] have proposed blind image watermarking algorithms. Podilchuk and Zeng [37] have proposed an interesting extension that exploits the properties of human perceptual systems to embed the watermarks more effectively.

The watermark may also be embedded in the transform domain e.g. in the discrete cosine transform (DCT) or the discrete wavelet transform (DWT) [18, 26, 36]. An advantage of transform domain embedding is that a statistical description of the transform coefficients of multimedia data, e.g. images, is available. This knowledge has been exploited to design optimal watermark detectors for DCT domain watermarking [18].

1.3.2 Watermarking with side information

In this approach, blind digital watermarking is treated as a communication with side information at the transmitter. Figure 1.3 shows a block diagram of such a communication system. This approach was proposed independently by Cox et al. [13] and Chen and Wornell [4, 7, 8] in 1999. Chen and Wornell brought the work of Costa [9] to the attention of the watermarking community. Costa [9] derives an

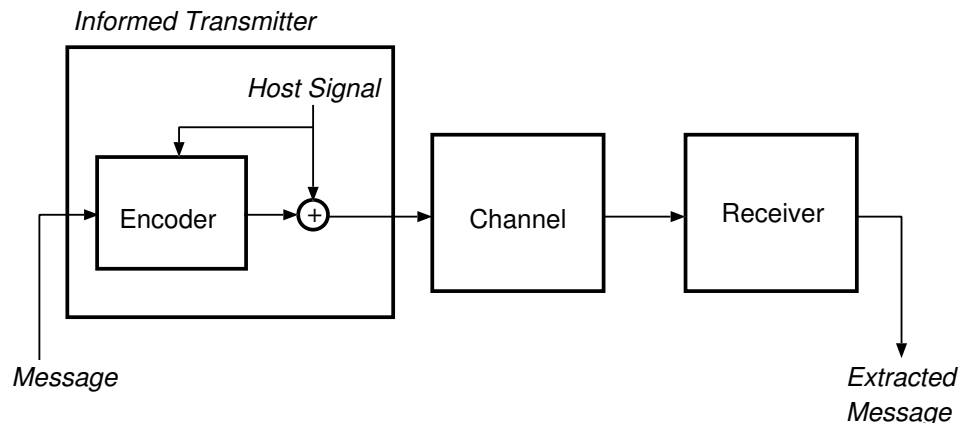


Figure 1.3. Block diagram of a watermarking system that utilizes side information during the embedding process.

expression for the capacity of a communications channel with a known source of interference, showing that the capacity of the communication system in Figure 1.3 is independent of the interference under certain conditions. Chen and Wornell [4, 7, 8, 6, 5] extend Costa’s result to watermarking and propose a class of algorithms which they call Quantization Index Modulation (QIM). A number of schemes based on Costa’s result have been reported by Eggers and Girod [14, 15] and by Miller et al. [33].

We provide an example of quantization index modulation (QIM). Figure 1.4 illustrates binary dither modulation. The information is embedded in the host through the choice of the quantizer. The host is quantized by the quantizer P to embed a “0” while the host is quantized by Q to embed a “1”. These quantizers can be pseudo-randomly dithered with a dither sequence known only to the encoder and the decoder. This provides the security required for watermarking applications.

The received signal is quantized to the nearest reconstruction point in the set $\{P \cup Q\}$. A reconstruction point belonging to P indicates a “0” was hidden while a point belonging to Q indicates that a “1” was hidden. The distortion due to embed-

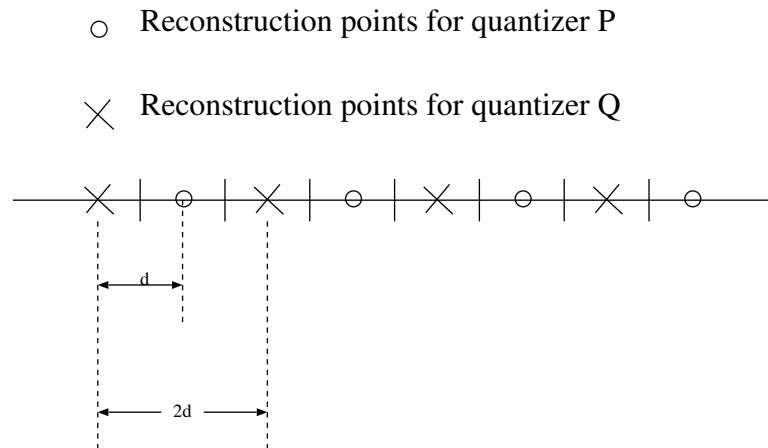


Figure 1.4. An example quantization index modulation (QIM) system.

ding is equal to the noise introduced by the quantization process. Multidimensional lattices can be used to obtain better rate-distortion trade-offs [8, 15].

1.3.3 Game theoretic watermarking

A game theoretic approach to watermarking has been proposed by Moulin and O’Sullivan [35] and by Eggers and Girod [15]. In this paradigm, the watermarking is viewed as a game between the embedder and the attacker. The embedder tries to maximize the amount of information that can be embedded while the attacker tries to minimize it. Moulin and O’Sullivan discuss the case of watermarking i.i.d Gaussian data [35]. Some interesting extensions to the above result have been reported by Su et. al [15] and by Moulin et. al [34].

1.4 Thesis Outline

This thesis proposes methods to improve the robustness of modulation based watermarking systems. Watermarking has been considered as a power constrained communications problem. The power limit arises naturally due to the need for maintaining the perceptual quality of the watermarked signals. A number of watermarking algo-

rithms such as those mentioned in section 1.3.1 are based on this paradigm. However, existing algorithms do not account for the band-limited nature of the watermarking channel. The contribution of this thesis is to design robust watermarking algorithms that account for the band-limited channel.

The limit on the bandwidth of the watermarking channel is due to (a) fundamental limit on the frequency of sampled data systems create a natural limit, (b) Operations that are low-pass in nature such as printing and scanning, and (c) Anticipating band-limited (low-pass) attacks. The low-pass operations do not affect the images, since images have a decaying spectrum. Thus the watermark spectrum must avoid the high frequency regions of the image where the watermark can be easily wiped out.

In Chapter 2, we consider the problem of improving the reliability of watermarking algorithms. Channel coding has been used to improve the performance of watermarking algorithms [20, 19, 16, 1]. Coding improves the performance of watermarking systems by adding redundancy in the form of parity. However, coding based on the Hamming distance is not suitable for band-limited channels. We propose the use of bandwidth efficient error control techniques such as trellis coded modulation (TCM) [43] in watermarking. Simulations demonstrate the effectiveness of TCM.

In Chapter 3, we consider the problem of improving the performance of watermarking algorithms in intersymbol interference (ISI) channels. It is well known that band-limited channels cause ISI [38] which impairs the performance of communication systems. A method to design ISI-free signals via the Nyquist criterion [38] is proposed in this chapter. We demonstrate the performance of our waveforms via experiments.

Extensions to the algorithms developed in Chapters 2 and 3 are proposed in Chapter 4. We design a system that uses TCM in conjunction with ISI-free signals.

A equalizer for watermarking systems is also presented in this chapter. Simulations verify the performance of our proposed systems.

In Chapter 5, we conclude this thesis and provide some possible directions for future work.

CHAPTER 2

EFFICIENT ERROR CONTROL FOR DIGITAL WATERMARKING WITH TRELLIS CODED MODULATION

Digital watermarking is equivalent to band-limited, power-limited digital communication. In this chapter, we point out a fundamental flaw in the use of error correcting codes that are based on Hamming distance *for the watermarking problem*. This flaw arises from the band-limited nature of the watermarking channel. Instead, we advocate that *only* coded-modulation techniques can provide efficient error control in band-limited watermarking channels. We demonstrate examples of Trellis Coded Modulation (TCM) applied in watermarking.

2.1 Introduction

Channel coding has been widely used to improve the reliability of communications systems. This idea extends to watermarking. Channel codes increase the minimum Hamming distance between codewords by appending bits to the message words. BCH codes have been proposed by Hernandez et al. [20]. The application of convolutional codes and the Viterbi algorithm to watermarking applications is presented in [16, 32]. Turbo codes and iterative decoding for watermarking have been proposed in [1, 16].

In this chapter, we point out a fundamental weakness of error control codes based on the Hamming distance in watermarking applications and also provide a remedy for this problem. The source of the weakness is the band-limited nature of watermarking channels. It is well known from digital communications [23] that in

band-limited channels, codes based on Hamming distance perform even worse than the uncoded case¹. Efficient error control for band-limited channels is made possible by trellis coded modulation (TCM) [43, 44, 45], which is based on maximizing the *Euclidean distance* between the coded sequences.

Why is the watermarking channel band-limited? We mention three reasons (a) fundamental (Nyquist) limit on the frequency of sampled data systems create a natural limit², (b) Operations that are low-pass in nature such as printing and scanning, and (c) Anticipating band-limited (low-pass) attacks. The low-pass operations do not affect the images since images have a decaying spectrum. The watermark spectrum must avoid the high frequency regions of the image where an attacker can wipe out the watermark with impunity.

Our literature search revealed that Cox et al. [12] proposed a method they call TCM. However, upon closer scrutiny, this turns out to be a misnomer. Their approach consists of concatenated but separable coding and modulation which is based on maximizing the free Hamming distance between the coded sequences, while TCM is based on maximizing the free Euclidean distance.

We build our TCM experiments on the baseline system of Honsinger and Rabbani [21]. Examples are provided to demonstrate the inefficacy of the codes based on the Hamming distance and effectiveness of coded modulation-schemes.

2.2 Watermarking by TCM

Figure 2.1 illustrates the block diagram of the proposed system. The information bits are encoded by the TCM encoder. The watermark is formed by modulating the encoded symbols. We employ the modulation scheme proposed by Honsinger

¹The comparisons are made on the basis of equal data rate and bandwidth.

²We restrict ourselves to digital watermarking.

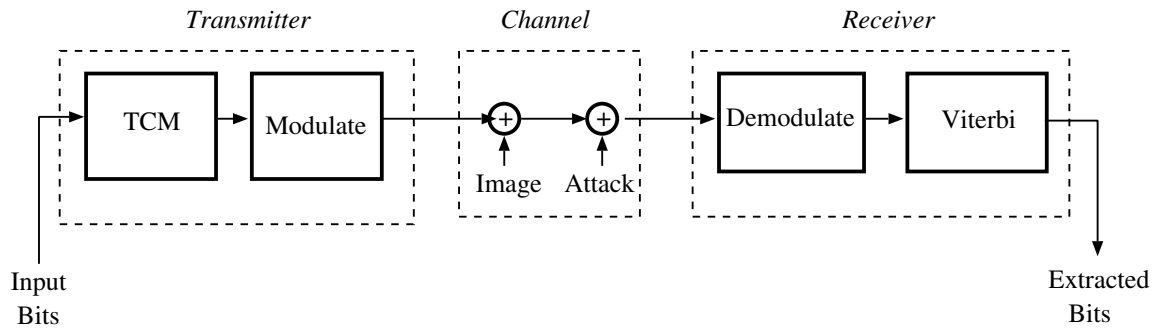


Figure 2.1. Block diagram of a watermarking system with TCM

and Rabbani [21] in our watermarking system. The information is extracted by demodulation and soft-decision Viterbi decoding.

2.2.1 Baseline System

We provide a brief description of the baseline system of Honsinger and Rabbani [21], whose modulation we borrow for our scheme. The symbols (either uncoded or coded) are placed in a two dimensional array M . M is modulated with a two dimensional pseudo-random phase signal C to form the watermark. The watermark is added to the host image I to form the watermarked image I' . The embedding is given by

$$I'(x, y) = \alpha(M(x, y) * C(x, y)) + I(x, y) \quad (2.1)$$

where (x, y) denotes the location of a sample, $*$ denotes circular convolution and α is the embedding strength. The design of C is described in [22].

The host image is tiled and (2.1) is repeated in all the tiles to improve the quality of the signal at the demodulator. The embedding strength α is maintained the same across all the tiles in our experiments.

At the receiver (extraction), the tiles are summed together before demodulation is performed. The demodulator is a matched filter matched to C .

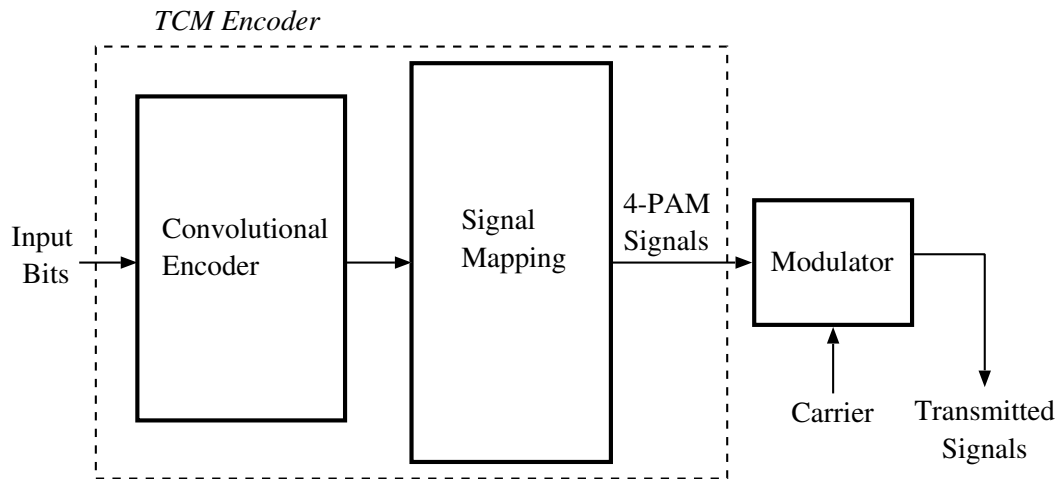


Figure 2.2. Block diagram of the TCM transmitter

2.2.2 TCM Scheme

Figure 2.2 illustrates the block diagram of the proposed transmitter. The information bits are encoded by a rate $k/(k+1)$ convolutional encoder. The resulting bits are mapped into signals chosen from an expanded signal constellation. The redundancy required for error control is obtained by employing this expanded modulation constellation. Finally, the watermark is formed by modulating the TCM encoded symbols with the pseudo-random phase signal as described in section 2.2.1.

The coding gain of TCM arises due to set partitioning [43] which maximizes the Euclidean distance between the coded sequences. Since the baseline scheme uses binary signaling, we expand the modulation constellation to 4-PAM. Figure 2.3 illustrates the partitioning of 4-PAM signals into two subsets B_0 and B_1 . The normalized minimum Euclidean distance of our sub-constellations ($d_{min} = 2$) is greater than the normalized minimum Euclidean distance of the parent constellation ($d_{min} = 1$), as shown in Figure 2.3.

The performance improvement provided by the coding system relative to the uncoded case is measured in terms of the asymptotic coding gain γ [43, 49]. The

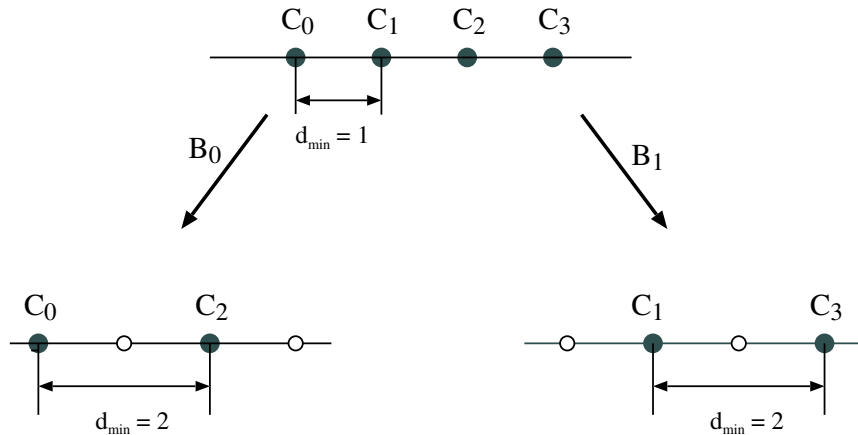


Figure 2.3. Set partitioning of 4-PAM signal set

asymptotic coding gain is given by

$$\gamma = \frac{d_{free/coded}^2}{d_{free/uncoded}^2} \quad (2.2)$$

where d_{free} is the minimum free distance. d_{free} is the minimum Euclidean distance between a pair of valid sequences.

Figure 2.4 illustrates the structure of the four-state TCM encoder. The output of the convolutional encoder selects one of the four signals from the expanded constellation. The sequences generated by the TCM encoder can be described by the trellis shown in Figure 2.5. The minimum free distance of the four-state code is the distance between the pair of codewords represented by the highlighted paths in Figure 2.5. The asymptotic coding gain in this case is 2.5 dB.

The coding gain of the 4-PAM encoder can be improved by increasing the memory of the convolutional encoder. Figures 2.6 and 2.7 illustrate the encoder and the trellis for the eight-state TCM encoder. In this case the asymptotic coding gain is 3 dB.

At the receiver, the demodulated symbols are decoded using the soft-decision

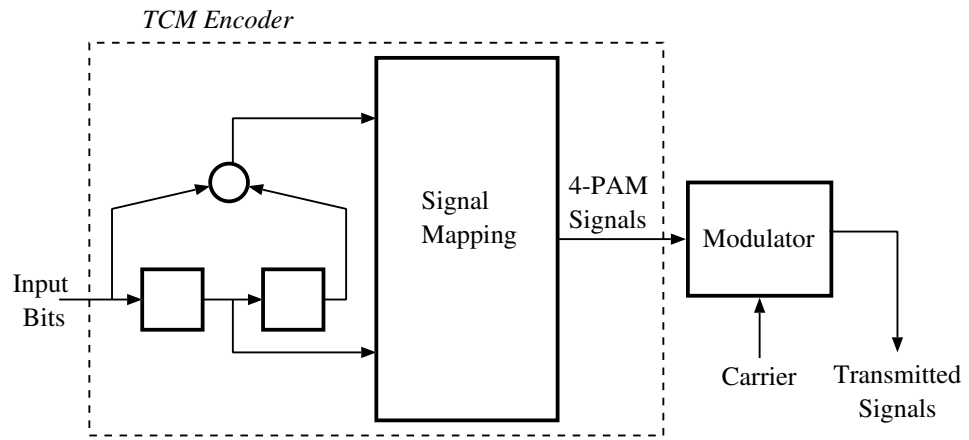


Figure 2.4. Block diagram of the four-state TCM transmitter

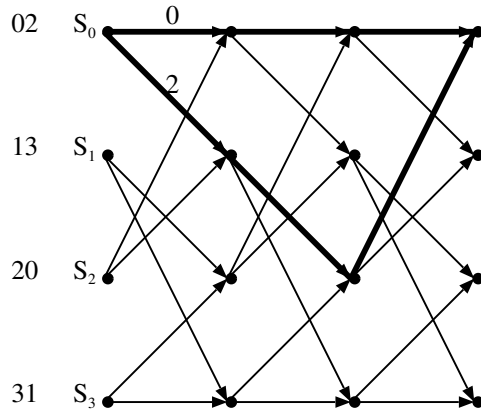


Figure 2.5. Trellis for the four-state encoder.

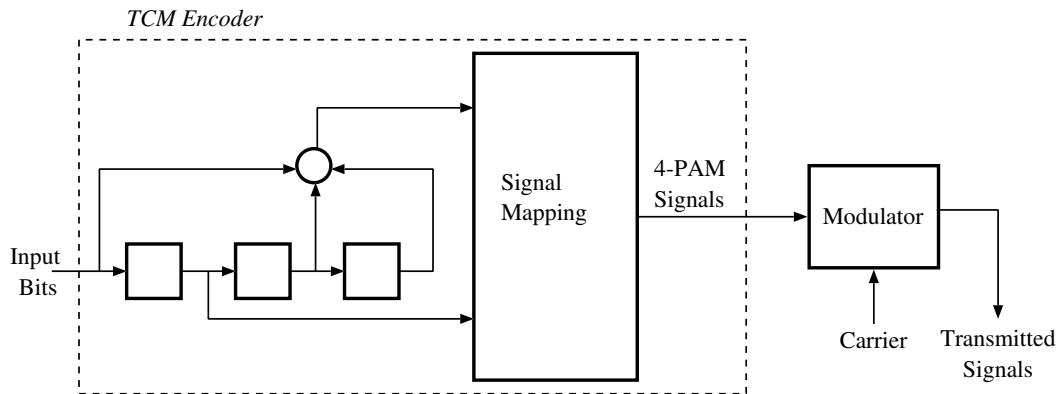


Figure 2.6. Block diagram of the eight-state TCM transmitter

Viterbi decoder [43, 49].

2.3 Experimental Results

We study the performance of the uncoded, TCM and a coding followed by expanded modulation scheme via simulations. The attack on the watermarking systems is assumed to be AWGN.

A four-state as well as eight-state TCM encoder is employed in the simulations. The generator polynomial is $g_0 = D$ and $g_1 = 1 + D^2$ for the four-state encoder and $g_0 = D$ and $g_1 = 1 + D^2 + D^3$ for the eight-state encoder.

In the case of the coding followed by expanded modulation scheme, we use a four state rate $1/2$ convolutional code with generator polynomials $g_0 = 1 + D^2$ and $g_1 = 1 + D + D^2$. The coded bits are mapped into 4-PAM signal points via natural mapping.

We consider two scenarios at the receiver, a blind extraction scheme where the host is unknown at the receiver and an informed scheme where the host image is completely known at the receiver. Figures 2.8 and 2.9 illustrate the blind and the informed extraction scenarios. We use a 512×512 grayscale Lena as the host image.

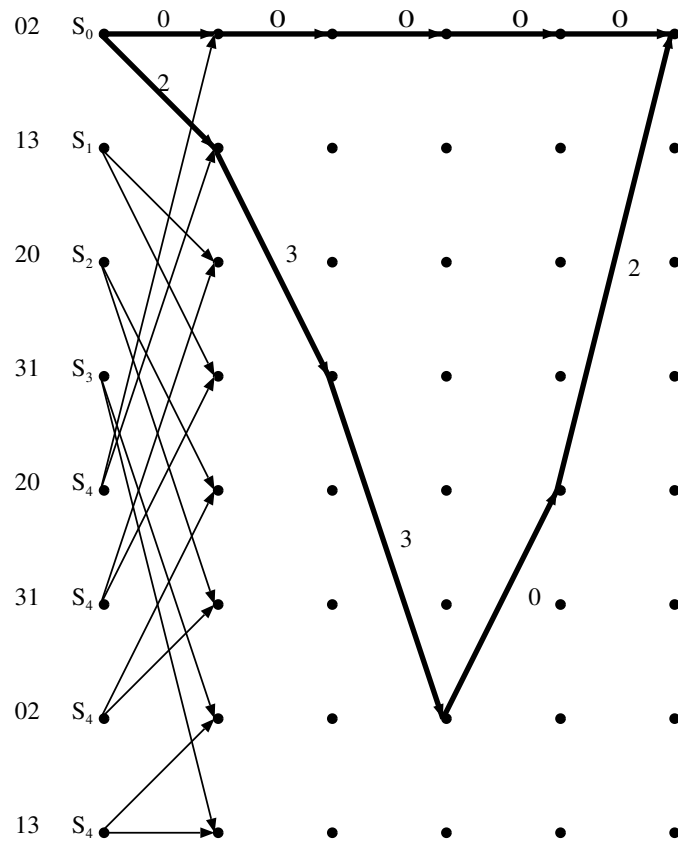


Figure 2.7. Trellis for the eight-state encoder.

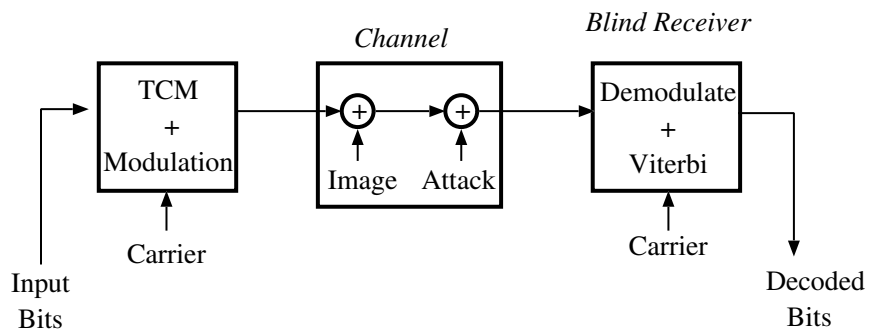


Figure 2.8. Block diagram of blind extraction scheme

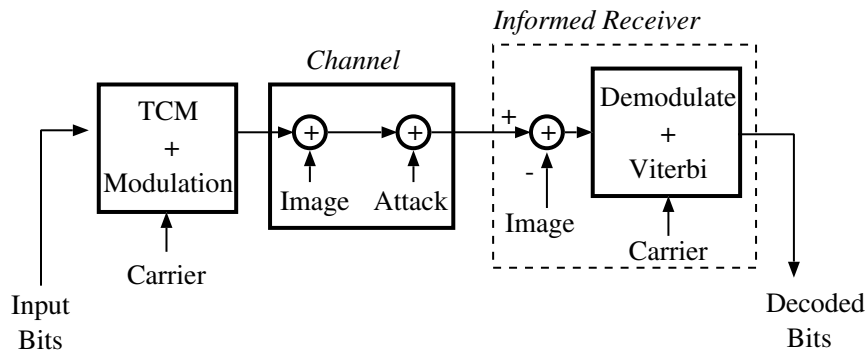


Figure 2.9. Block diagram of informed extraction scheme

The modulating signal C is an 128×128 array constructed from a public/private key cryptography system, as described in [22]. The average power of the watermark is adjusted so that the peak signal-to-watermark ratio (PSWR) is 38 dB. We choose 38 dB as the PSWR to preserve the visual quality of the watermarked image.

We consider a payload of 123 bits. The message template is designed as described in [21]. Experiments show that the embedding strength can be reliably estimated from the watermarked signal and can therefore be assumed at the decoder. We vary the noise samples in a Monte Carlo fashion to obtain the average bit error rate (BER).

We repeat the experiment with a 484 bit payload. In this case the template is a two dimensional rectangular lattice. Figures 2.10 through 2.16 demonstrate our results.

Figure 2.10 compares the performance of the uncoded, TCM and coding followed by expanded modulation schemes. TCM and the uncoded system outperform the coding followed by expanded modulation scheme. Figure 2.11 compares TCM with binary signaling. Clearly TCM performs better than binary signaling.

Figure 2.12 compares the performance of the coded and the uncoded schemes

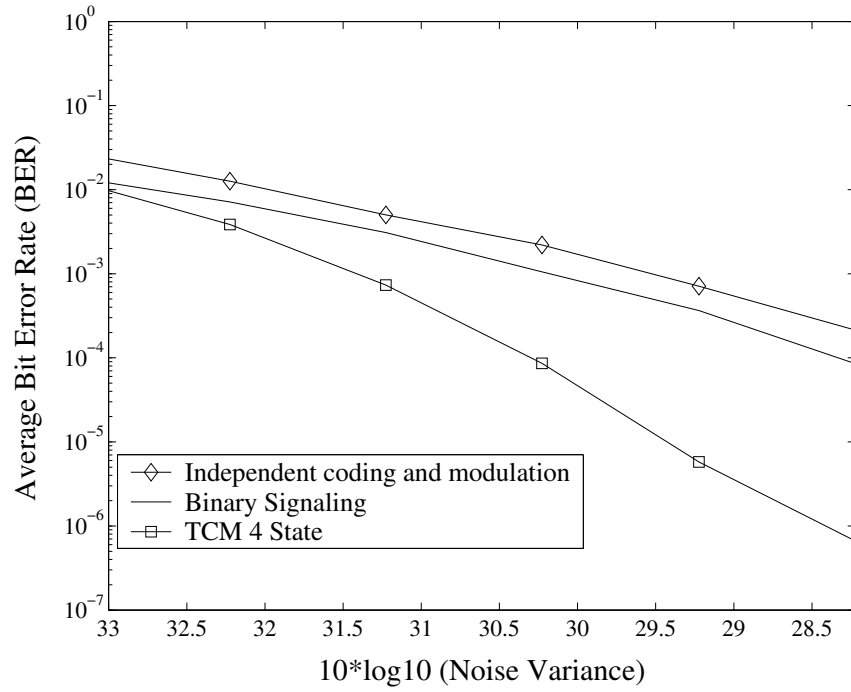


Figure 2.10. BER performance of TCM and coding followed by expanded modulation in a 512×512 host (Lena).

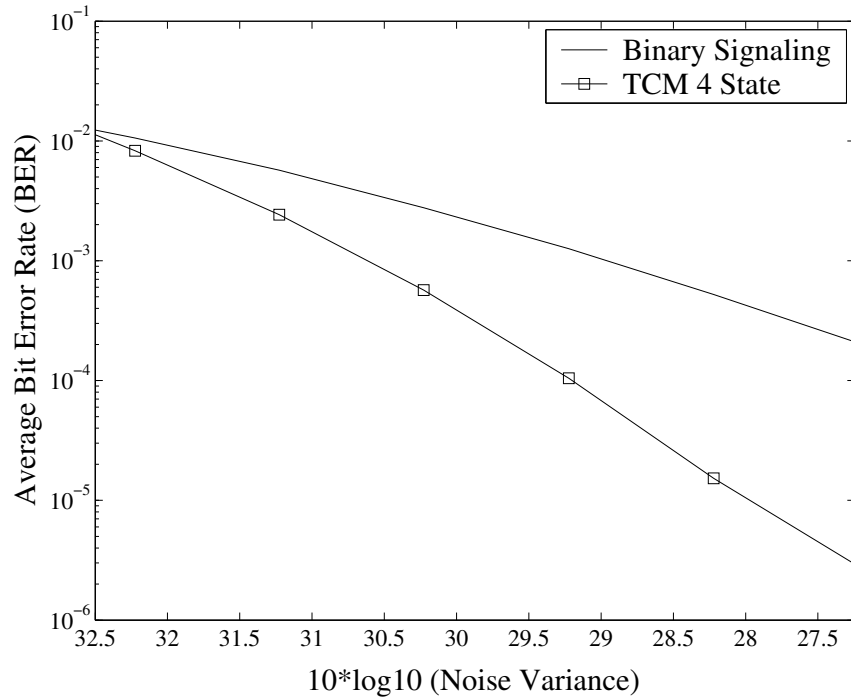


Figure 2.11. BER performance of TCM versus baseline system with a payload of 484 bits in a 512×512 host (Lena).

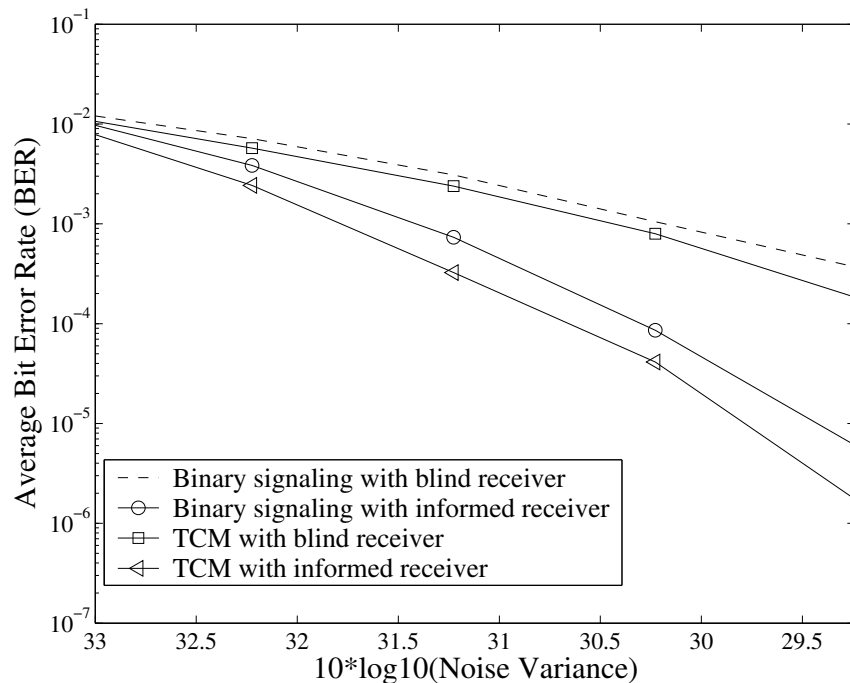


Figure 2.12. BER performance with blind and informed receivers in a 512×512 host (Lena).

for the blind and the informed receivers. Interestingly, there is no significant degradation in the performance of the blind receiver.

Figure 2.13 compares the performance of the eight-state TCM, the four-state TCM and the binary signaling schemes. The eight state code performs better than the four state code by 0.5 dB as expected [43].

Figures 2.14 and 2.15 compare the performance of the TCM and binary signaling schemes in different host images. The results indicate that the TCM scheme outperforms the binary signaling as expected.

We need to estimate the embedding strength because TCM uses non-binary signaling and the image may undergo amplification or a shift in luminance. We perform a linear minimum mean squared error (MMSE) estimation of the signal constellation from the demodulated values before decoding. Figure 2.16 compares MMSE

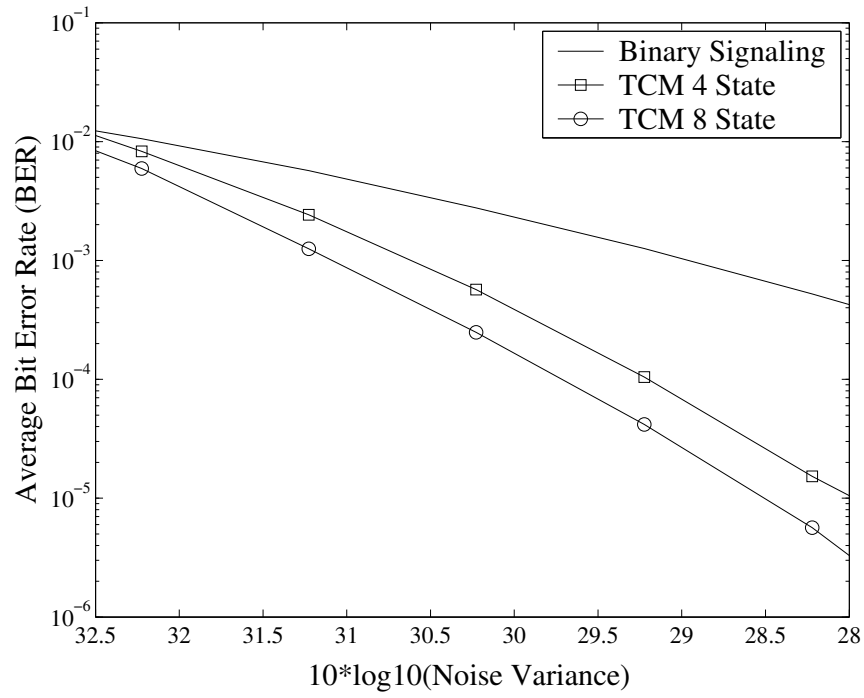


Figure 2.13. BER performance with 4-state and 8-state TCM codes in a 512×512 host (Lena).

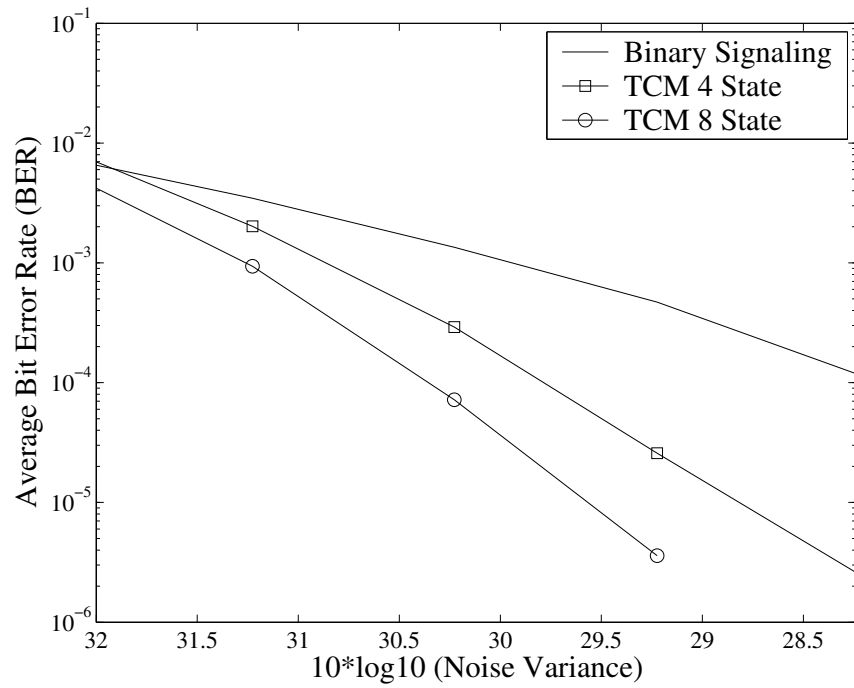


Figure 2.14. BER performance of TCM and baseline system in a 1024×1024 host (Stream).

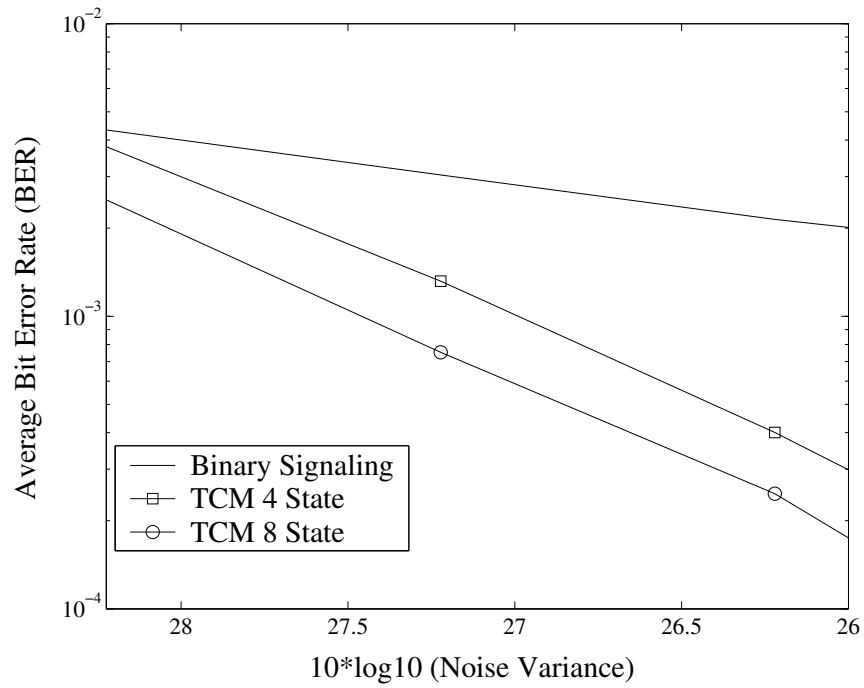


Figure 2.15. BER performance of TCM and baseline system in a 512×512 host (Tiffany).

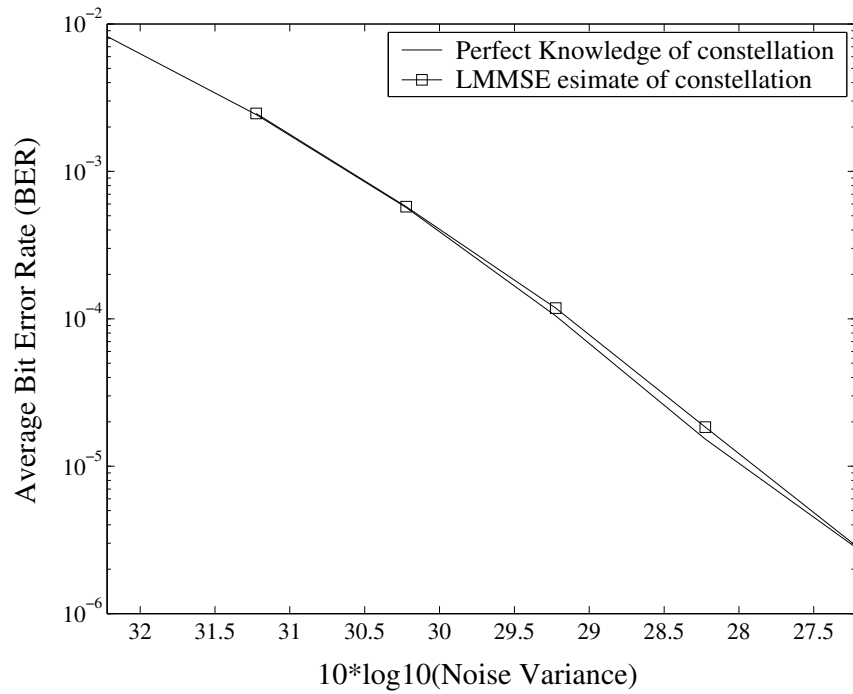


Figure 2.16. MMSE estimated decision boundaries versus perfect knowledge of the same.

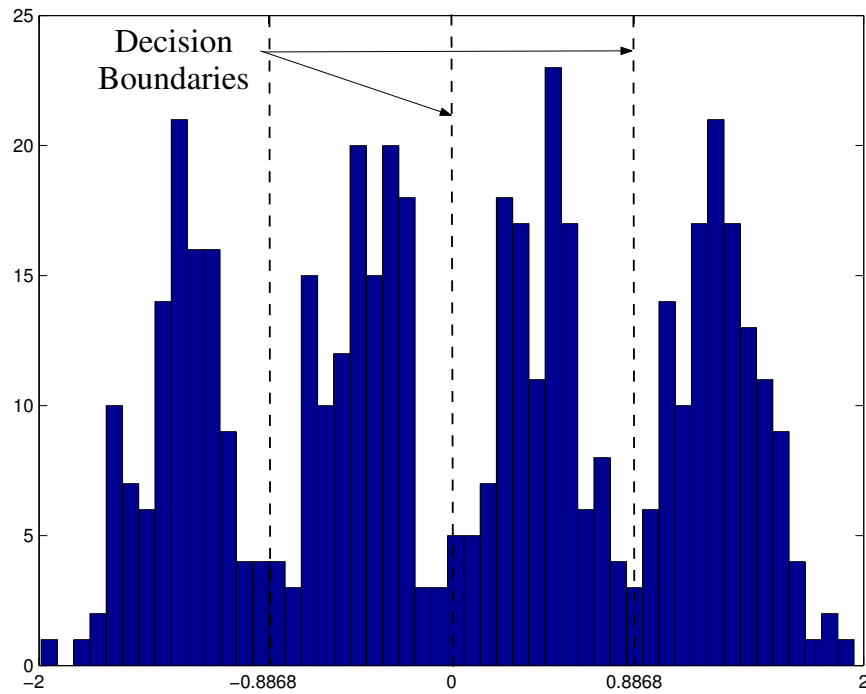


Figure 2.17. Decision boundaries estimated from demodulated data.

estimated decision boundaries with perfect a-priori knowledge of the same. There is no significant degradation in the performance of the receiver with the estimated decision boundaries. Figure 2.17 shows the estimated decision boundaries at 27 dB attack (AWGN) noise power.

CHAPTER 3

SIGNAL DESIGN FOR ROBUST WATERMARKING ON ISI CHANNELS

A method is presented in this chapter to design watermarks robust to intersymbol interference (ISI). This method is general enough to be incorporated into any modulation based watermarking algorithms. The performance of our waveforms are analyzed via experiments.

3.1 Introduction

In general, natural images are band-limited and have a decaying spectrum. We illustrate this fact with the periodogram of two typical images in Figure 3.1. Figure 3.1 shows that the image power spectrum is concentrated around DC. The watermark spectrum must stay clear of these low frequencies to minimize the interference caused by the host.

It is possible for an image to persist despite low-pass operations due to its decaying spectrum. This can be understood by observing the periodograms in Figure 3.2. The watermark spectrum must avoid the high frequency regions where the low-pass operations can wipe out a watermark without visually distorting the image. Hence the high frequency regions of the image spectrum may be considered to be in the stop band of the watermarking channel. From the above it is clear that there is a limit on the bandwidth of the watermarking channel.

Band-limited channels cause signals to spread, resulting in intersymbol in-

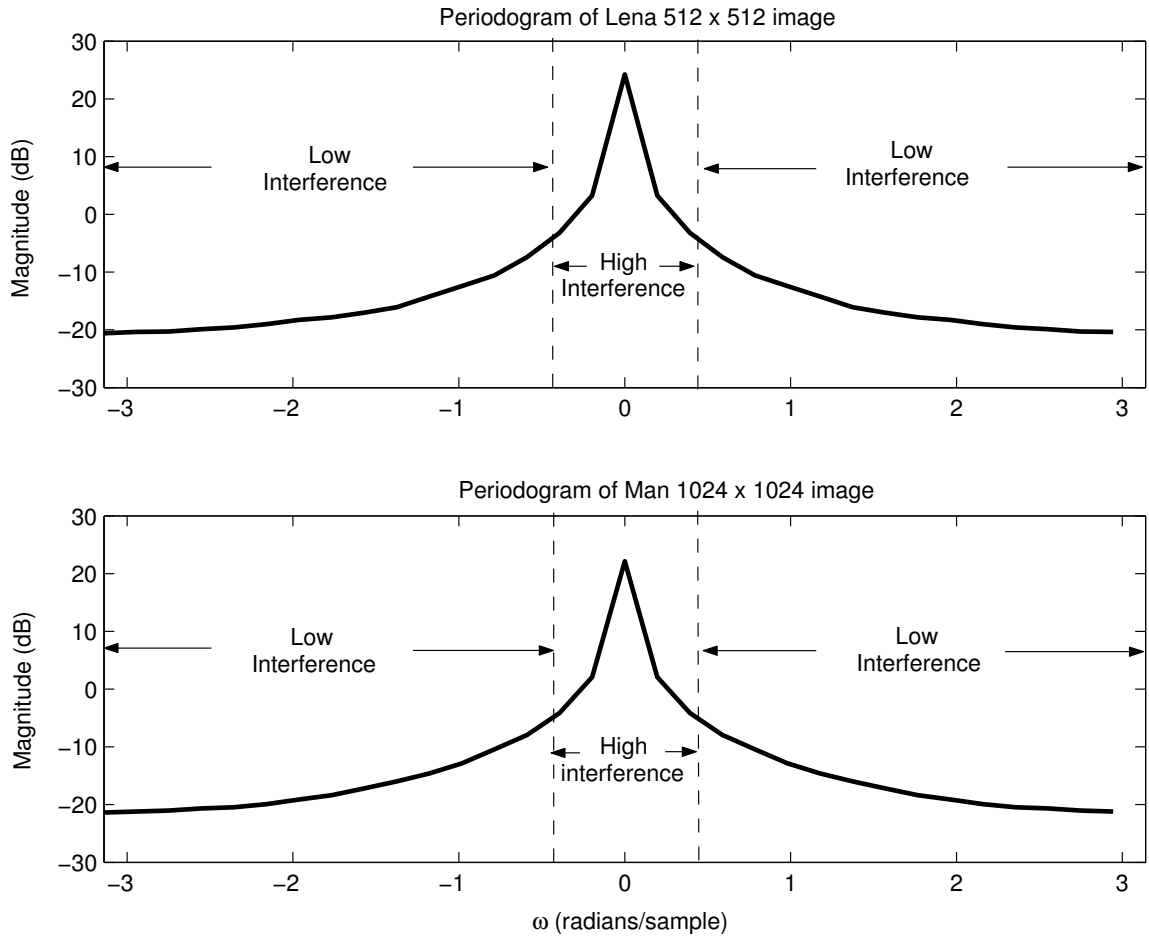


Figure 3.1. Periodograms illustrating the high interference around the DC regions of typical images.

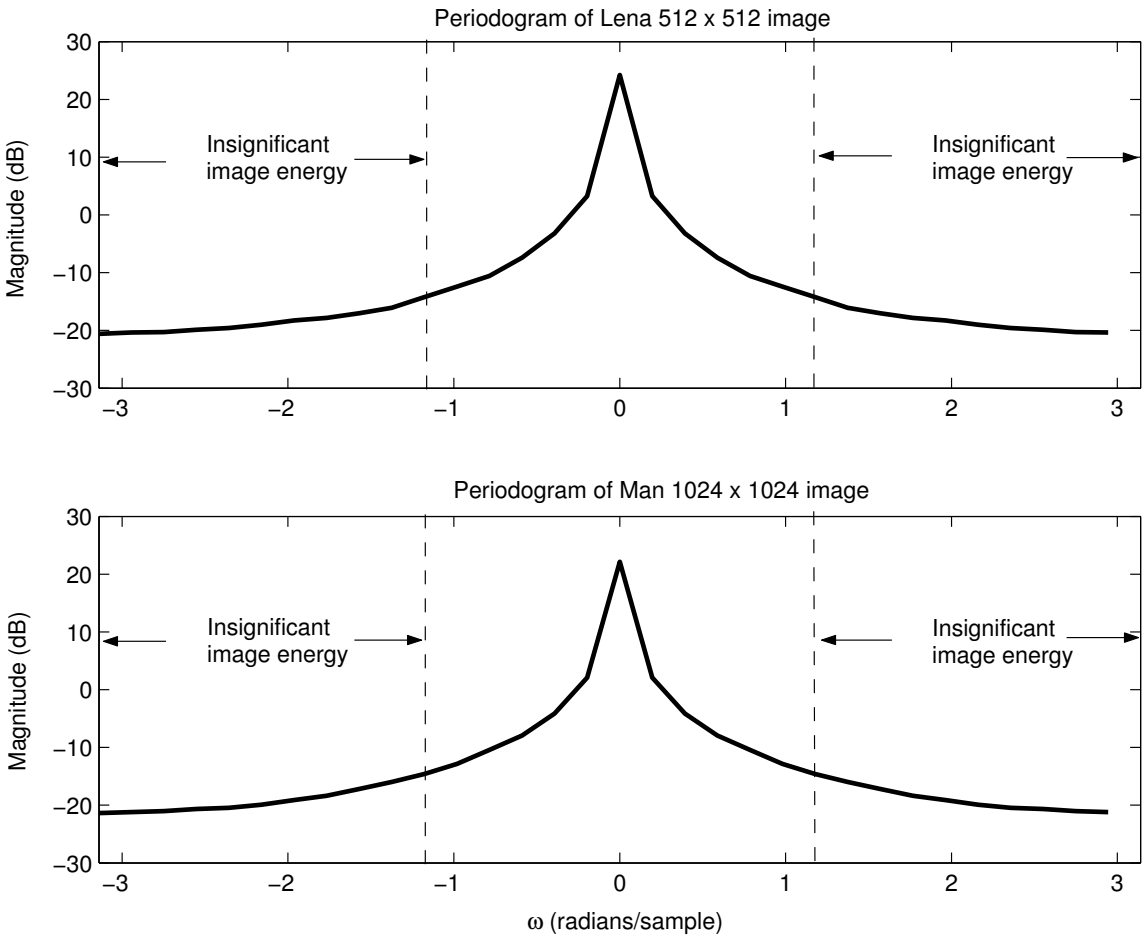


Figure 3.2. Periodograms illustrating the insignificant energy regions of typical images

terference (ISI). Unless it is appropriately addressed, ISI significantly impairs the quality of a digital communication system [38]. Previous watermarking algorithms to our knowledge have not systematically addressed the issue of ISI.

We aim to design ISI-resistant watermarks via the Nyquist criterion [38], which states that the spectrum of the detected signal must alias to a white spectrum after sampling. However, these signals have a low-pass spectrum making them unsuitable for image watermarking. This difficulty arises due to the intensity of the image power spectrum at DC. The core of our contribution is to devise a modulation scheme to keep the watermark spectrum clear of DC as well as the high frequencies (where an attack can wipe out the watermark with impunity) while at the same time satisfying the Nyquist criterion.

In our specific examples we compare the performance of our watermarking waveform with the one proposed by Honsinger and Rabbani in [22]. Experiments demonstrate the performance of our waveforms.

3.2 Signal Design via the Nyquist criterion

We aim to design signals with zero ISI for a known watermarking channel. A necessary and sufficient condition is that the spectrum of the sampled signal aliases to a white spectrum (Nyquist condition) [38]. A separate requirement is to avoid the high level of interference imposed by low-frequency components of the host image. To reconcile these two requirements, we modulate the Nyquist pulse to obtain the watermark.

To demonstrate, consider a plot of our watermark spectrum in Figure 3.3. The desired watermark spectrum avoids the DC region as well as the high frequencies, where an attack may destroy the watermark while leaving the image relatively unscathed. The two-dimensional version of the desired watermark spectrum is shown in Figure 3.4.

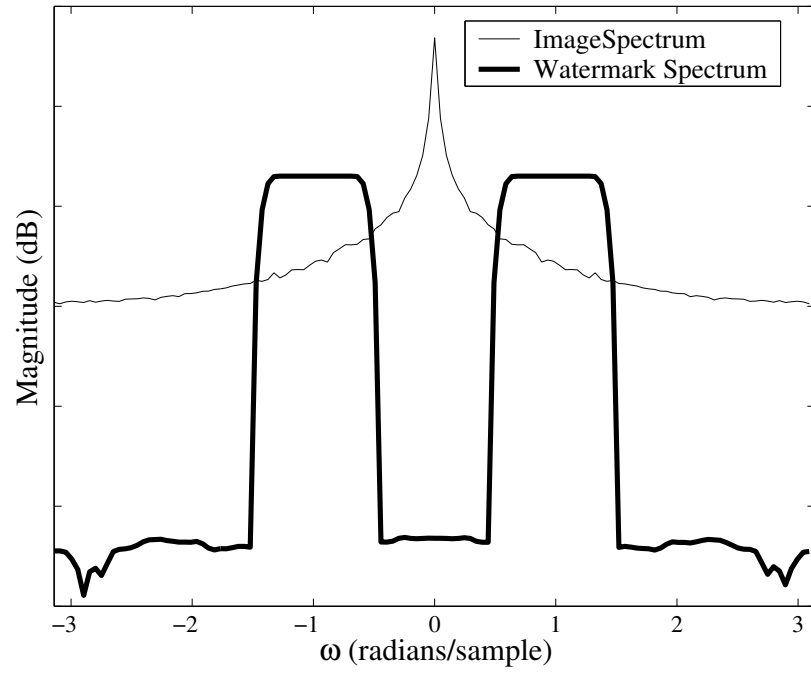


Figure 3.3. Plot of the watermark spectrum and the image spectrum.

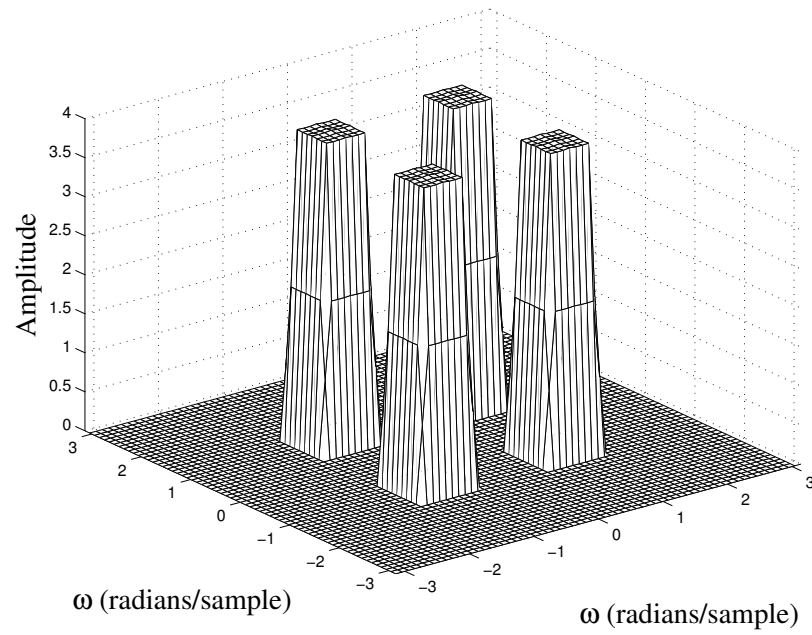


Figure 3.4. Magnitude spectrum of the watermarking pulse.

The design of the modulating signal is done in two steps. First we design a square root Nyquist filter. Because this filter is low-pass, it cannot be directly used in watermarking applications. Therefore we shift the frequency spectrum of the square root Nyquist filter via modulation.

The simplest Nyquist pulse is the sinc pulse. However, in our application the support of the pulse shaping filter is limited. The spectrum of the time (space) limited sinc does not alias to a white spectrum after sampling. Therefore a sinc pulse cannot be used in our image processing application. We need to design an appropriate pulse that satisfies our constraints.

The desired 2-D filter is separable into two 1-D FIR filters. We aim to design FIR filters with the desired frequency support, subject to the constraint on their zero-crossings, i.e, that they are ISI-free. We use the eigenfitler design method of Vaidyanathan and Nguyen [46] for this purpose.

3.2.1 Review of Eigenfitler Design

The eigenfilters method is a least squares approach to linear phase filter design wherein we minimize a quadratic measure of the error between the desired response $D(\omega)$ and the amplitude response $G(\omega)$ of the FIR filter. The desired frequency response is given by

$$D(\omega) = \begin{cases} 1 & , \quad 0 \leq \omega \leq \omega_p \\ 0 & , \quad \omega_s \leq \omega \leq \pi \end{cases} \quad (3.1)$$

where ω_p and ω_s are the pass-band and the stop-band frequencies.

The frequency response of the length L linear phase filter $G(\omega)$ is given by

$$\begin{aligned} G(\omega) &= \sum_{n=1}^K b_n \cos n\omega \\ &= \mathbf{b}^t \mathbf{c} \end{aligned} \quad (3.2)$$

where $K = (L - 1)/2$ assuming that L is odd and

$$\mathbf{b} = [b_0 \ b_1 \ \cdots \ b_K]^t \quad (3.3)$$

$$\mathbf{c} = [1 \ \cos\omega \ \cdots \ \cos K\omega]^t \quad (3.4)$$

The error E is the sum of the pass-band error and the stop-band error. The stop-band error is given by

$$\begin{aligned} \mathbf{E}_s &= \int_{\omega_s}^{\pi} [D(\omega) - G(\omega)]^2 \frac{d\omega}{\pi} \\ &= \int_{\omega_s}^{\pi} \mathbf{b}^t \mathbf{c} \mathbf{c}^t \mathbf{b} \frac{d\omega}{\pi} \\ &= \mathbf{b}^t \mathbf{Q}_s \mathbf{b} \end{aligned} \quad (3.5)$$

where

$$\mathbf{Q}_s = \int_{\omega_s}^{\pi} \mathbf{c} \mathbf{c}^t \frac{d\omega}{\pi} \quad (3.6)$$

The pass-band error can be written as

$$\mathbf{E}_p = \int_0^{\omega_p} e_p^2(\omega) \frac{d\omega}{\pi} \quad (3.7)$$

where

$$\begin{aligned} e_p(\omega) &= [D(\omega) - G(0)] \\ &= (\mathbf{1} - \mathbf{c})^t \mathbf{b}. \end{aligned} \quad (3.8)$$

We use the zero-frequency response $G(0)$ since we can now formulate the pass-band error as a quadratic measure in \mathbf{b} . E_p can now be written as

$$\begin{aligned} \mathbf{E}_p &= \int_0^{\omega_p} \mathbf{b}^t (\mathbf{1} - \mathbf{c})(\mathbf{1} - \mathbf{c})^t \mathbf{b} \frac{d\omega}{\pi} \\ &= \mathbf{b}^t \mathbf{Q}_p \mathbf{b} \end{aligned} \quad (3.9)$$

where \mathbf{Q}_p is given by

$$\mathbf{Q}_p = \int_0^{\omega_p} (\mathbf{1} - \mathbf{c})(\mathbf{1} - \mathbf{c})^t \frac{d\omega}{\pi} \quad (3.10)$$

The total error E can be written as

$$\mathbf{E} = \mathbf{b}^t \mathbf{Q} \mathbf{b} \quad (3.11)$$

where \mathbf{Q} is a real, symmetric and positive definite matrix and is given by

$$\mathbf{Q} = (1 - \beta)\mathbf{Q}_p + \beta\mathbf{Q}_s, \quad 0 \leq \beta \leq 1 \quad (3.12)$$

where the elements of \mathbf{Q} are given by

$$\mathbf{Q}_{n,m} = \frac{(1 - \alpha)}{\pi} \int_0^{\omega_p} (1 - \cos n\omega)(1 - \cos m\omega)d\omega + \frac{(\alpha)}{\pi} \int_{\omega_s}^{\pi} (\cos n\omega \cos m\omega)d\omega \quad (3.13)$$

The matrix \mathbf{Q} can be easily computed from (3.13) once we are given the band edges ω_p and ω_s as well as α .

The error \mathbf{E} in (3.11) is to be minimized subject to the constraint $\mathbf{b}^t \mathbf{b} = 1$. The solution \mathbf{b} to (3.11) is the eigenvector of \mathbf{Q} corresponding to the minimum eigenvalue of \mathbf{Q} [46].

We use the eigenfilters method to design a filter (pulse) with zero crossings at the desired sampling instants. We modify the vector \mathbf{b} to include the zero crossing constraint.

$$\mathbf{b} = [b_0 \ \cdots \ b_{J-1} \ 0 \ b_{J+1} \ \cdots \ b_{2J-1} \ 0 \ b_{2J+1}, \ \cdots]^t \quad (3.14)$$

where J is sampling rate.

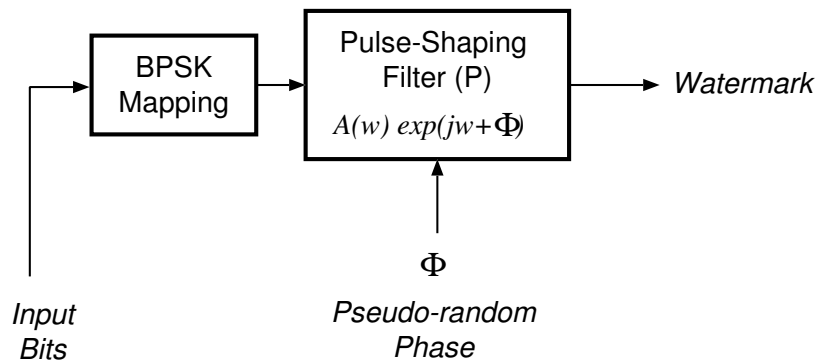


Figure 3.5. Transmitter of the proposed scheme.

Therefore, the rows and columns of \mathbf{Q} whose indices are multiples of J do not contribute to the total error \mathbf{E} . The problem is restated as minimizing the error $\mathbf{E}_1 = \hat{\mathbf{b}}^t \hat{\mathbf{Q}} \hat{\mathbf{b}}$ where

$$\hat{\mathbf{b}} = [b_0 \cdots b_{J-1} \quad b_{J+1} \cdots b_{2J-1} \quad b_{2J+1}, \cdots]^t \quad (3.15)$$

and

$$\hat{\mathbf{Q}} = \begin{pmatrix} Q_{0,0} & \cdots & Q_{0,J-1} & Q_{0,J+1} & \cdots & Q_{0,2J-1} \\ Q_{1,0} & \cdots & Q_{1,J-1} & Q_{1,J+1} & \cdots & Q_{1,2J-1} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots \\ Q_{J-1,0} & \cdots & Q_{J-1,J-1} & Q_{J-1,J+1} & \cdots & Q_{J-1,2J-1} \\ Q_{J+1,0} & \cdots & Q_{J+1,J-1} & Q_{J+1,J+1} & \cdots & Q_{J+1,2J-1} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots \end{pmatrix} \quad (3.16)$$

We compute the appropriate eigenvector of $\hat{\mathbf{Q}}$ to obtain $\hat{\mathbf{b}}$. We insert zeros every J samples in $\hat{\mathbf{b}}$ to obtain our Nyquist filter impulse response.

3.3 Watermarking with Nyquist Pulses

Figure 3.5 illustrates the structure of the proposed transmitter (embedding). The modulating signal P is a two-dimensional band-limited pulse with a pseudo-random phase. This signal is constructed in the frequency domain and then transformed to a

space domain signal. The following relationship is used to construct P .

$$F(u, v) = A \cdot \cos(\Phi) + j \cdot A \cdot \sin(\Phi) \quad (3.17)$$

where F is the Fourier transform of P , Φ is the phase and A is the magnitude of the modulating signal P .

The magnitude A of the modulating pulse P is derived from that of the Nyquist filter whose design is described in the previous section. We ensure that our modulating signal P is real by imposing the conjugate symmetry constraint on its Fourier transform [27], i.e ,

$$F(u, v) = F^*(-u + mK, -v + nK), \quad m, n = 0, \pm 1, \pm 2, \dots \quad (3.18)$$

where $*$ denotes complex conjugation and K is the size of our modulating signal P .

The phase Φ is derived from a pseudo-random number generator with a user-specified key. Thus only users with the key will be able to encode and decode the watermark. The pseudo-random phase ensures secrecy required in a watermarking system.

The BPSK pulses representing the information bits are placed in a 2-dimensional array M . The message image is modulated by P to form our watermark. The watermark is added to the host image I to form the watermarked image I' . The embedding operation is given by

$$I'(x, y) = \alpha(M(x, y) * P(x, y)) + I(x, y) \quad (3.19)$$

where α is the embedding strength, (x, y) denotes the location of a sample and $*$ denotes circular convolution. Figure 3.4 illustrates the magnitude spectrum of the modulated pulse.

The host image is tiled and (3.19) is repeated in all the tiles to improve the quality of the signal at the demodulator. The embedding strength α is maintained the same across all the tiles in our experiments.

The channel consists of low pass filtering and additive white Gaussian noise (AWGN). The above operation is given by

$$R(x, y) = H(x, y) * I'(x, y) + N(x, y) \quad (3.20)$$

where H is the impulse response of the low pass filter and $N(x, y)$ is an additive white Gaussian noise (AWGN) sample.

Assuming synchronization at the receiver (extraction), the tiles are summed together before demodulation is performed. The demodulator is a matched filter (correlator) matched to the modulating signal P . This is given by

$$M'(x, y) = \alpha(M(x, y) * P(x, y) \otimes P(x, y)) + N(x, y) \otimes P(x, y) \quad (3.21)$$

where M' denotes the extracted message image, $N(x, y)$ is a AWGN sample and \otimes denotes circular correlation.

The demodulated symbols are recovered by sampling the output of the demodulator at predefined locations (same as the locations in M). The transmitted pulses are estimated from the phase of the demodulated samples.

3.4 Experiments

We evaluate the performance of the proposed scheme via simulations. We compare the performance of our method with Honsinger and Rabbani's method [21].

We assume two scenarios at the receiver (extraction), (a) blind scheme where the host is unknown at the receiver and, (b) informed scheme where the host image

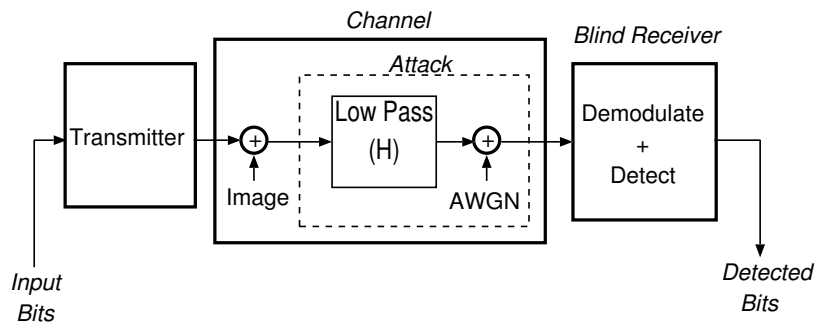


Figure 3.6. Block diagram of blind extraction scheme.

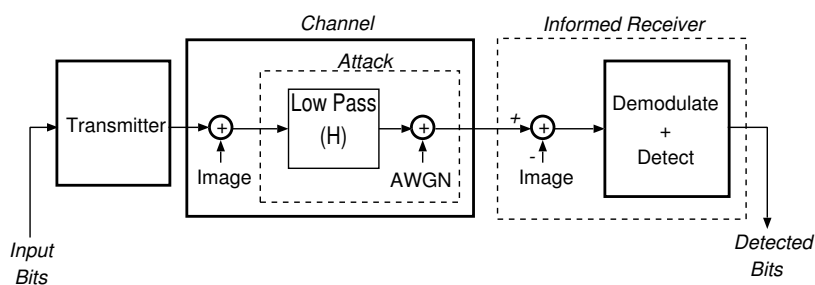


Figure 3.7. Block diagram of informed extraction scheme.

is completely known at the receiver, as illustrated in Figures 3.6 and 3.7.

We consider a payload of 256 bits. The message template is a two-dimensional 128×128 lattice with the pulses arranged in a 16×16 grid on the template. The modulating signal P is a 128×128 array with a rectangular magnitude spectrum. P is constructed from a public/private key cryptography system as described previously.

The band-limited channel H is a low-pass filter with a cut-off frequency $0.4453f_n$ where f_n is the Nyquist frequency. The average power of the watermark is adjusted so that the peak signal-to-watermark ratio (PSWR) is 44 dB. We choose 44 dB to preserve the visual quality of the watermarked image to the same level as the baseline method. We use the parameters described in [21] to evaluate Honsinger and Rabbani's scheme. The average power of the watermark in [21] is adjusted so that the PSWR is 38 dB. The watermark in [21] is embedded at a higher average power

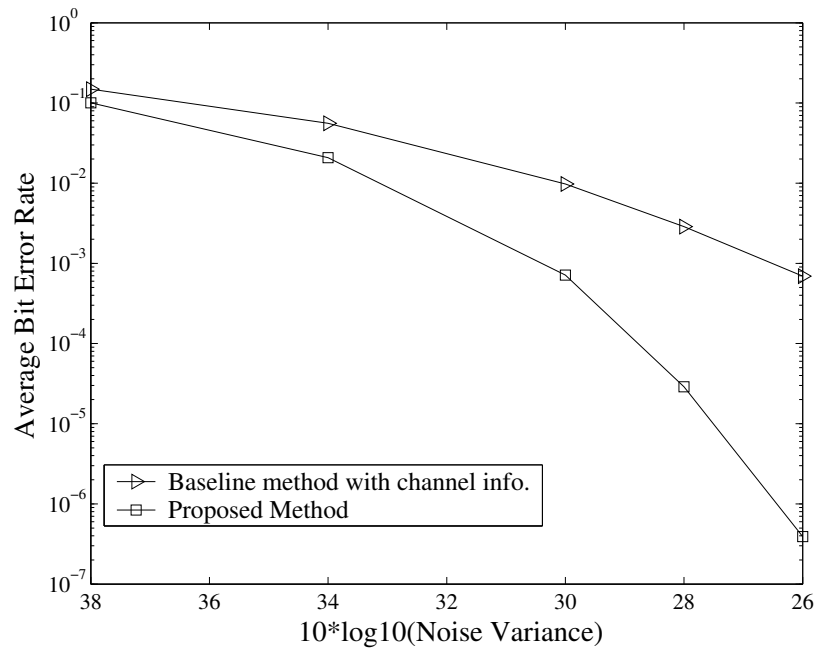


Figure 3.8. Performance comparison in the informed receiver case with a 1024 x 1024 host.

compared to our scheme. This ensures fairness in comparisons as the visual quality of the watermarked image in method [21] is similar to that in the proposed method. The two systems are subjected to the same amount of AWGN. We vary the noise samples in a Monte Carlo fashion to obtain the average BER.

Figures 3.8 through 3.13 demonstrate the simulation results. Figures 3.9 and 3.10 compares the performance of our system with the baseline system of [21] for a 1024×1024 host. We consider two scenarios for the system in [21]: receiver with perfect knowledge of the channel (H) and no knowledge of the channel. The first scenario ensures fairness in comparisons as we filter out the noise that lies in the stop-band of the channel. It is seen from Figures 3.9 and 3.10 that the proposed scheme outperforms the method in [21]. Figures 3.12 and 3.13 illustrates the BER comparison for 512×512 images.

Figure 3.8 and 3.11 illustrates the BER performance for the informed receiver.

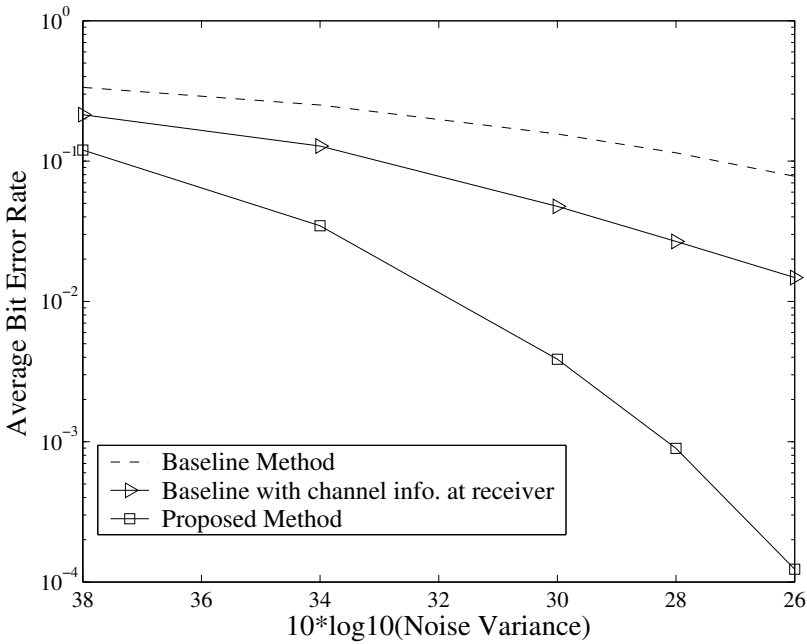


Figure 3.9. Performance comparison in the blind receiver case with a 1024 x 1024 host (Man).

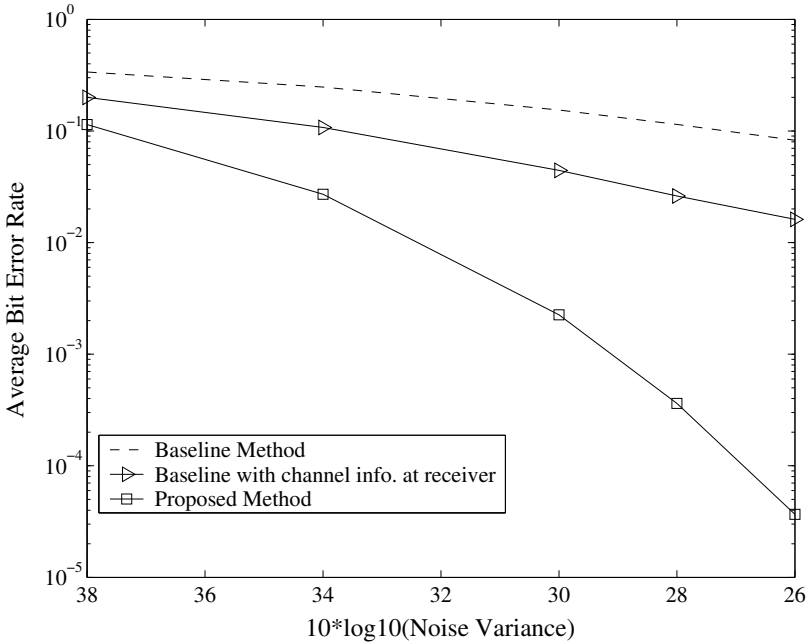


Figure 3.10. Performance comparison in the blind receiver case with a 1024 x 1024 host (Stream).

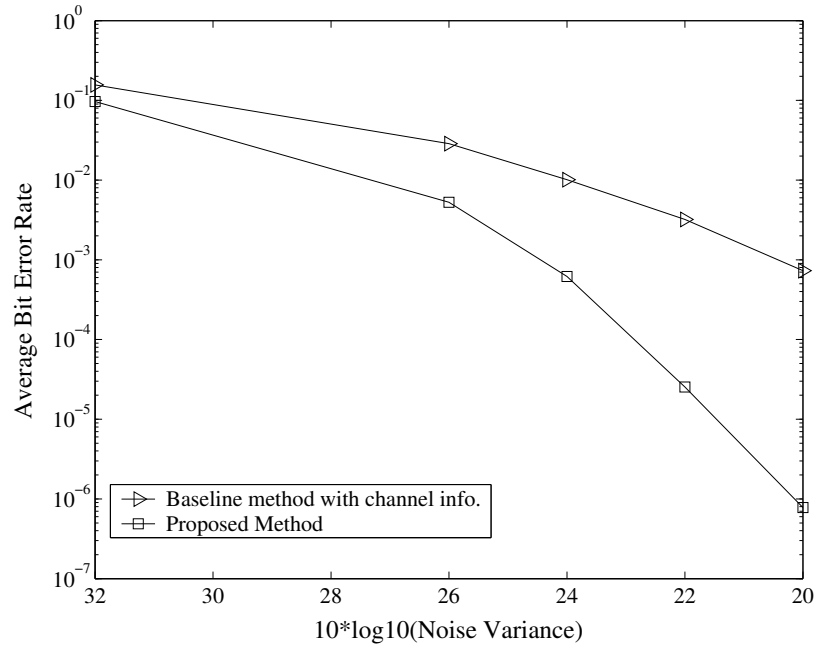


Figure 3.11. Performance comparison in the informed receiver case with a 512 x 512 host.

We compare the performance of our system with the baseline system which has perfect knowledge of the channel (H). Our method provides an improvement of 4 dB.

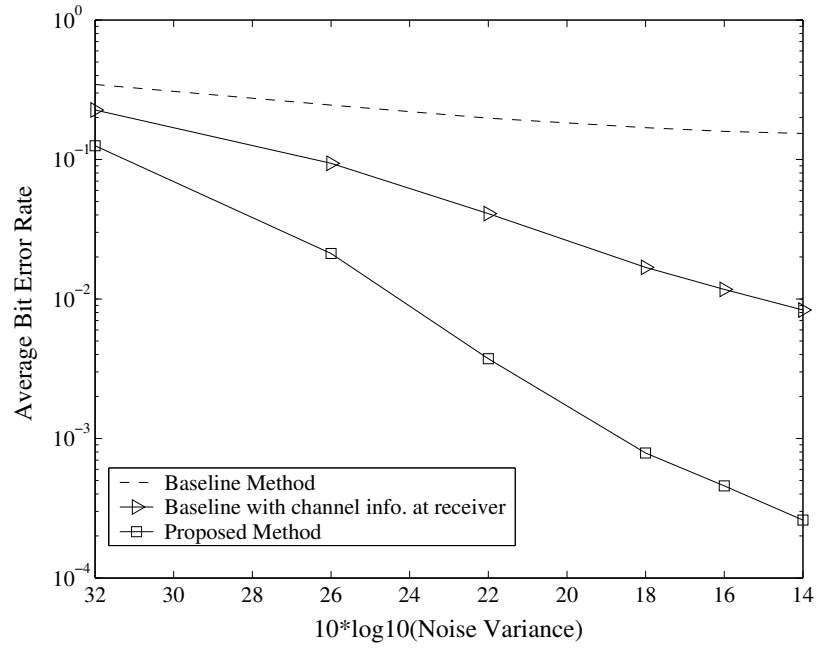


Figure 3.12. Performance comparison in the blind receiver case with a 512 x 512 host (Peppers).

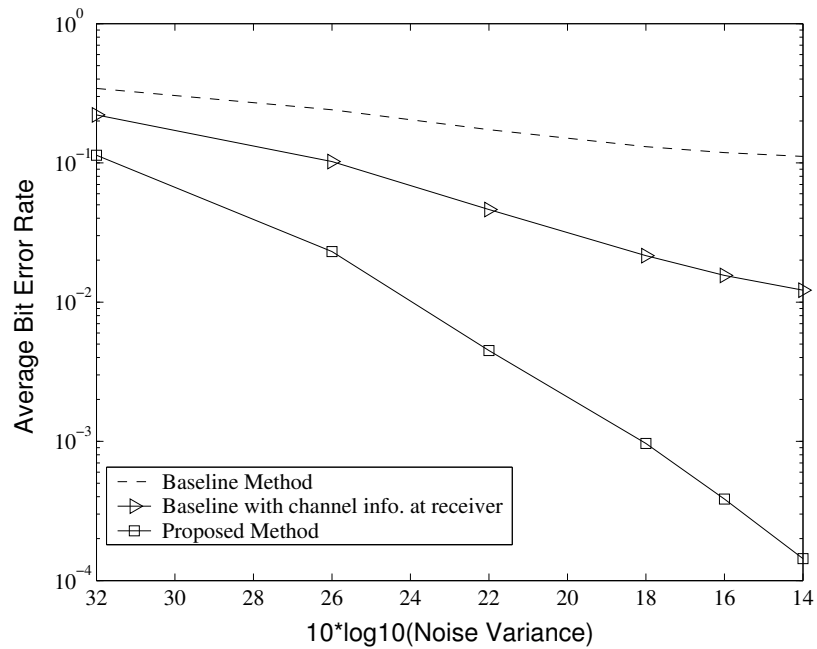


Figure 3.13. Performance comparison in the blind receiver case with a 512 x 512 host (Tiffany).

CHAPTER 4
TWO METHODS TO IMPROVE THE ROBUSTNESS OF WATERMARKING IN
BAND-LIMITED CHANNELS

Here we propose extensions to algorithms developed in Chapters. 2 and 3. We consider the problem of error control for systems employing the band-limited waveforms developed in Chapter 3. A linear equalizer for watermarking systems is also presented in this chapter.

4.1 Error Control for Band-Limited Watermark Signals

In Chapter 3, we design a watermark for distortion-free transmission in band-limited channels. Error control may be employed to further improve the performance of these systems. We study the use of bandwidth efficient error control schemes such as trellis coded modulation (TCM) [43] in the above watermarking systems.

Figure 4.1 illustrates the block diagram of the proposed scheme. The information bits are encoded with a four state TCM encoder. Figure 4.2 illustrates the trellis

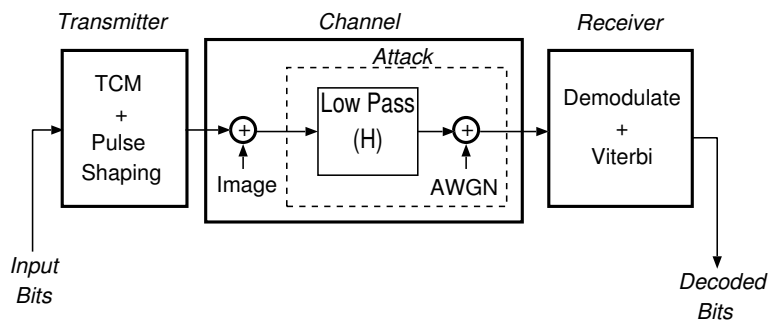


Figure 4.1. Block Diagram of a watermarking system with TCM

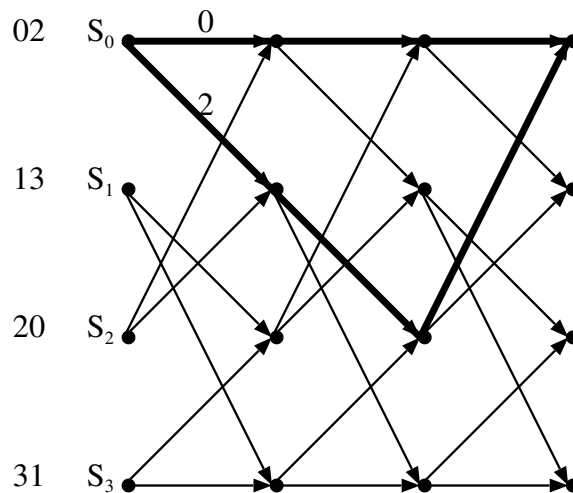


Figure 4.2. Trellis of our TCM encoder

for the TCM encoder. The watermark is formed by modulating the encoded bits with the band-limited watermarking waveforms developed in the previous chapter.

The channel model consists of a low-pass filter and additive white Gaussian noise (AWGN). The embedded information is estimated by demodulation and soft-decision Viterbi algorithm.

The performance of the above system is verified via experiments. The experiments deliver a payload of 256 bits. The channel H is a low-pass filter with a cut-off frequency of $0.4453f_n$, where f_n is the Nyquist frequency (in each dimension). Figures 4.3 and 4.4 illustrate the results for two different 1024×1024 images. The coded system outperforms the uncoded system in both cases.

4.2 Watermarking in Unknown Band-Limited Channels

Generally the characteristics of watermarking channels may not be known with sufficient precision at the time of designing the watermark waveforms. Therefore, despite pulse shaping at the transmitter, some residual ISI may persist.

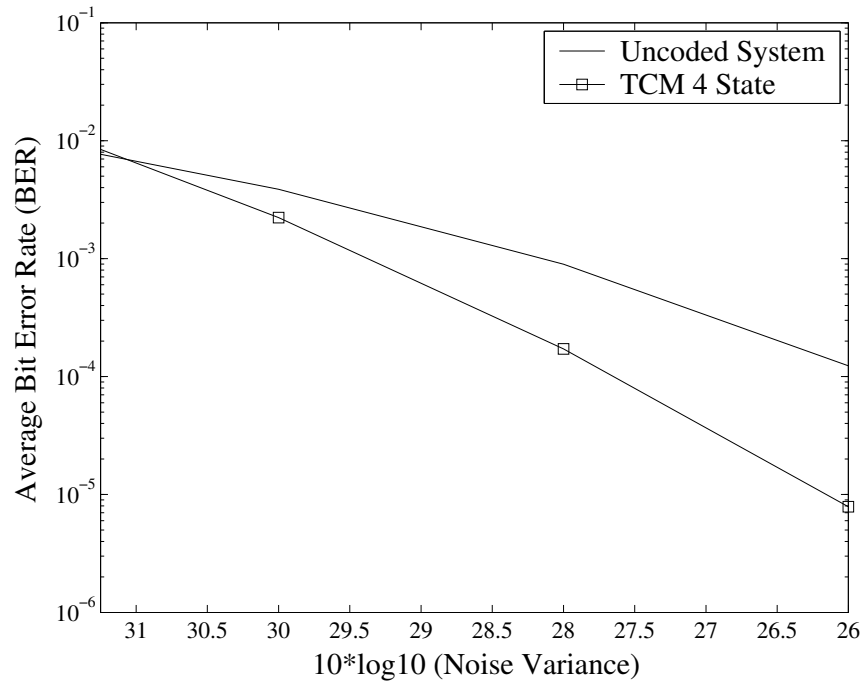


Figure 4.3. BER performance of TCM and uncoded system in a 1024 x 1024 host. (Man)

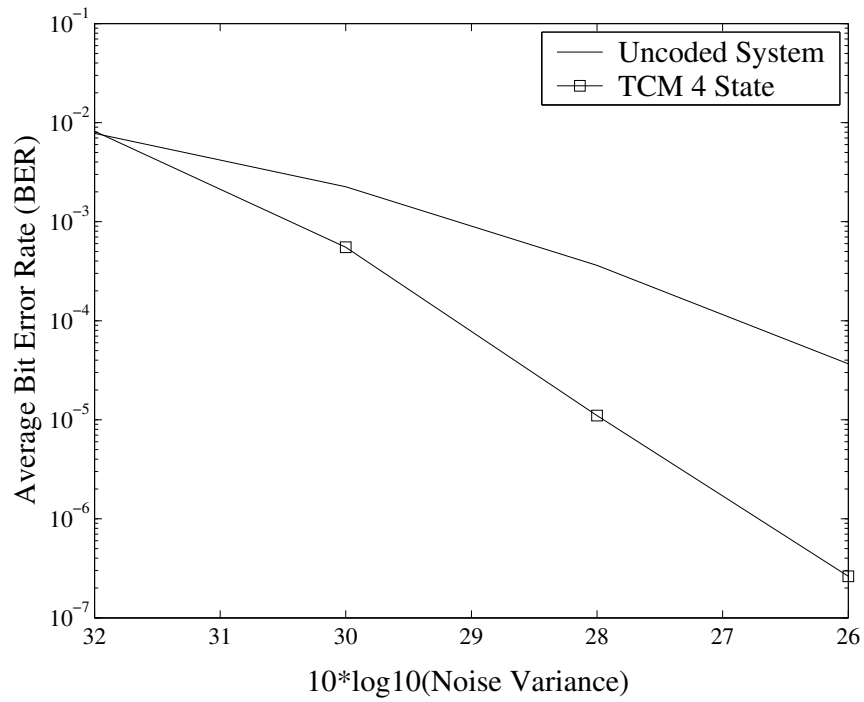


Figure 4.4. BER performance of TCM and uncoded system in a 1024 x 1024 host. (Stream)

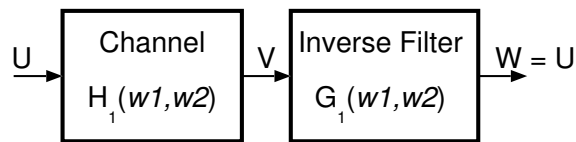


Figure 4.5. Principle of inverse filtering.

We intend to mitigate the above residual distortion at the receiver of watermarking systems. Communications receivers employ equalizers [38] to compensate for distortions due to ISI. This idea extends to watermarking systems. A linear filter to combat ISI is proposed in this section.

A simple method to compensate for the distortions caused by linear filtering is by inverse filtering [27]. Figure 4.5 illustrates the operation of a inverse filter. The following assumes two-dimensional signals, however the discussion is general. The input U is convolved by a system H_1 to form the output V . This can be written as

$$V(\omega_1, \omega_2) = H_1(\omega_1, \omega_2) * U(\omega_1, \omega_2) \quad (4.1)$$

where $V(\omega_1, \omega_2)$, $H_1(\omega_1, \omega_2)$ and $U(\omega_1, \omega_2)$ are the Fourier transforms of V , H_1 and U respectively. The output of the inverse filter G_1 is given by

$$W(\omega_1, \omega_2) = G_1(\omega_1, \omega_2) * V(\omega_1, \omega_2) \quad (4.2)$$

where $G_1(\omega_1, \omega_2)$ is the Fourier transform of the inverse filter. To recover the original signal we need:

$$G_1(\omega_1, \omega_2) = \frac{1}{H_1(\omega_1, \omega_2)} \quad (4.3)$$

When H_1 is close to zero, $G_1(\omega_1, \omega_2)$ is large in magnitude. To handle this, H_1 in 4.3 is modified as

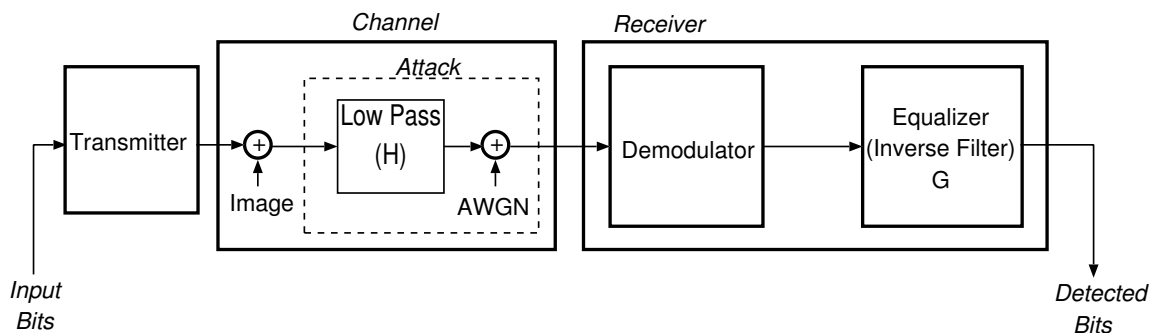


Figure 4.6. Block diagram of a watermarking system employing a equalizer

$$H_1(\omega_1, \omega_2) = \begin{cases} \frac{1}{H_1(\omega_1, \omega_2)} & |H_1(\omega_1, \omega_2)| > \epsilon \\ \epsilon & |H_1(\omega_1, \omega_2)| < \epsilon \end{cases}$$

for a small $\epsilon > 0$.

Figure 4.6 shows the block diagram of the proposed scheme which is an extension of the scheme in Chapter 3. The equalizer in Fig. 4.6 is a inverse filter that reduces the effects of the distortions due to ISI. We assume receiver has perfect knowledge of the channel response. With this knowledge, the inverse filter G is given by

$$G(\omega_1, \omega_2) = \frac{1}{H(\omega_1, \omega_2)} \quad (4.4)$$

and

$$H(\omega_1, \omega_2) = \begin{cases} \frac{1}{H(\omega_1, \omega_2)} & |H(\omega_1, \omega_2)| > \epsilon \\ \epsilon & |H(\omega_1, \omega_2)| < \epsilon \end{cases}$$

Simulations are performed to evaluate the above system. We employ the same parameters as those used in the experiments of Chapter 3. The band-limited channel H is characterized by an ideal low-pass filter with a cutoff frequency of $0.3828f_n$ where f_n is the Nyquist frequency (in each dimension).

Figures 4.7 and 4.8 illustrate the experimental results for two 1024×1024 gray scale images. The system with no equalizer is referred to as the threshold detection

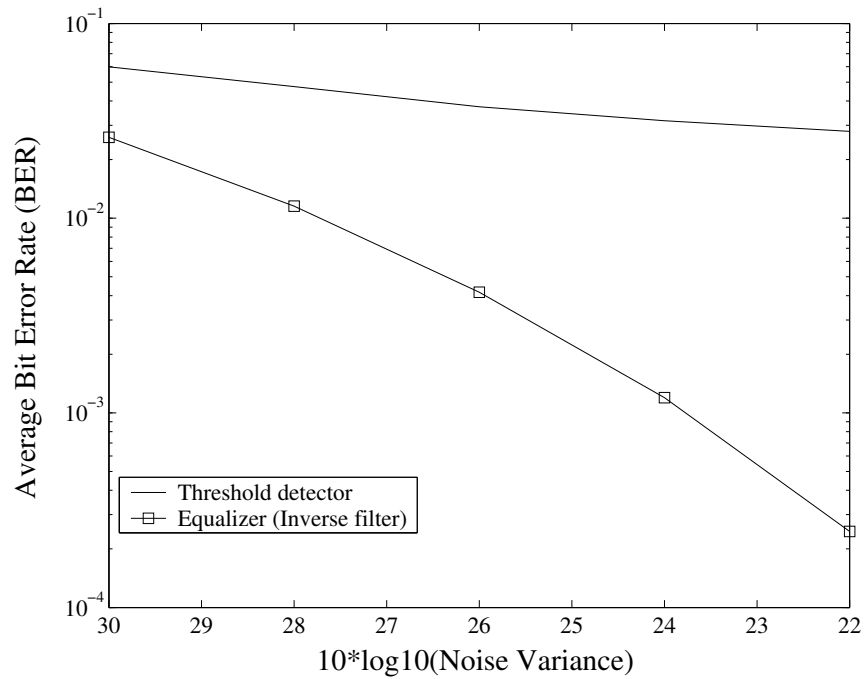


Figure 4.7. Performance comparison with and without equalizers in a 1024 x 1024 host. (Man)

system since the detection is performed via simple thresholding. It is clear from the figures that the equalizer provides substantial gain over the simple threshold based detection system.

Figure 4.9 illustrates a system with equalizer and error control. A four state TCM encoder is used in the above system. At the receiver, equalization is performed before applying the soft-decision Viterbi algorithm.

Figures 4.10 and 4.11 illustrate the results for 1024 × 1024 grayscale images. We use the same parameters as those used in the previous experiment. The coded system outperforms the uncoded system in both cases.

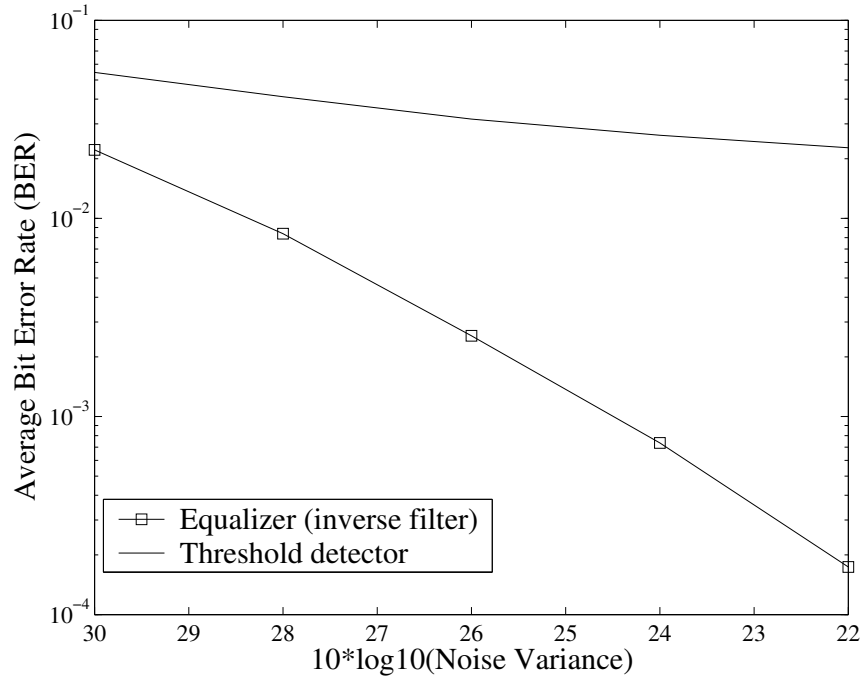


Figure 4.8. Performance comparison with and without equalizers in a 1024 x 1024 host. (Stream)

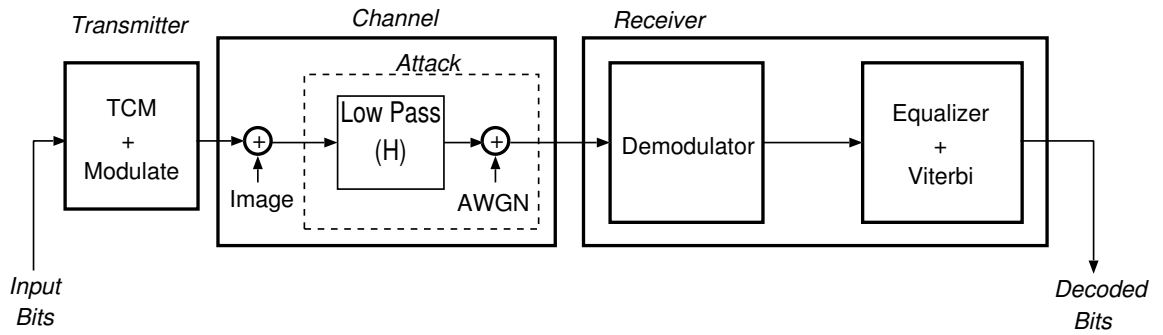


Figure 4.9. Block diagram of a watermarking system with equalizer and error control

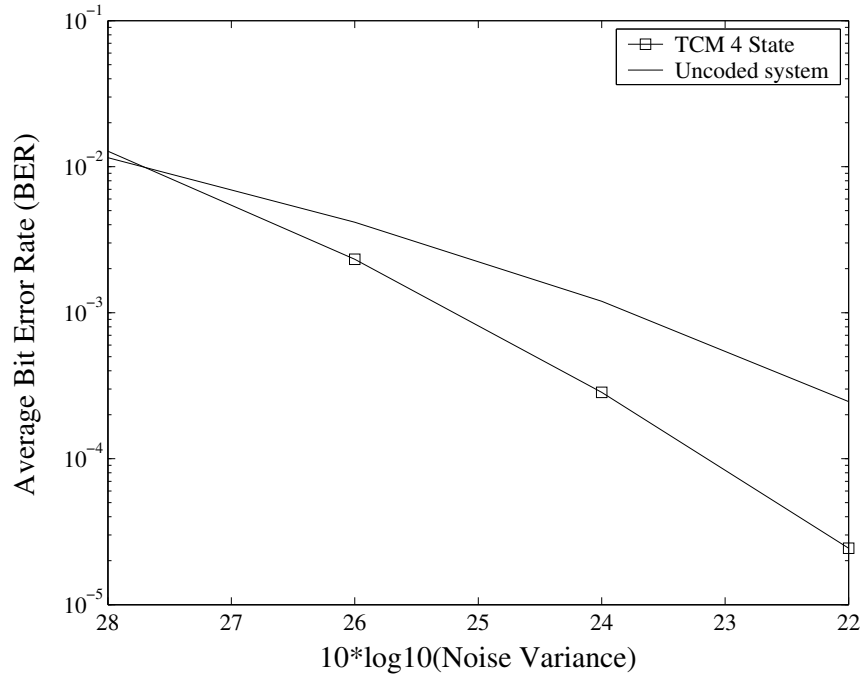


Figure 4.10. Performance comparison illustrating the coding gain due to TCM in a 1024 x 1024 host. (Man)

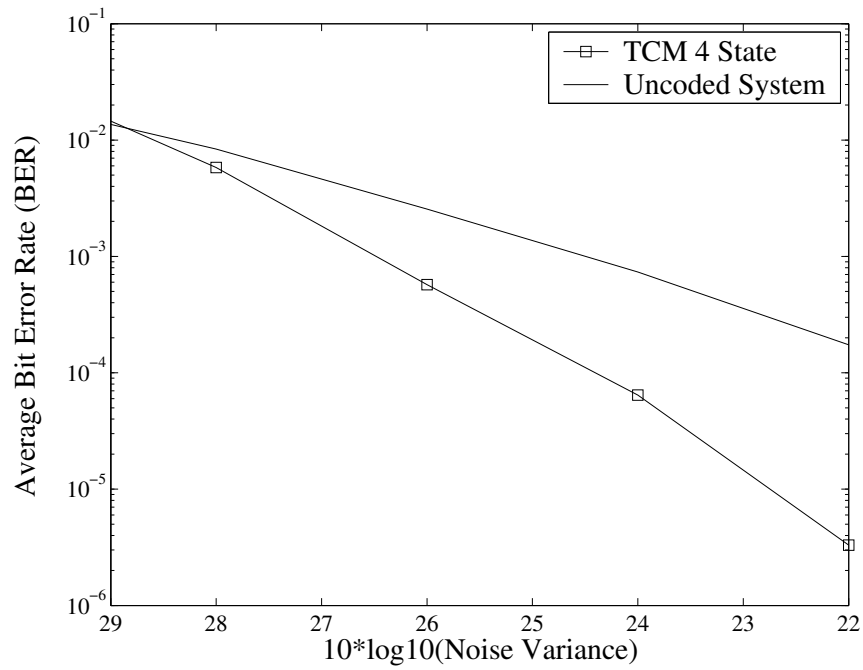


Figure 4.11. Performance comparison illustrating the coding gain due to TCM in a 1024 x 1024 host. (Stream)

CHAPTER 5

CONCLUSIONS

The watermarking system can be viewed as a power limited band-limited digital communications system. Existing watermarking systems to the best of our knowledge, do not appropriately address the band-limited aspect of watermarking in their design. This thesis proposes three methods that address the band-limited nature of watermarking.

We design a trellis coded modulation (TCM) scheme for watermarking which provides error control without decreasing the information rate. This method is general enough to be incorporated into any existing modulation based watermarking algorithm. Simulation results indicate that TCM outperforms the existing methods for error control at signal-to-noise ratios (SNR) of interest.

We present ISI-free watermark signals that are designed via the Nyquist criterion. The filters that generate the ISI-free waveforms can be easily incorporated into any existing watermarking algorithm. Experimental results indicate good gains over methods that are not ISI-aware.

Finally, we design a linear equalizer to mitigate ISI in watermarking receivers. The design of the equalizer follows the well known technique of zero forcing [38]. Experiments indicate an improvement in performance at attack noise powers of interest.

Future work in this area may take any of the following directions.

To avoid the disadvantages of zero forcing, which leads to the classical noise

enhancement problem [38], we can use a minimum mean squared error (MMSE) equalizer. Another interesting alternative is to use non-linear techniques such as decision-feedback equalizers in watermarking systems. It has been shown [38] that these perform better than the linear methods such as the zero forcing or the MMSE equalizers. The optimum receiver¹ for channels with ISI and additive white Gaussian noise (AWGN) consists of matched filtering followed by maximum likelihood sequence estimation (MLSE). It will be interesting to apply a two-dimensional Viterbi algorithm [30] to implement the sequence estimation in watermarking applications.

This thesis assumes coherent detection at watermarking receivers. However, there are certain attacks such as rotation, cropping, scaling that may affect the synchronization at the receiver. Honsinger and Rabbani [21] have proposed some novel methods to recover synchronization at the receivers. It would be of interest to extend these methods in the context of our algorithms. Another method to achieve synchronization at the receivers employs the so called synchronization codes [38]. An interesting direction would be to design synchronization codes for our watermarking systems.

¹in the sense of minimum probability of error

REFERENCES

- [1] F. Balado, F. P. Gonzalez, and S. Scalise. Turbo coding for sample-level watermarking in the dct domain. In *Proc. IEEE ICIP*, volume 3, pages 1003–1006, October 2001.
- [2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. In *IBM Systems Journal*, volume 35, pages 313–336, 1996.
- [3] J. A. Bloom, I. J. Cox, T. Kalker, J. Linnartz, and M. L. Miller. Copy protection for dvd video. *Proceedings of the IEEE*, 87(7):1267–1276, July 1999.
- [4] B. Chen and G. Wornell. Dither modulation: a new approach to digital watermarking and information embedding. In *Proc. SPIE: Security and Watermarking of Multimedia Contents*, pages 342–353, January 1999.
- [5] B. Chen and G. Wornell. An information-theoretic approach to the design of robust digital watermarking systems. In *Proc. IEEE ICASSP*, pages 823–827, April 1999.
- [6] B. Chen and G. Wornell. Preprocessed and postprocessed quantization index modulation for digital watermarking. In *Proc. SPIE: Security and Watermarking of Multimedia Contents*, pages 48–59, January 2000.
- [7] B. Chen and G. Wornell. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, IT-47(4):1423–1443, May 2001.

- [8] Brian Chen. Design and analysis of digital watermarking: information embedding and data hiding systems. PhD Dissertation, MIT, Cambridge, June 2000.
- [9] M. H. Costa. Writing on dirty paper. *IEEE Transactions on Information Theory*, IT-29(3):439–441, May 1983.
- [10] I. J. Cox, J. Killian, F. T. Leighton, and T. Shannon. Secure Spread Spectrum Watermarking for Multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, December 1997.
- [11] I. J. Cox, M. L. Miller, and J. A. Bloom. Watermarking applications and their propoerties. In *International Conference on Information Technology:Coding and Computing*, pages 6–10, April 2000.
- [12] I. J. Cox, M. L. Miller, and J. A. Bloom. Digital watermarking. Morgan Kaufmann Publishers, October 2001.
- [13] I. J. Cox, M. L. Miller, and A. L. Mckellips. Watermarking as Communications with Side Information. *Proceedings of the IEEE*, 87(7):1127–1141, July 1999.
- [14] J. Eggers and B. Girod. Quantization effects in digital watermarking. *Signal Processing*, 81(2):239–263, February 2001.
- [15] J. Eggers and B. Girod. Informed watermarking. Kluwer Academic Publishers, 2002.
- [16] F. P. Gonzalez, J. R. Hernandez, and F. Balado. Approaching the capacity limit in image watermarking: a perspective on coding techniques for data hiding applications. *Signal Processing*, 81(6):1215–1238, June 2001.
- [17] F. Hartung and M. Kutter. Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7):1079–1107, July 1999.

- [18] J. R. Hernandez, M. Amado, and F. P. Gonzalez. Dct-Domain Watermarking techniques for still Images: Detector Performance Analysis and a new Structure. *IEEE Transactions on Image Processing*, 9(1):55–68, January 2000.
- [19] J. R. Hernandez, F. P. Gonzalez, 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 in Communications*, 16(4):510–524, May 1998.
- [20] J. R. Hernandez, F. Perez-Gonzalez, and J. R. Rodriguez. The impact of channel coding on the performance of spatial watermarking for copyright protection. In *Proc. IEEE ICASSP*, volume 5, pages 2973–2976, 1998.
- [21] C. Honsinger and M. Rabbani. Data embedding using phase dispersion. International Conference on Information Technology: Coding and Computing (Invited Paper), April 2000.
- [22] C. W. Honsinger and M. Rabbani. Method for generating an improved carrier for use in an image data embedding application. United States Patent 6,044,156, March 2000.
- [23] S. H. Jamali and T. Le-Ngoc. Coded-modulation techniques for fading channels. Kluwer Academic Publishers, 1994.
- [24] U. Kohl, J. Lotspiech, and M. A. Kaplan. Safeguarding digital library content and users: Protecting documents rather than channels. <http://www.dlib.org/dlib/september97/ibm/09lotspiech.html>, 1997.
- [25] J. Lacy, S. Quackenbush, A. Reibman, and J. Snyder. Intellectual property protection and digital watermarking. In *Information Hiding, Second International Workshop Proceedings*, volume 1525, pages 158–168, April 1998.

- [26] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk. Watermarking digital image and video data: A state-of-the-art overview. *IEEE Signal Processing Magazine*, 17(5):20–46, September 2000.
- [27] J. S. Lim. Two-Dimensional Signal and Image Processing. Prentice Hall, 1991.
- [28] C-Y. Lin and S. F. Chang. A robust image authentication algorithm surviving jpeg compression. In *SPIE: Storage and Retrieval Image/Video Databases*, January 1998.
- [29] C-Y. Lin and S. F. Chang. A robust image authentication algorithm surviving jpeg compression. In *SPIE: Security and Watermarking of Multimedia Contents*, January 1999.
- [30] R. Link and S. Kallel. Optimal use of markov models for dpcm picture transmission over noisy channels. *IEEE Transactions on Communications*, 41(10):1702–1711, October 2000.
- [31] J. Linnartz, T. Kalker, and J. Haitzma. Detecting electronic watermarks in digital video. In *Proc. IEEE ICASSP*, pages 2071–2074, March 1999.
- [32] M. F. Mansour and A. H. Tewfik. Efficient decoding of watermarking schemes in the presence of false alarms. In *Proc. of IEEE Workshop on Multimedia and Signal Processing*, pages 523–528, October 2001.
- [33] M. L. Miller, G. Doerr, and I. J. Cox. Dirty -paper trellis codes. In *Proc. IEEE ICIP*, pages 129–132, September 2002.
- [34] P. Moulin, M. K. Mihcak, and G. I. A. Lin. An information theoretic model for image watermarking and data hiding. In *Proc. IEEE ICIP*, September 2000.

- [35] P. Moulin and J. A. O'Sullivan. Information-theoretic analysis of information hiding. preprint, 1999.
- [36] C. I. Podilchuk and E. J. Delp. Digital watermarking: Algorithms and Applications. *IEEE Signal Processing Magazine*, 18(4):33–46, July 2001.
- [37] C. I. Podilchuk and W. Zeng. Image-adaptive watermarking using visual models. *IEEE Journal on Selected Areas in Communications*, 16(4):525–539, May 1998.
- [38] J. G. Proakis. Digital Communications. McGraw Hill, Fourth Edition, 2001.
- [39] D. L. Robie and R. M. Mersereau. Video error correction using steganography. In *Proc. IEEE ICIP*, pages 207–226, October 2001.
- [40] J. R. Smith and B. O. Comiskey. Modulation and information hiding in images. In *Information Hiding, First International Workshop Proceedings*, pages 207–226, June 1996.
- [41] H. Stone. Analysis of attacks on image watermarks with randomized coefficients. NEC Technical Report, 1996.
- [42] A. Z. Tirkel, G. A. Rankin, R. van Schyndel, W. J. Ho, N. R. A. Mee, and C. F. Osborne. Electronic watermark. In *Proc. Digital Image Computing, Technology and Applications*, pages 666–672, December 1993.
- [43] G. Ungerboeck. Channel coding with multilevel/phase signals. *IEEE Transactions on Information Theory*, 28:55–67, January 1982.
- [44] G. Ungerboeck. Trellis-coded modulation with redundant signal sets, Part I: Introduction. *IEEE Communications Magazine*, 25(2):5–11, February 1987.
- [45] G. Ungerboeck. Trellis-coded modulation with redundant signal sets, Part II: State of the art. *IEEE Communications Magazine*, 25(2):12–21, February 1987.

- [46] P. P. Vaidyanathan and T. Q. Nguyen. Eigenfilters: A new approach to Least-Squares FIR filter design and applications including Nyquist filters. *IEEE Transactions on Circuits and Systems*, cas-34(1):11–23, January 1987.
- [47] C. De Vleeschouwer, J. F. Delaigle, and B. Macq. Invisibility and application functionalities in perceptual watermarking - an overview. *Proceedings of the IEEE*, 90(1):64–77, January 2002.
- [48] S. Voloshynovskiy and S. Pereira amd I. T. Pun. Attack modelling: Towards a second generation watermarking benchmark. *Signal Processing*, 81:1177–1212, 2001.
- [49] S. B Wicker. Error Control Systems for Digital Communication and Storage. Prentice Hall, 1995.
- [50] R. B. Wolfgang and E. J. Delp. Fragile watermarking using the vw2d watermark. In *Proc. Electronic Imaging'99*, pages 204–213, January 1999.

VITA

Vimal Thilak was born in Madras, India on February 16, 1978, the son of Krishna Thilak and Vanaja Thilak. After completing his work at the St. Joseph's College, Bangalore, India, in 1995, he entered Sri Jayachamarajendra College of Engineering at Mysore, India. He graduated with a Bachelor of Engineering in Electronics and Communication Engineering in 1999. He was employed by Lucent Technologies, Bangalore, India during the summer of 2000. In September 2000, he entered the Graduate School of The University of Texas at Dallas where he began full-time work towards a Master of Science in Electrical Engineering degree.