QUANTIZATION BASED DATA HIDING STRATEGIES WITH VISUAL APPLICATIONS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ERSİN ESEN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
ELECTRICAL AND ELECTRONICS ENGINEERING

FEBRUARY 2010

Approval of the thesis:

QUANTIZATION BASED DATA HIDING STRATEGIES WITH VISUAL APPLICATIONS

submitted by **ERSİN ESEN** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Electrical and Electronics Engineering Department, Middle East Technical University** by,

Prof. Dr. Canan Özgen

Dean, Graduate School of **Natural and Applied Sciences** _____

Prof. Dr. İsmet Erkmen

Head of Department, **Electrical and Electronics Engineering** _____

Assoc. Prof. Dr. A. Aydın Alatan

Supervisor, **Electrical and Electronics Engineering, METU** _____

Examining Committee Members

Prof. Dr. Murat Aşkar
Electrical and Electronics Engineering, METU _____

Assoc. Prof. Dr. A. Aydın Alatan
Electrical and Electronics Engineering, METU _____

Assoc. Prof. Dr. Kıvanç Mıhçak
Electrical and Electronics Engineering, Boğaziçi University _____

Assist. Prof. Dr. Hüsrev Taha Sencar
Computer Engineering, TOBB University _____

Assoc. Prof. Dr. İsmail Avcıbaş
Electrical and Electronics Engineering, Başkent University _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: **ERSİN ESEN**

Signature:

ABSTRACT

QUANTIZATION BASED DATA HIDING STRATEGIES WITH VISUAL APPLICATIONS

Esen, Ersin

Ph.D., Department of Electrical and Electronics Engineering

Supervisor: Assoc. Prof. Dr. A. Aydın Alatan

February 2010, 119 pages

The first explored area in this thesis is the proposed data hiding method, TCQ-IS. The method is based on Trellis Coded Quantization (TCQ), whose initial state selection is arbitrary. TCQ-IS exploits this fact to hide data. It is a practical multi-dimensional that eliminates the prohibitive task of designing high dimensional quantizers. The strength and weaknesses of the method are stated by various experiments.

The second contribution is the proposed data hiding method, Forbidden Zone Data Hiding (FZDH), which relies on the concept of "forbidden zone", where host signal is not altered. The main motive of FZDH is to introduce distortion as much as needed, while keeping a range of host signal intact depending on the desired level of robustness. FZDH is compared against Quantization Index Modulation (QIM) as well as DC-QIM and ST-QIM. FZDH outperforms QIM even in 1-D and DC-QIM in higher dimensions. Furthermore, FZDH is comparable with ST-QIM for certain operation regimes.

The final contribution is the video data hiding framework that includes FZDH, selective embedding and Repeat Accumulate (RA) codes. De-synchronization due to selective embedding is handled with RA codes. By means of simple rules applied to the embedded frame markers, certain level of robustness against temporal attacks is introduced. Selected coefficients are used to embed message bits by employing multi-dimensional

FZDH. The framework is tested with typical broadcast material against common video processing attacks. The results indicate that the framework can be utilized in real life applications.

Keywords: Data hiding, watermarking, Quantization Index Modulation, Distortion Compensation, Scalar Costa Scheme, Forbidden Zone Data Hiding, selective embedding

ÖZ

NİCEMLEME TABANLI BİLGİ SAKLAMA STRATEJİLERİ VE GÖRSEL UYGULAMALARI

Esen, Ersin
Doktora, Elektrik-Elektronik Mühendisliği Bölümü
Tez Yöneticisi: Doç. Dr. A. Aydın Alatan

Şubat 2010, 119 sayfa

Bu tezde ilk olarak, önerilen TCQ-IS yöntemi ele alınmaktadır. Bu yöntem, Kafes Tabanlı Nicemleme'ye (TCQ) dayanmaktadır. TCQ-IS ilk durum seçimindeki belirsizliği kullanmaktadır. Yöntem çok boyutlu ve pratik olması sebebiyle oldukça zorlayıcı olan çok boyutlu nicemleme tasarımını elimine eder. Yöntemin kuvvetli ve zayıf yönleri deneyler aracılığıyla belirtilmiştir.

Tezin ikinci katkısı, önerilen yeni bilgi saklama yöntemi, Yasak Bölgeli Bilgi Saklama'dır (FZDH). FZDH, yeni sunulan konakçı sinyalinin değiştirilmeyecek kısımlarını tanımlayan "yasak bölge" kavramına dayanır. FZDH'nin temel motivasyonu konakçı sinyalinin bazı bölümlerini hiç değiştirmemek ve bozunumu gerekli olduğu miktarda gerçekleştirmektir. FZDH, Nicemleme Dizin Modülasyonu (QIM), DC-QIM ve ST-QIM yöntemleri ile karşılaştırılmaktadır. FZDH, QIM'i 1-B'de bile geçerken daha yüksek boyutlardaDC-QIM'den de iyi sonuçlar vermektedir; ST-QIM ile ise belirli durumlarda benzer performans elde etmektedir.

Bu tezin sonuncu katkısı, FZDH, seçimli gömme ve Yinele Biriktir (RA) kodlarını içeren bir video bilgi saklama çerçevesidir. Seçimli gömmeden kaynaklanan senkronizasyon

kaybının üstesinden RA kodları ile gelinmektedir. Gömülen kare senkronizasyon işaretleriyicilerine uygulanan basit kurallar sayesinde zamansal ataklara karşı belirli bir gürbüzlük elde edilmektedir. Seçilen katsayılar, FZDH'nin çok boyutlu hali ile mesaj bitlerini saklamak için kullanılmaktadır. Önerilen çerçeve tipik televizyon verisi ile sık kullanılan video işleme ataklarına karşı denenmiştir. Sonuçlar, önerilen çerçevenin gerçek hayat uygulamalarında başarıyla kullanılabileceğini göstermektedir.

Anahtar Kelimeler: Bilgi saklama, görünmez damgalama, Nicemleyizi Dizin Modülasyonu, Skalar Costa Yöntemi, Yasak Bölgeli Bilgi Saklama, seçimli gömme

To my family.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my advisor, Prof. A. Aydın Alatan, without whom this long course of study would not be possible.

I am also indebted to the members of the Thesis Monitoring Committee, Prof. Murat Aşkar and Prof. Kıvanç Mıhçak, for their valueable comments and suggestions throughout this study. Additionally, I have to admit that I highly benefited from working together with Prof. Kıvanç Mıhçak at Microsoft Research.

I would like to express my gratefulness to the rest of the Thesis Jury members, Prof. Hüsrev Taha Sencar and Prof. İsmail Avcıbaş, for their effort in examining this thesis and comments.

I have to express my special thanks to my colleagues Dr. Alper Koz, Tuğrul Kağan Ateş, my intern Zafer Doğan for their valueable involvement and contributions in various aspects of the work contained in this thesis.

Any acknowledgement would be incomplete without mentioning the efforts of my teachers. Starting from my primary school teacher, Mrs. Senar Doğantepe, I would like to thank by heart to all my teachers and instructors at Karadeniz Ereğli Cumhuriyet İlkokulu, Karadeniz Ereğli Anadolu Lisesi, İstanbul Atatürk Fen Lisesi, Bilkent University, and Middle East Technical University.

Finally, I would like to express my sincere thankfulness to my parents, Ali and Emine Esen, my sisters, Esra and Feyza, and all members of my large family, whose existence made life more bearable.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

NOTATION

- s: host signal
- N: dimension of the host signal
- m: embedded data
- $\mathcal{M}$: order of m
- $q()$: quantizer
- $q_m()$: quantizer used for m
- Δ: quantizer cell width
- $\mathcal{E}$: embedding function
- x: marked signal
- n: channel/attack noise
- w: additive watermark
- y: received marked signal
- $\mathcal{D}$: decoding function
- $d(.,.)$: distance function
- $\hat{m}$: decoded data
- $d()$: dither sequence belonging to a specific message m
- α: DC-QIM control parameter
- r: FZDH control parameter
- Λ: lattice
- Λ_m: lattice associated with m
- p: projection direction
- Q(): complementary error function,
- P(E): probability of decoding bit error
- QIM: Quantization Index Modulation
- DM: Dither Modulation
- DC-QIM: Distortion Compensated Quantization Index Modulation
- ST-QIM: Spread Transform Quantization Index Modulation
- SCS: Scalar Costa Scheme

- FZDH: Forbidden Zone Data Hiding
- FZ: Forbidden Zone
- AZ: Allowed Zone
- TCQ: Trellis Coded Quantization
- bps: bits per sample
- fps: frame per second
- iid: independent and identically distributed
- pdf: probability density functions
- TCQ-IS: Trellis Coded Quantization Initial State
- TCQ-PS: Trellis Coded Quantization Path Selection
- VQ: Vector Quantizer
- WNR: Watermark to Noise Ratio
- SNR: Signal to Noise Ratio
- PSNR: Peak Signal to Noise Ratio
- AWGN: Additive White Gaussian Noise
- HVS: Human Visual System
- RA Codes: Repeat Accumulate Codes

CHAPTER 1

INTRODUCTION

Data hiding is the process of imperceptibly embedding some information into a medium, which can be related to the information content or not. Since the early ages, data hiding is used for mainly secret communication. In the modern age, emergence of the new media types and novel needs aroused as a consequence resulted in the revival of the data hiding field. The activity of the field can be seen in Figure 1.1. The very first publication [1] in the given source is encountered in 1994. Following years witnessed an ever increasing trend. Current momentum implies that this trend will not change in the near future.

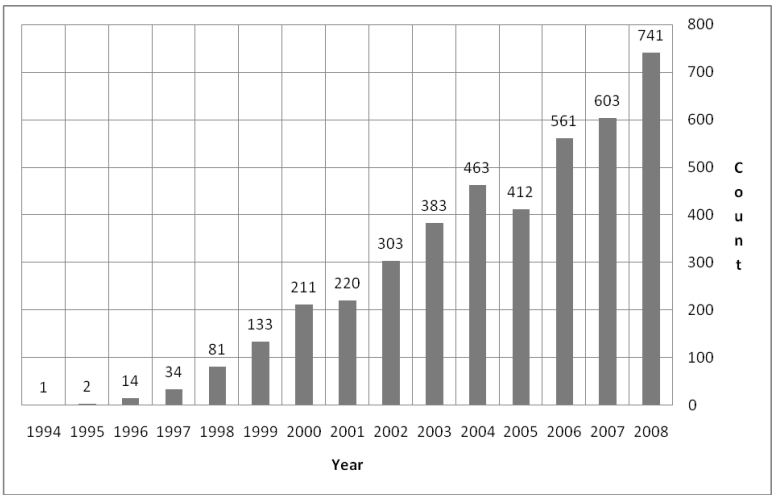


Figure 1.1: Number of publications related to "watermarking[1]" per year. (Source: IEEE Xplore[2])

[1] "Watermarking" is used in the search instead of "data hiding", since the latter can be mixed with the same term in software engineering field and sometimes the latter is not preferred in the metadata.
[2] http://ieeexplore.ieee.org.

Recent areas of interest within the field is tried to be captured by means of the frequency of the key terms, which is shown in Figure 1.2. Based on this observation, one can claim that recent trend is mostly focused on applications. As a result of hundreds of works in the last fifteen years, data hiding field has reached to a certain level of maturity and hence, the developed framework is applied to many different areas.

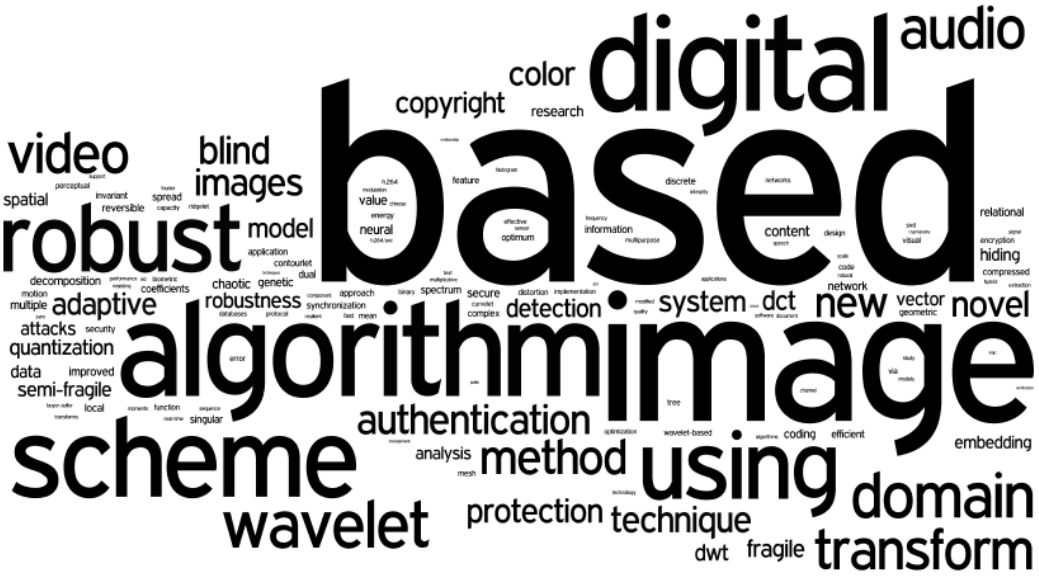


Figure 1.2: Frequency of the words (larger font size corresponds to a more frequent word) in the titles of the publications in 2008 related to “watermarking”. (Source: IEEE Xplore)

1.1 Motivation

The motivations of this thesis dwell on three major points.

- *The necessity for practical higher dimensional data hiding codes.* Scalar schemes cannot achieve the theoretical limits, which can be approached asymptotically by random and infinite length codebooks. Naturally, these schemes are impractical and hence, design of manageable higher dimensional data hiding codes is a significant part of the field.
- *Adjusting trade-off between robustness and imperceptibility by practical means*. Data hiding can be considered similar to the joint source-channel coding. A data hiding code should be a good source code (minimal distortion) and at the same time a good channel code (maximal separation). Hence, there exists a trade-off between robustness (channel code) and imperceptibility (source). One cannot increase robustness without increasing the embedding distortion (with the collateral risk of sacrificing imperceptibility). However, the way this adjustment is performed is crucial and constitutes the topic of many works in the field.

- *Design of end-to-end real-life visual applications.* Visual domain is the most preferred domain for data hiding applications. There exists various aspects for a complete system; however most of the works deal with certain parts of the problem. A complete application should take into account robustness-invisibility trade-off, Human Visual System adaptation, error correction, data packet handling, temporal synchronization and similar issues. Hence substantial effort is required to design and develop such systems. Design of a complete video data hiding application constitutes the last motivation of this dissertation.

1.2 Main Contributions of the Thesis

The main objective of this thesis is to explore quantization based data hiding methods with visual applications as its primary focus. Major contributions of the thesis made in this perspective are summarized in the following items complying with the chronological advance.

- The first contribution of the thesis is the outcome of the quest for practical high dimensional data hiding code, namely TCQ-IS, which is explored in Chapter 4. TCQ-IS depends on Trellis Coded Quantization. A simple redundancy in the conventional TCQ structure is exploited to hide data. The proposed method is applied to image data hiding and its strength and weaknesses are reported.

- The second contribution of the thesis is the outcome of the search for better adjustment of the trade-off between imperceptibility and robustness: Forbidden Zone Data Hiding (FZDH), which is explored in Chapter 5. FZDH approaches this trade-off from a different perspective and yields promising results.

- The final contribution of the thesis is a complete video data hiding framework, which is described in Chapter 6. The framework incorporates selective embedding, error correction, erasure handling, temporal synchronization, and FZDH, as well as other conventional data hiding methods. The framework is tested with common video processing attacks. System parameters, for which error-free decoding can be attainable, are determined and reported as a result of the experiments.

1.3 Outline of the Thesis

This thesis is organized as follows.

Chapter 2 gives an overview of the data hiding problem. The formulation of this problem and the general framework are briefly introduced. Generic terminology and notations utilized throughout the thesis are given. Additionally, fundamental requirements, types and applications of data hiding are summarized.

Chapter 3 presents a review of quantization based data hiding. Conventional quantization based methods are described and an image data hiding application is presented.

Chapter 4 introduces the proposed high dimensional quantization based data hiding method, namely TCQ-IS.

Chapter 5 presents the proposed data hiding paradigm, Forbidden Zone, and the data hiding method, namely Forbidden Zone Data Hiding, that relies on this concept.

Chapter 6 proposes the video data hiding framework that contains the proposed data hiding method and error correction coding in order to obtain an error-free framework for various common attacks.

Chapter 7 summarizes the dissertation and its main contributions with some concluding remarks.

CHAPTER 2

DATA HIDING

Data hiding is essentially a communication system, in which some data is conveyed within a host medium and transmitted to the receiver.

Following the terminology in [2], we utilize the term *data hiding* interchangeably with *information embedding/hiding*. The general term of *data hiding* encapsulates hiding some data, which can be related to the host or not, imperceptibly and/or secretly. In this sense, it contains *steganography* (covered writing) for secret communication and *watermarking* for copyright protection.

In this chapter, we briefly introduce the framework and fundamental notions of data hiding.

2.1. Framework

The framework of data hiding is shown in Figure 2.1. It is composed of two major operations (embedding and decoding) and the channel laying in between.

In the embedding step, host signal is mapped to a marked signal depending on the data to be hidden. System parameters denote the required parameters specific to the utilized data hiding method. The same parameters should also be available to the decoder. The optional cryptographic key is required for security applications.

The channel refers to the modifications made on the marked signal before the receiver.

The decoder operates on the received signal and extracts the hidden data. The existence of the host signal at the decoder is optional.

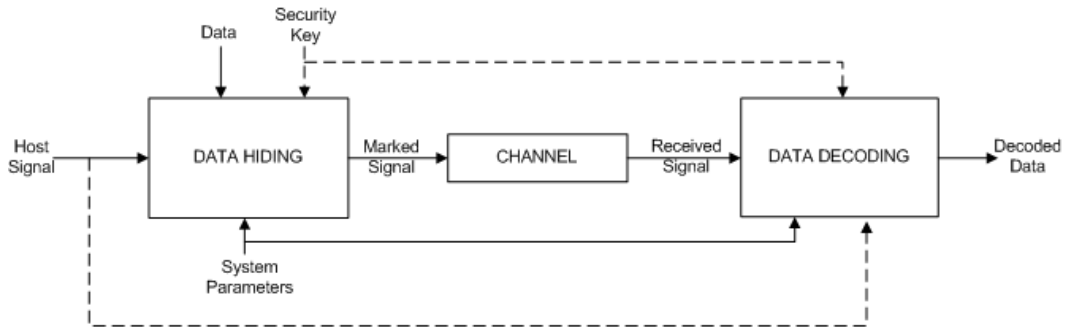


Figure 2.1: Data hiding framework. *Dashed* lines correspond to optional parameters.

We utilize the following definitions in this framework.

- *Host Signal*: The medium into which the data will be hidden. It can be any suitable type such as image, audio, video, or even text [3]. The main requirement on the host signal is that it should have some sort of redundancy that can be used to hide data imperceptibly. This redundancy depends on the type of the signal. For instance, for the visual case Human Visual System (HVS) whereas for the audio case Human Auditory System (HAS) should be taken into count. In some contexts *cover* [2], [4] or *original* [5] terms are utilized instead of the term *host*. However, we prefer the term *host* due to its generic meaning.
- *Message*: The data to be hidden. We utilize message and data interchangeably. They contain all sorts of data including watermarks and secret communication messages.
- *Marked Signal*: The medium which conveys the hidden data. Its type is identical to the host signal. In some contexts, *stego* [5] or *embedded object* [4] are utilized instead of the term *marked signal*.

- *Embedding Function*: The function that maps the host signal to marked signal according to the message.
- *Embedding Distortion*: The distortion introduced to the host signal as a result of the embedding operation. In other words, it is equivalent to the difference between host signal and marked signal. In general, Euclidean distance is utilized to capture the embedding distortion. However, different distance metrics based on perceptual models can also be employed [6].
- *Security Key*: The cryptographic key optionally incorporated to the framework to provide security for the hidden message.
- *System Parameters*: Method specific parameters required for embedding and decoding.
- *Attack*: Any sort of modification on the marked signal. It can intentional or unintentional. It depends on the host signal type.
- *Received Signal*: The signal received by the decoder, in other words attacked marked signal.
- *Decoding Function*: The function that decodes the hidden data from the received signal.
- *Blind Data Hiding*: The mode of data hiding, in which host signal is not required at the decoder. In some contexts the term *public* [2] or *oblivious* [5] is utilized.
- *Nonblind Data Hiding*: The mode of data hiding, in which the decoder requires the host signal. In some contexts *private* [2], [4], *informed* [2] or *non-oblivious* [5] is utilized.

2.2. Fundamental Data Hiding Requirements

There are four main requirements of a typical data hiding system: *imperceptibility*, *robustness*, *capacity*, and *security*. The degree of importance of any requirement depends on the type of the application. Some applications may not request some of these basic requirements, except imperceptibility, which is indispensable for most of the data hiding applications.

- *Imperceptibility*: There should not be perceptual degradation due to data hiding. Ideally one could not be able to distinguish host signal and marked signal. Marked signal should be similar to the host signal:

$$x_m \approx s, \qquad \forall m \tag{2.1}$$

  The similarity and the tolerable distortion are determined with respect to the host signal type. For visual host signal HSV is taken into account and for aural host signal HAS is taken into account.

- *Robustness*: It is the dependability and strength of a data hiding system after certain attacks, in terms of correctly decoding the hidden data. The degree of robustness is determined by the application. In general, data hiding algorithms are designed for certain attacks and allowable distortion levels.

- *Capacity*: It refers to the feasible number of message bits that can be hidden in the host signal. The amount may range from one bit to millions of bits, which depends on the application.

- *Security*: For some applications security may be crucial. In that case, algorithms should secure the hidden data so that adversaries can not intrude or interfere by any means.

  We should note that security is not within the scope of this thesis, we target generic non-private applications.

2.3. Types

According to the ingredients and targets, there are various types of data hiding applications. In this section, we briefly mention the major types.

- *Blind vs. Non-blind*: According to the existence of the host signal at the decoder, methods are grouped into two categories: *blind* and *non-blind*. In blind methods host signal is not used, whereas non-blind methods strictly require the host signal. There are also *semi-blind* (also called *semi-private* [4]) methods, where partial information about the host signal is available at the decoder. Within our scheme, *system parameters* are specific to the algorithm; hence, existence of the system parameters at the decoder does not alter being blind. In this thesis, our focus is on the *blind* case.

- *Fragile vs. Robust*: This categorization refers to the degree of the robustness. In some cases, hidden information is expected to withstand a very limited set of attacks, since detection of the removal is also valuable. These types of methods are called *fragile*. They are mainly used in authentication applications as in [7], [8]. On the other hand, hidden information is expected to survive against a broader range of attacks. In this thesis, our focus is on the *robust* case.

- *Spread Spectrum*: Spread spectrum watermarking, which is proposed by Cox *et. al.* [9], is one of the earliest watermarking algorithms. Watermarking problem is viewed as a communications problem and message is spread to the whole spectrum for security and robustness purposes. Spread spectrum technique is widely used in the field. For instance Kalker et al. [10] applied to video watermarking and Kirovski and Malvar [11] applied to audio watermarking.

- *Quantization based*: This type refers to the methods that map the host signal to marked signal by means of quantizers. The knowledge of quantizers suffice to decode hidden data; hence quantization based methods are *blind*. Quantization based methods are essentially binning schemes [6]. They have asymptotically equivalent performances with nonblind methods [12]. In this thesis, this type of methods forms the focus of the scope.

2.4. Applications

Data hiding gained popularity firstly due to copyright protection. However, as time passed by various data hiding applications emerged. In this section, we provide a brief list of common applications.

- *Copyright Protection*: Digital watermarking is utilized for the proof of ownership. Some information related (content owner, production information, etc.) to the host media is embedded with the purpose of copyright protection. This type of applications involves extensive security issues as a result of the existence of adversaries. There exist various applications of this kind. For instance, Digimarc [13] provides commercial solutions for all multimedia types. Furthermore, DVDs contain such a mechanism [14] to provide copy protection.

- *Authentication*: It refers to determining the authenticity of the received signal by means of the hidden data. Mostly *fragile* data hiding is used for this purpose as in image and video authentication methods [7], [8]. In [15], a multimodal framework is proposed for multimedia authentication. Recent works combine *reversible* data hiding and authentication as in [16], [17]. Authentication can be also used to gain information about the attack. For instance modified regions of an image can be located [18].

  Authentication can be useful for certain application domains, such as medical and military archives. In this case, reversible data hiding constitutes a viable choice due to the importance of the host signal itself.

- *Fingerprinting*: In this application, a marked signal is distributed to different users with user specific information embedded in the host signal. The target is to identify the user of the marked signal, such that in case of a leakage the user can be identified. This application is important for the content distributors.

- *Steganography* (covered writing): This refers to secret communication by means of data hiding. The data is hidden in such a way that the existence of the hidden data is not detectable. The problem of detecting the hidden data is called *steganalysis.*

- *Copy Detection*: It refers to the detection of the copies of the original content after various attacks. Data hiding provides an active solution for this problem. Some information is embedded in the distributed content and copies are detected by the hidden data. On the other hand, content based copy detection provides a passive solution for the same problem. In this case, content itself is assumed to be hidden data.

  In the presence of online media distributors, copy detection is crucial for duplicate removals as well as preventing abuses.

- *Broadcast Monitoring (Auditing)*: This refers to tracking the marked signal in a broadcast environment. The problem is similar to *copy detection*. However, the attack is the broadcast medium itself. Therefore, broadcast monitoring is expected to withstand milder modifications with respect to *copy detection*.

  There are various broadcast monitoring applications and commercial products. Depovere *et. al.* [19] proposed a system for video monitoring. A similar system for audio is proposed in [20]. There are also commercial companies [21], [22], [23] that provide broadcast monitoring solutions for audio and video.

- *Multimedia Indexing*: Data hiding can also be used for multimedia indexing. Indexing is used for efficient retrieval of identical or similar contents. In this respect, hiding index values in the content itself introduces the advantage that index values are conveyed with the content itself and no additional information is needed. A typical system is presented in [24]. However, the disadvantage of such an approach is the requirement for the extraction of index values before retrieval. This limitation restricts its usability.

- *Quality Measurement*: Assessment of the perceptual quality of the media is critical for some application domains. Data hiding provides an automatic way to this problem. A typical audio quality measurement method is presented in [25].

- *Device Identification*: Devices can be identified by using their specific characteristics exposed onto their outputs. In this regard, data hiding can be used to identify the device by embedding device specific information into its output. In this way, printers or digital cameras can be identified. Khanna *et. al.* [26] present a review of watermarking based device identification and provide a comparison against identification based on intrinsic features of the device.

2.5. Attacks

Attack is the modification of the marked signal before the decoder. Depending on the intention, they can be grouped into two major types: *malicious* (*intentional*) and *non-malicious* (*non-intentional*). Malicious attacks are related to security applications, in which adversaries try to detect the existence of the hidden data or decode/remove the hidden data. On the other hand, non-malicious attacks are the common modifications that the marked signal is exposed to in the channel.

In general, there is a certain limit on the amount of the attack, since received signal should still be perceptually similar to the host signal. However, the existence of the attack deteriorates the communication performance between encoder and decoder.

In this thesis, our scope includes only non-malicious attacks. We do not target security applications.

Possible visual attacks can be listed as follows.

- Compression
- Noise Addition

    - AWGN
    - Salt & Pepper Noise
- Filtering
- Intensity Adjustments
    - Contrast/Brightness Adjustment
    - Histogram Equalization
- Morphological Operations
- Geometric Attacks (for a review refer to [27])
    - Scaling
    - Cropping
    - Rotation
    - Bending
    - Warping
    - Shear

There exists benchmarking programs that evaluate the performances against various attacks. Stirmark [28] is one of the mostly used benchmarking programs. Checkmark [29] and Optimark [30] can also be used for the same purpose.

The relation between attacks and applications are given in Table 2.1.

Table 2.1: Attack and application relation (+ denotes obligatory robustness, o denotes optional robustness, and – denotes no relation).

Application vs. Attack	***Compression***	***Broadcast Channel Noise***	***Filtering***	***Intensity Change***	***Morphological Operations***	***Geometric Attacks***
Copyright Protection	+	+	+	+	+	+
Authentication	+	o	o	o	o	o
Fingerprinting	+	-	+	+	+	+
Steganography	+	o	o	o	o	o
Copy Detection	+	+	+	+	+	+
Broadcast Monitoring	+	+	-	+	-	-
Multimedia Indexing	+	-	o	o	o	o
Quality Measurement	+	+	+	+	+	+
Device Identification	+	-	o	o	o	o

CHAPTER 3

QUANTIZATION BASED DATA HIDING

In quantization based data hiding, host signal is modified using quantizers. Main process is to partition the host signal range into disjoint sets, whose members are determined using the reconstruction points of the quantizers. Each message bit is associated with a specific quantizer. During data hiding, corresponding quantizer is utilized. At the decoder, host signal is not required; only quantizer parameters are needed. Each candidate message is tested and the one with the minimum distance is determined as the hidden message.

Quantization based data hiding can be considered analogous to binning technique widely used in communication theory. For instance, binning is used in the encoding with side information at the transmitter only problem [31]. In [32], it is shown that channel capacity does not depend on the side information. This problem is analogous to blind data hiding, where host signal constitutes the side information. The analogy states that blind data hiding methods can achieve the capacity of non-blind data hiding methods asymptotically. Furthermore, capacity analysis in [32] formed a basis for capacity analysis of quantization based data hiding methods.

Quantization based methods can be encapsulated within Quantizaton Index Modulation (QIM) framework, which is introduced by Chen and Wornell in 1999 [33]. All data hiding methods that contain quantization or some form of binning is a member of QIM family. For instance, one of the oldest and simplest data hiding method of least significant bit modulation is also QIM type. Chen and Wornell introduced different types of QIM as Dither Modulation (DM), Distortion Compensated QIM (DC-QIM), and Spread Transform QIM (ST-QIM) [33], [12]. Independently, Eggers introduced Scalar Costa Scheme [34], which is equivalent to DC-QIM. Similarly, Quantized Projection method of Perez-Gonzalez [35] is equivalent to ST-QIM. Methods that involve additional

post-processing are also introduced as in error thresholding method of Ramkumar and Akansu [5].

A comprehensive review of quantization based methods, as well as decoding error and capacity analysis, can be found in [6]. In general, host statistics is not taken into account as a result of high-resolution quantization assumption (i.e. embedding distortion is much lower than the host power). The decoding error analysis of scalar quantization based methods, which involves host statistics, can be found in [36].

In this chapter, we give brief definitions of the fundamental quantization based methods: QIM, DC-QIM, Lattice-QIM, ST-QIM, and Error Thresholding variant of QIM. Finally, we apply QIM to image data hiding and report its decoding error performance against various attacks.

3.1. Quantization Index Modulation (QIM)

The popular data hiding technique QIM is introduced in [33]. QIM corresponds to selection of a quantizer index (or a sqeuence of indices) depending on the embedded data and then quantization of the host signal using the associated quantizer (or a sequence of quantizers). In this respect, generic embedding function for QIM is given in (3.1).

$$x = q_m(s) \tag{3.1}$$

Chen and Wornell introduced a convenient and simple structure as Dither Modulation (DM) [33], [12]. In DM, a base quantizer is utilized. All the other quantizers are obtained by shifting the quantization cells and reconstruction points of the base quantizer via a dither sequence. The dither sequence is modulated with m and different embedding functions are generated. Embedder function of DM is given in (3.2).

$$q_m(s) = q(s + d(m)) - d(m) \tag{3.2}$$

Dither sequence can be pseudo-randomly chosen for security purposes. Otherwise, constant values are sufficient with the constraint that dither values are separated as far as possible for different *m*. One of the most commonly used dither sequence is given in (3.3). The embedder functions (for *m*=0 and *m*=1) obtained using this dither sequence and Δ=1 are shown in Figure 3.1.

$$d(m) = \begin{cases} \Delta/4, m = 0 \\ -\Delta/4, m = 1 \end{cases} \tag{3.3}$$

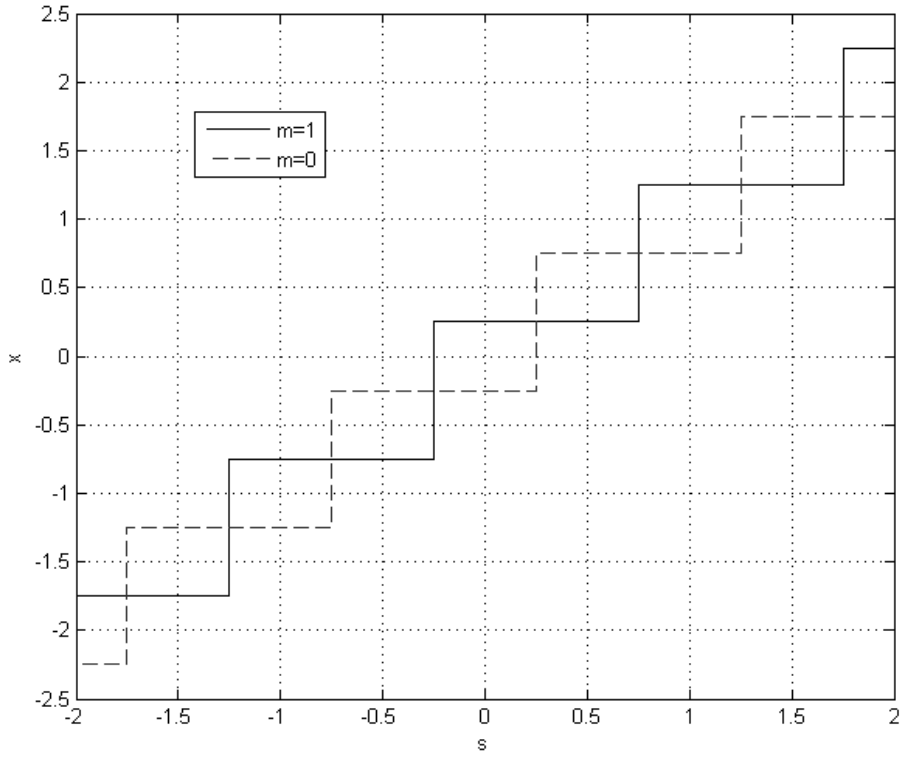


Figure 3.1: Sample embedding functions of QIM (solid line indicates the embedding function of *m*=1, whereas dashed line represents the case for *m*=0).

QIM decoder is a minimum distance decoder. The closest reconstruction point to the received signal is found. The index of the associated quantizer yields the extracted data:

$$\hat{m} = \arg\min_{m\in\{0,1\}} \|y - y_m\|, \tag{3.4}$$

where $y_m=q_m(y)$.

3.2. Distortion-Compensated QIM (DC-QIM)

Regular QIM performs poorly for low WNR. Chen introduced DC-QIM [12] as a remedy for this problem. DC-QIM is essentially a post-processing after QIM. First, the minimum distance (d_{min}) between quantizers is increased by a scale parameter ($0<\alpha<1$), which leads to greater robustness to channel noise. However, embedding distortion is also increased by a factor $1/\alpha^2$. At the second stage, a fraction (1- α) of the additional embedding distortion is added back to the quantization value in order to compensate this additional distortion. The embedding function of DC-QIM is given in (3.5)

$$x = q_m(\alpha s) + (1-\alpha)s \tag{3.5}$$

Independently, Eggers introduces Scalar Costa Scheme (SCS) [34], which is an equivalent form of DC-QIM. The embedder function of SCS is given in (3.6). Both embedding functions share the same characteristics.

$$x = s + \alpha(q_m(s) - s) \tag{3.6}$$

A typical embedding function pair of DC-QIM is shown in Figure 3.2 It is clear that embedding functions are more concentrated around $x=s$ line than QIM.

The distortion compensation term can be treated as interference or noise during decoding [12]. Hence the overall noise is the addition of the channel noise and the additional distortion compensation term, $(1-\alpha)\varepsilon/\alpha^2$. Then the SNR at decoder becomes:

$$SNR(\alpha) = \frac{d_{\min}^2/\alpha^2}{(1-\alpha)^2\varepsilon/\alpha^2 + \sigma_n^2} = \frac{d_{\min}^2}{(1-\alpha)^2\varepsilon + \alpha^2\sigma_n^2} \quad , \tag{3.7}$$

where d_{min} is the minimum distance between quantizers, ε is the embedding distortion and σ_n^2 is the channel noise power. Then, the optimal α that maximizes the SNR is given by:

$$\alpha = \frac{WNR}{1+WNR} \quad . \tag{3.8}$$

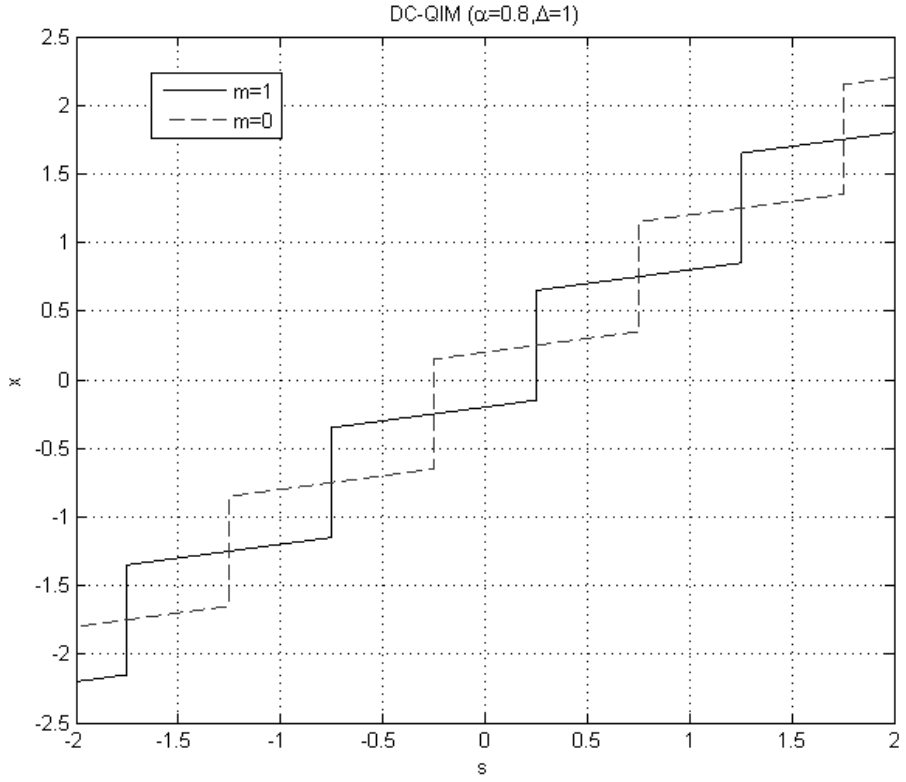


Figure 3.2: Sample embedding functions of DC-QIM (solid line indicates the embedding function of *m*=1, whereas dashed line represents the case for *m*=0).

Similar to QIM, minimum distance decoder is used for DC-QIM as in (3.9).

$$\hat{m} = \arg\min_{m\in\{0,1\}} \|y - y_m\| \tag{3.9}$$

3.3. Lattice QIM

An *N*-dimensional lattice, Λ, is a discrete subgroup of the Euclidean space R^N with addition operation, as

$$\lambda_1 \epsilon \Lambda \text{ and } \lambda_2 \epsilon \Lambda \rightarrow \lambda_1 \pm \lambda_2 \epsilon \Lambda \, . \tag{3.10}$$

Λ can be defined by using an *N* by *N* dimensional generator matrix G (which is non-unique):

$$\Lambda = \{\lambda = Gx: x \epsilon Z^N\}. \tag{3.11}$$

A *coset* of Λ is defined as a translated version of it. If $x \epsilon R^N$ then $(x + \Lambda)$ is a coset of Λ.

For quantization modulation, nested lattices are used. In order to obtain a nested-lattice pair, a *sublattice*, $\Lambda`$, of $\Lambda$ is formed. The generator matrix of $\Lambda`$, G`, is obtained by subsampling G:

$$G`=JG, \tag{3.12}$$

where J_{NxN} is the sampling matrix. The number of cosets of $\Lambda`$ is equal to the determinant of J and their union form Λ as follows:

$$\Lambda = \bigcup_{m=0}^{\det(J-1)} \Lambda`_m \, . \tag{3.13}$$

In (3.13) $\Lambda`_m$ is a coset of $\Lambda$. A sample of nested lattices is shown in Figure 3.3, where nine cosets of $\Lambda`$ (represented by the big hexagonal) form Λ (represented by small hexagonals).

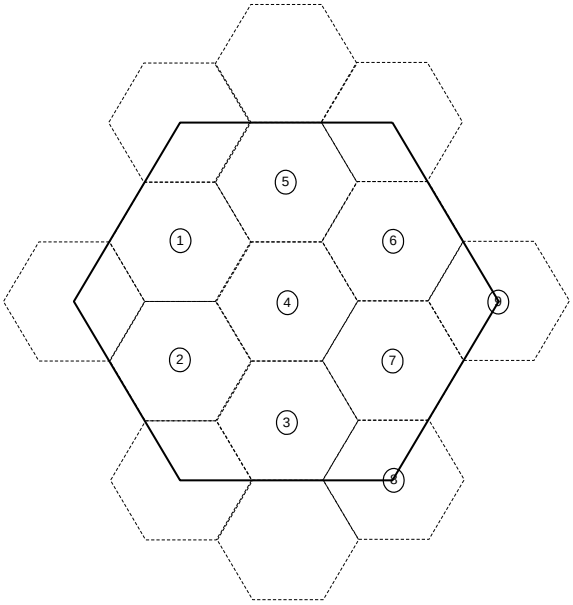


Figure 3.3: A sample 2-D nested lattices.

Quantization in a lattice can represented by a quantization function $Q_\Lambda(x)$, which maps all $x \in R^N$ to the nearest point in Λ. Using this quantization, the fundamental Voronoi cell of Λ can be defined as,

$$V = \{x \in R^N : Q_\Lambda(x)=0\}. \tag{3.14}$$

A nested lattice pair is employed in Lattice-QIM. Embedder and decoder use the same pair. Each message $m \in \{0,..,det(J)-1\}$ is associated with a coset Λ_m of $\Lambda`$. Embedding is performed by quantizing the input s to the nearest point in Λ_m:

$$x(m) = Q_{\Lambda m}(s). \tag{3.15}$$

At the decoding minimum distance decoding is performed:

$$m = \arg\min_{m} d(y, \Lambda_m), \tag{3.16}$$

where d(.,.) is any appropriate distance metric.

Equations (3.15) and (3.16) represent the lattice QIM embedding and decoding, respectively. Distortion compensation can also introduced to this scheme, which will result in DC-Lattice QIM.

The nested lattice pair should be designed sucht that the fundamental requirements of data hiding, namely *imperceptibility* and *robustness*, are met. In order to improve imperceptibility, Q_Λ should be a good Vector Quantizer; that is V should be as spherical as possible [6]. On the other hand, for improving robustness, cosets should be as far as possible [6].

3.4. Spread Transform QIM

ST-QIM is another multi-dimensional variant of QIM. In ST-QIM host signal vector is quantized along a direction ***p***. ***p*** is chosen randomly and hence host signal is spread along the random direction. The embedder function of ST-QIM is:

$$\mathbf{x} = \mathbf{s} + (q_m(\mathbf{s}^{\mathbf{T}}\mathbf{p}) - \mathbf{s}^{\mathbf{T}}\mathbf{p})\mathbf{p}\,, \tag{3.17}$$

where ***p*** is a unit vector. The projection of ***s*** onto ***p*** is quantized. The resultant error is used to scale ***p***, which is added back to ***s***. Figure 3.4 displays the process for 2-D.

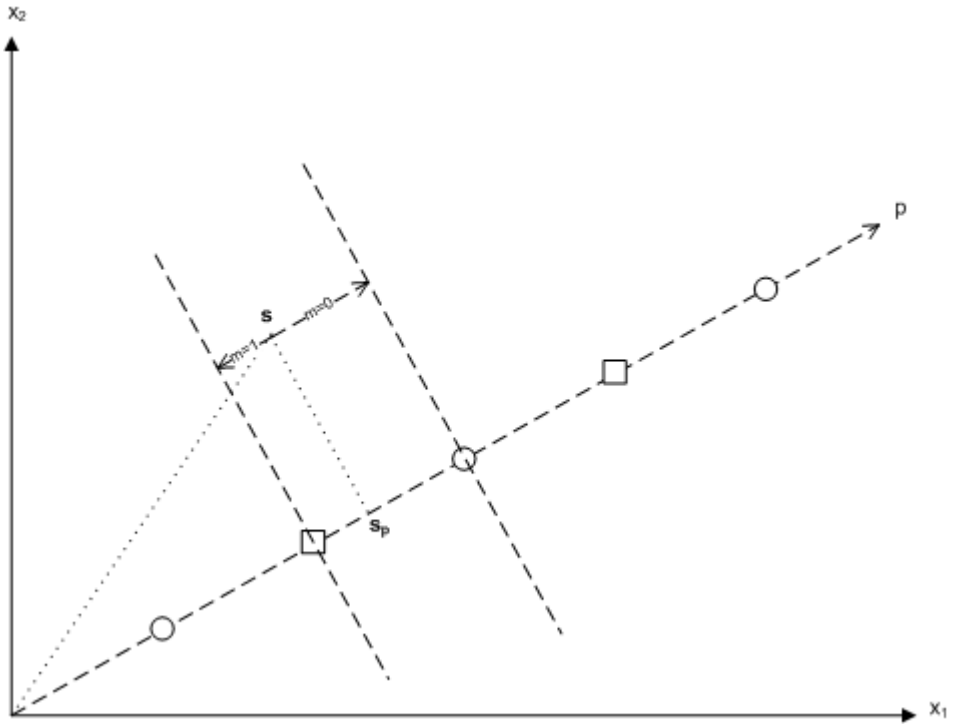


Figure 3.4: ST-QIM embedding function.

DM version is given in (3.18).

$$x = q(\mathbf{s}^{\mathrm{T}}\mathbf{p} + d(m)) - d(m) \tag{3.18}$$

Similarly DC-QIM can also be used. Furthermore, as a different extension multiple projection directions can utilized. For instance, Mihcak et. al. [73] utilize a set of pseudo-randomly chosen directions.

At the decoder, received signal is projected on the same direction and the usual minimum distance decoder is applied:

$$\hat{m} = \arg\min_{m\in\{0,1\}} d(\mathbf{y}^{\mathrm{T}}\mathbf{p}, \Lambda_m) \tag{3.19}$$

3.5. Error Thresholding

Ramkumar and Akansu [37], [5] interpreted data hiding as a signal technique using periodic signal constellations. Their periodic signaling with thresholding refers to hard limiting the error due to quantization. Error term in (3.20) is hard limited to a given value as in (3.21).

$$e = s - q_m(s) \tag{3.20}$$

$$\tilde{e} = \begin{cases} sign(e)\beta/2, & |e| > \beta/2 \\ e, & else \end{cases} \tag{3.21}$$

where $\beta<\Delta$. Then the marked signal obtained as:

$$x = s + \tilde{e} \quad . \tag{3.22}$$

A typical embedder function is shown in Figure 3.5. It is seen that Error thresholding has very similar characteristics with DC-QIM and their decoding error performances are quite close [38].

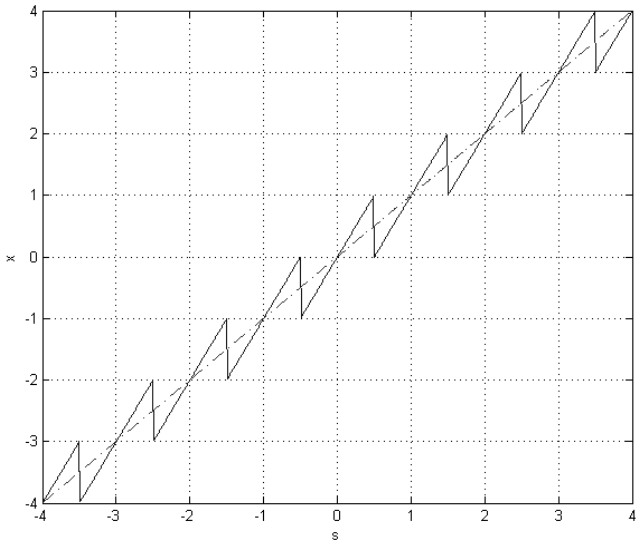


Figure 3.5: Error thresholding prototype embedder function with β=0.4 and Δ=1.

3.6 Image Data Hiding with QIM

We apply QIM to images using DFT magnitude coefficients. We select DFT magnitude coefficients since DFT magnitude domain remains to be the most robust transform as shown in [39]. If DFT magnitude domain is preferred one should be careful about the preservation of the conjugate symmetry.

In a typical application of QIM to visual content [40] an image is processed block-wise. For each block one bit is hidden. For this purpose, 2D DFT of the block intensity values are obtained. The mid-frequency coefficients are selected to hide data. These coefficients are altered by using QIM according to the message bit. If the message bit is 0, then the quantizers belonging to {0,1,0,1,..} sequence is employed. Otherwise, {1,0,1,0,..} sequence is utilized. After embedding, inverse DFT is taken and the host signal values are replaced with the marked values. The number of total hidden bits is equal to the number of blocks.

At the decoder, the same parameters (i.e, quantizer cell width, block size, selected coefficients and image size) are utilized. If the received image has different dimensions, it should be scaled back to its original size. The selected coefficients are quantized with the two set of quantizer sequences. The bit corresponding to the minimum total distance is decided. This process is repeated for all the blocks and hidden bit sequence is extracted.

In the aforementioned scheme data hiding rate depends on the image and block size. Robustness depends on the number of selected transform coefficients and the quantizer cell width. On the other hand, these system parameters affect invisibility in an opposite manner. Therefore, these parameters should be determined according to the requirements of the application.

The decoding error performance of QIM with typical parameters is tested. Figure 3.6 shows the grayscale host image of size 512 by 512. Block size is 64 by 64. 975 middle frequency coefficients are selected. The quantizer cell width is taken as 3000. The marked image is shown in Figure 3.7. Embedding distortion PSNR is 32 dB. In this test powerful embedding distortion is introduced in order to observe the limits of the scheme. The hidden 64 bits are extracted correctly for the following attacks:

- JPEG compression down to Quality Factor 20.
- 40% downscaling (with linear interpolation to return back to original size)
- Horizontal translation up to 16 pixels.
- Ink-jet printer output and scanning of this printer output.

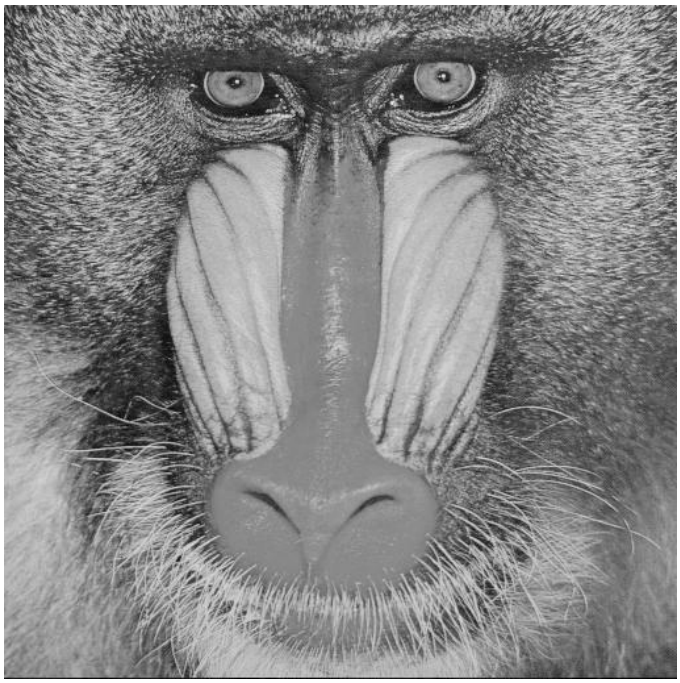


Figure 3.6: Host image.

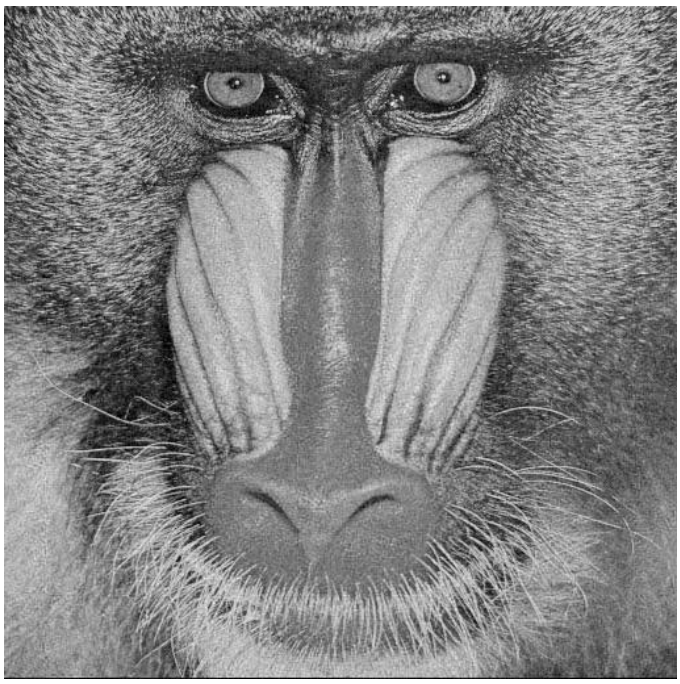


Figure 3.7: Marked image.

The marked image is also tested with Stirmark [28]. The results are given Table 3.1.

Table 3.1: Stirmark results.

Attack	**BER**
Random removal of 17 rows and 5 columns	0
2x2 Median Filter	0
3x3 Median Filter	0
4x4 Median Filter	0
JPEG 10	0.0156
JPEG 20	0
JPEG 40	0
JPEG 60	0
0.25^{o} rotation (clockwise)	0
0.50^{o} rotation	0.0156
0.75^{o} rotation	0.0469
1.00^{o} rotation	0.1094
2.00^{o} rotation	0.5625
%50 downscaling	0.25
%25 downscaling	0
%10 downscaling	0

It can be clearly observed that with such a powerful embedding distortion the scheme could be quite robust to conventional compression, median filtering, and interpolation attacks. However, even small rotations could deteriorate the results significantly. This fact is due to the need for spatial synchronization of the blocks.

CHAPTER 4

DATA HIDING USING TRELLIS CODED QUANTIZAION

In higher dimensions, selection of the quantizer to be used during data hiding becomes important. However, beyond certain dimensions the best quantizers in terms of quantization error are not known [57]. In this regard, quantizers with structured codebooks become helpful for being able to increase the host signal dimension. In this chapter, we describe two methods that are based on Trellis Coded Quantization (TCQ) [68]. First of these approaches is (TCQ-PS) a simplified version Chou's TCM-TCQ approach [69]. The second method is a practical method that exploits the redundancy in the selection of the initial state (TCQ-IS).

4.1 TCQ

TCQ [68] can be considered as a special case of trellis coding. The main ideas behind TCQ are due to trellis coded modulation (TCM) [70]. TCQ employs a set of trellises and set partitioning ideas of TCM in order to achieve better distortion performance with low complexity.

TCQ uses a trellis and an associated codebook. A sample trellis of 4 states is shown in Figure 4.1, in accordance with its finite state machine and the codebook. In this figure, u is the input bit of the finite state machine, s_1, s_0 are the states, and o_1, o_2 are the outputs of this machine. The solid lines in the trellis correspond to u=0 and the dashed lines correspond to u=1. Each branch of the trellis is associated with a subset D_i of the codebook, whose index i is determined by the output of the finite state machine. In order

to design the codebook of TCQ, a scalar codebook C of size $2^{R+\acute{R}}$ is taken. *R* is the encoding rate and Ŕ represents the number of bits that specify the particular codeword in the selected subset. For the sample system in Figure 4.1, *R* is 2 bits per sample (bps), whereas Ŕ is equal to 1. For an encoding rate of 2 bps, C is twice larger than the corresponding scalar quantizer. After C is determined, it is partitioned into $2^{\acute{R}+1}$ subsets, each of which has 2^{R-1} codewords.

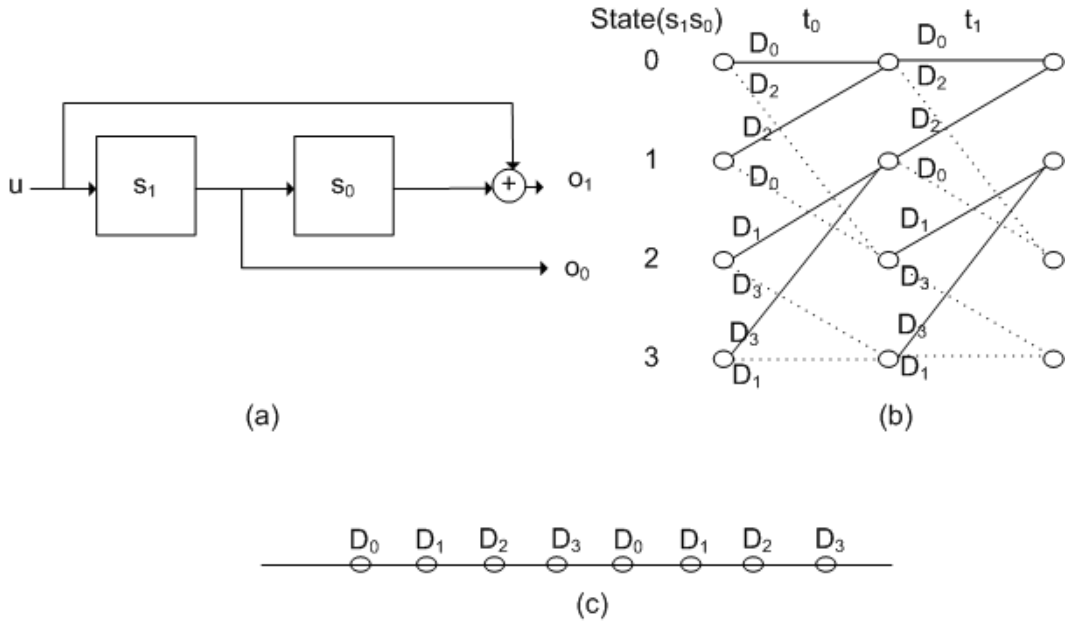


Figure 4.1: TCQ Structure.

In order to quantize an input sequence s of length m, a trellis of m stages is used. Viterbi algorithm is used to find the closest path to s among all possible trellis paths. m(*R*-Ŕ) bits specify the trellis path and *mŔ* bits specify the codeword in the selected subset. Although initial state selection is completely arbitrary, this state is generally selected as 0, since for long data sequences ($m >> log_2 N$, where *N* is the number of states) the effect of the initial state on Mean Square Error (MSE) is negligible [68].

4.2 TCQ Path Selection (TCQ-PS)

TCQ-PS is based on the TCM-TCQ scheme described in [69]. Using the same trellis structure in TCQ-IS, the coset selection in which the input signal s is to be quantized reduces to the trellis path determination according to the data w. Once the path is determined, s is quantized using the corresponding D_i. In that sense, TCQ-PS is also a member of QIM family. However, in this case, the quantizers are selected according to a trellis. Figure 4.2 shows a sample for TCQ-PS. The trellis path is determined with respect to the data w={0,1,1} starting always from the initial state 0. The data is quantized using the associated subsets of the branches in the order dictated by the trellis. In this scheme, embedding rate is 1 bps. At the decoding side, Viterbi algorithm is used to quantize the received signal using the trellis structure. Once the best path is found, the data is decoded starting from the initial state 0.

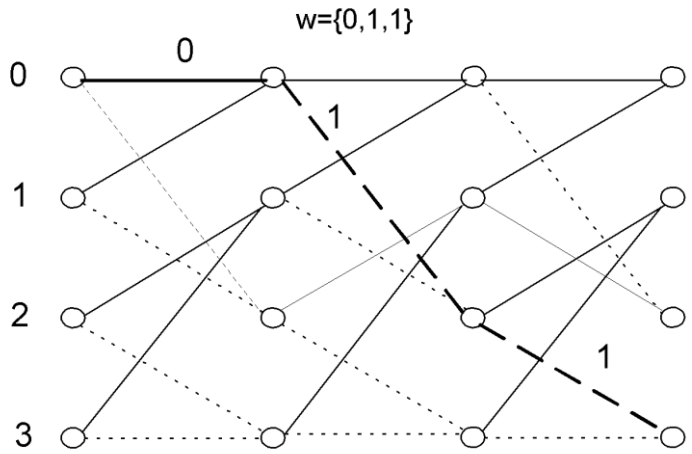


Figure 4.2: TCQ-PS embedding sample.

4.3 TCQ-IS

The proposed method makes use of TCQ, while considering the effects of the initial state (IS) on MSE. Since initial state selection is arbitrary in TCQ, one can embed information into the content by enforcing the selection of the initial state, accordingly.

After enforcing the selection of the initial state, the closest trellis path is determined by using Viterbi algorithm, as in conventional TCQ [68].

Figure 4.3 shows a sample embedding process for TCQ-IS. In this illustrated example, N=4, m=3, R=2, Ŕ=1. Since N is 4, one can hide 2 bits into the m input samples. Assuming, the data to hide is arbitrarily selected as w={0,1}, state 1 is chosen as the initial state. The corresponding closest path obtained by the Viterbi algorithm is shown with thicker branches.

The total number of bits that can be hidden by TCQ-IS is log_2N, which depends only on the number of states in the trellis. Embedding rate of TCQ-IS is log_2N/m bps. For a given m, one should use trellises with more states in order to hide more data.

In the decoding stage, all N states are considered as the candidate initial states. For each candidate initial state Viterbi algorithm is executed for the received input vector. The computed MSE values are stored and the initial state with minimum MSE gives the desired embedded data, as the index of the corresponding state.

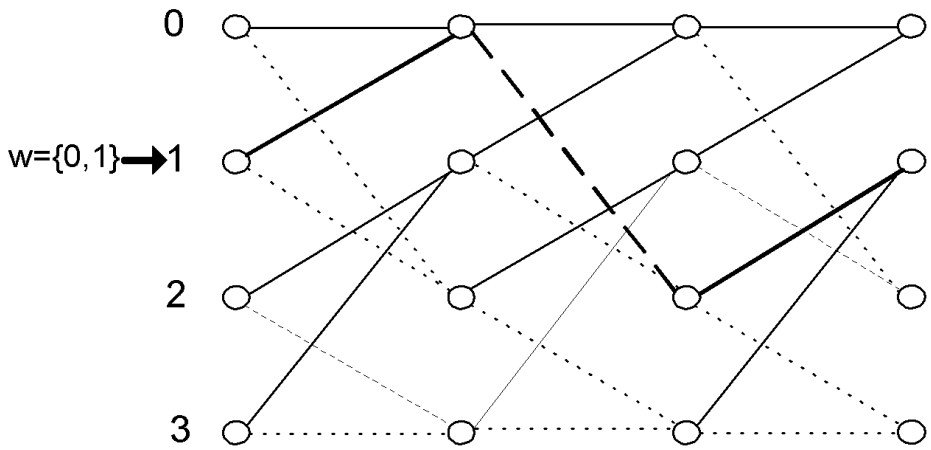


Figure 4.3: TCQ-IS embedding sample.

It should be noted that the embedding distortion due to information hiding is mainly determined by the bin widths of the quantizer (Figure 4.1), similar to other methods.

The robustness performance of TCQ-IS against data sequence length is shown in Figure 4.4. The robustness is measured by the relation between the probabilities of erroneous bit decoding versus WNR. Figure 4.4 displays the robustness of TCQ-IS with different lengths for Gaussian input source (zero mean, unit variance) against a Gaussian channel noise of zero mean, 0.5 variance. As apparent from Figure 4.4, increasing data length improves the performance. However, beyond a certain value, the improvement becomes indistinguishable. The reason for such a performance should be due to the fundamental problem (i.e. $m >> log_2 N$) for detecting the initial state, as the length increases.

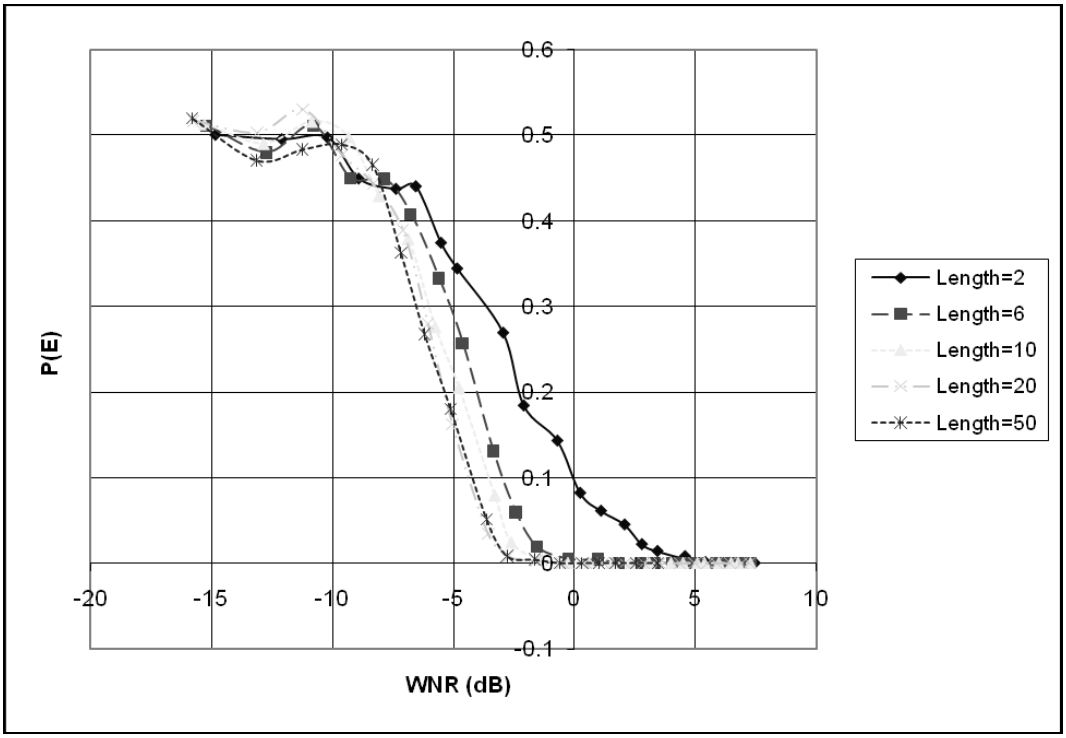


Figure 4.4: P(E) of TCQ-IS for different dimensions.

4.3.1 Interpretation of TCQ-IS as a Lattice QIM

We analyze TCQ-IS in 2-D and 3-D. Next, generalize the reasoning to multi-dimensional case and show that TCQ-IS is a lattice-QIM.

For 2-D, we utilize 4-state Ungerboeck state machine [70] and a uniform codebook for the TCQ structure, as in [45]. Hence, the explored 2-D case is composed of two input samples (and two stages of trellis), four subsets (each containing two codewords) in the codebook, and two message bits to identify the initial state.

The set of output codewords differ with respect to the initial state. For initial state 0, the possible output codewords are $\{D_0, D_0\}$, $\{D_0, D_2\}$, $\{D_2, D_1\}$, $\{D_2, D_3\}$. The constellation diagram for all initial states is depicted in Figure 4.5. The horizontal axis denotes the first

input sample and the vertical axis denotes the second input sample. The possible outputs for each initial state are shown using the corresponding index {0,1,2,3}.

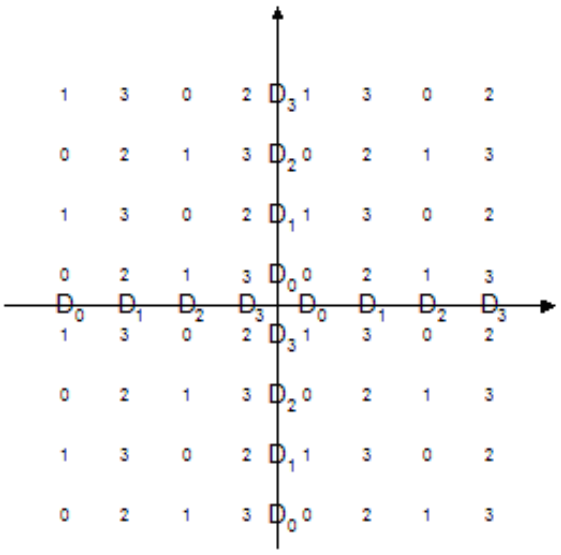


Figure 4.5: 2-D constellation.

Figure 4.5 illustrates that for 2-D case, TCQ-IS is a lattice QIM with an alternating cubic lattice. The generator matrices can be determined as (neglecting the axis offsets):

$$G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \& \, G' = \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix} \tag{4.1}$$

G is equal to the identity matrix, since Λ is equal to Z^2. The subsampling matrix J is equal to G` and determinant of J is equal four. Hence, the union of four cosets forms Λ. As a different observation, the constellation in Figure 4.5 is a typical coset code [68].

The quantization cells in Figure 4.5 are close to hexagonal. In this manner V is closer to spherical with respect to 2-D cubic lattice. By a simple error analysis, for uniform source and a fixed quantization cell width, Δ, the ratio of quantization MSE for cubic lattice and TCQ is found out to be constant and is equal to

$$\mathrm{MSE}_{\mathrm{TCQ}}(\Delta) / \mathrm{MSE}_{\mathrm{cubic}}(\Delta) = 0.969 . \qquad (4.2)$$

Eq. (4.2) states that quantization error is independent of Δ and 2-D TCQ-IS has a lower embedding distortion with respect to a 2-D Dither Modulation (DM) with scalar uniform base quantizer [12]. This fact is empirically verified and shown in Figures 4.6 and 4.6, for uniform (between –10 and 10) and Gaussian (zero mean and variance equal to 10) sources, respectively. The codebooks are enlarged to cover all of the input range, since we are not restricted with the bit allocation. The solid lines represent 2-D TCQ-IS embedding distortion and the dots represent 2-D DM embedding distortion. Figures 4.6 and 4.7 verify the validity of (4.2).

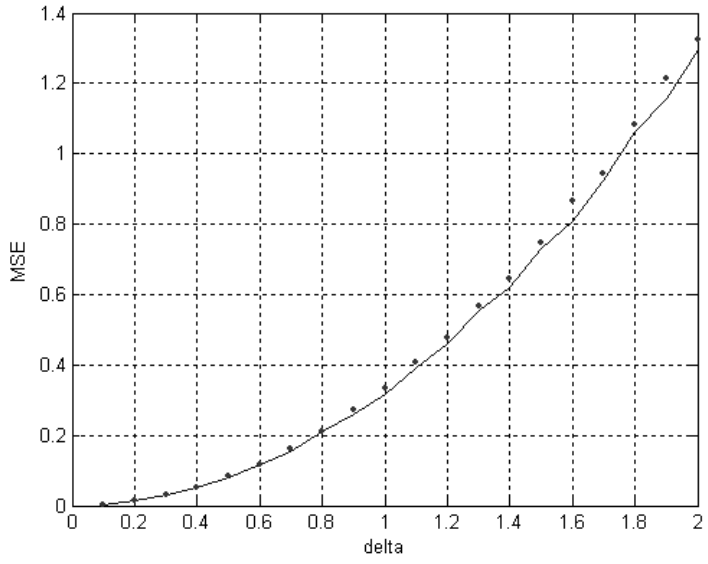


Figure 4.6: Embedding distortion for uniform source (-10, 10).

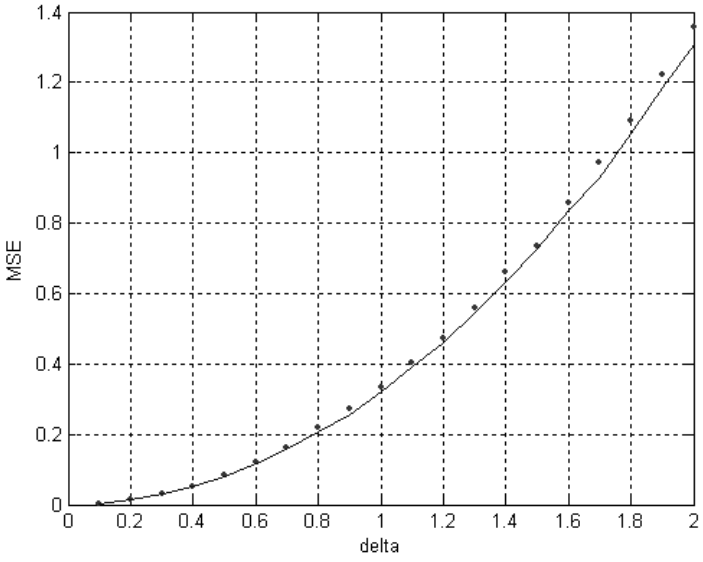


Figure 4.7: Embedding distortion for Gaussian source (0,10).

For 3-D case, three input samples (i.e. a trellis with three stages) are employed. The 3-D constellation is shown in Figure 4.8. Square, star, diamond, and circle represent the four sublattices, Λ_m.

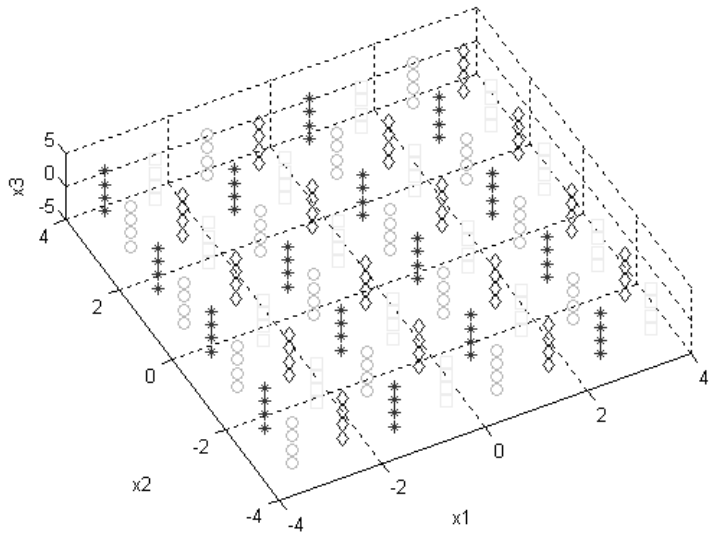


Figure 4.8: 3-D constellation of TCQ-IS.

In 3-D, Λ is a subgroup of Z^3 and hence, G is different from the identity matrix. The order of Z^3/Λ partition is given in (4.3).

$$|Z^3/\Lambda| = 4^3/(4x2^3) = 2. \tag{4.3}$$

In the denominator of (4.3), the term 2 is due to the number of trellis branches that are leaving a state and the multiplier 4 in front of it is due the number of initial states. Eq. (4.3) states that Λ fills Z^3 with a density ½. In order to obtain a density of 1 with four codewords, one should use an eight state trellis.

Similarly, the order of $Z^3/\Lambda`$ partition is $|Z^3/\Lambda`|=4^3/(2^3)=8$. Hence, $|\Lambda/\Lambda`|=4$ which is equal to det(J). As dictated by the TCQ structure, the union of four cosets of $\Lambda`$ forms Λ.

In *N* dimensions, $Z^N/\Lambda/\Lambda`$ is a partition chain. The partition orders are $|Z^N/\Lambda|=4^N/(4x2^N)=2^{N-2}$ and $|Z^N/\Lambda`|=4^N/2^N=2^N$. The order $|\Lambda/\Lambda`|$ is always four for all *N* due to the same TCQ structure used in all dimensions. In other words, for any dimension

N, the selection of the initial state in TCQ yields a coarse lattice, whose cosets form the fine lattice. This nested lattice pair can be used for data hiding by only selecting the initial state in TCQ. The coarse lattice $\Lambda`$ determines the embedding distortion. The fine lattice Λ, whose members can be interpreted as the channel codewords, is related to the P(E) performance of the data hiding system.

As a result, TCQ-IS constitutes a practical lattice QIM method. Since it does not introduce any additional complexity to TCQ, it is practically feasible and can be extended easily to higher dimensions. The additional burden is only in the decoding stage; in which all initial states should be tried.

4.4 Comparison of TCQ-IS, TCQ-PS, and QIM

The robustness of TCQ-IS, TCQ-PS and QIM are examined in terms of the relation between WNR and the probability of decoding error.

During the experiments, channel noise power is kept constant, while the watermark power is varied. The probability of error is computed as the ratio of erroneously decoded data bits to the number of total data bits. The final values are computed by averaging the results for random experiments. Two sources are used to embed data: a uniform source in the range (-1,1) and a Gaussian source with zero mean and unit variance. The TCQ structure in Figure 4.1 is utilized for both TCQ-IS and TCQ-PS during these simulations. The codebook is chosen so that it covers all input data range for the uniform source. For Gaussian source, the selected range contains most of the signal energy. Input data length is selected as 10. In order to equate the data embedding rate, QIM uses 1 sample to hide 1 bit and TCQ-IS operates on input samples in lengths of 2. The robustness of the methods is plotted with respect to various Gaussian channel noises in Figures 4.9, 4.10, 4.11 and 4.12.

The results in the figures indicate that, for all low-noise cases, TCQ-IS and QIM performs similar, which are better than TCQ-PS. On the other hand, for high noise case,

TCQ-IS has the best performance among the three methods. This fact is mostly due to the non-cubic lattice employed in TCQ-IS.

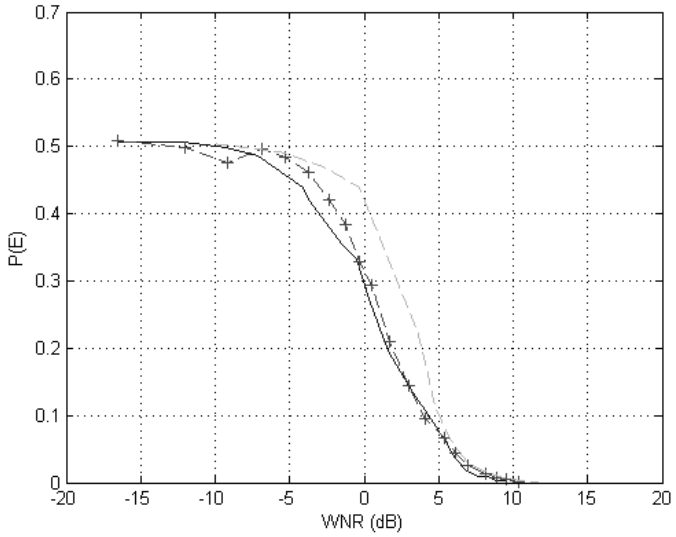


Figure 4.9: Uniform Source (-1,1) and Gaussian (0,0.5) Channel. (*Solid* line denotes TCQ-IS, *dashed* line denotes TCQ-PS, and dashed line with *plus* sign denotes DM)

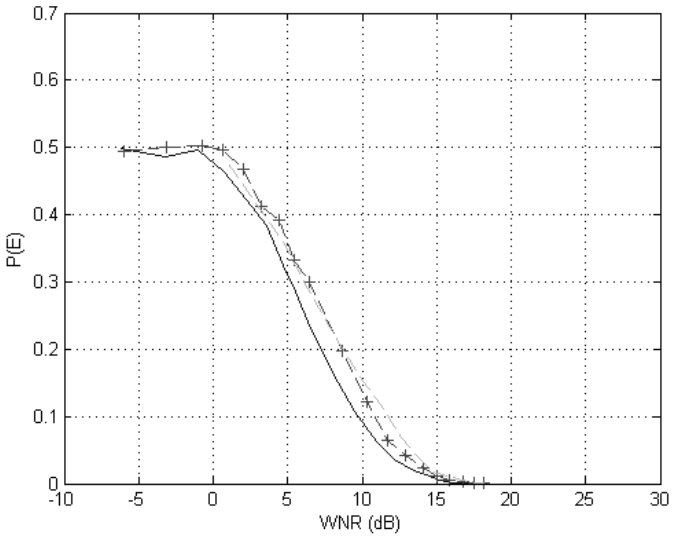


Figure 4.10: Uniform Source (-1,1) and Gaussian (0,1) Channel. (*Solid* line denotes TCQ-IS, *dashed* line denotes TCQ-PS, and dashed line with *plus* sign denotes DM)

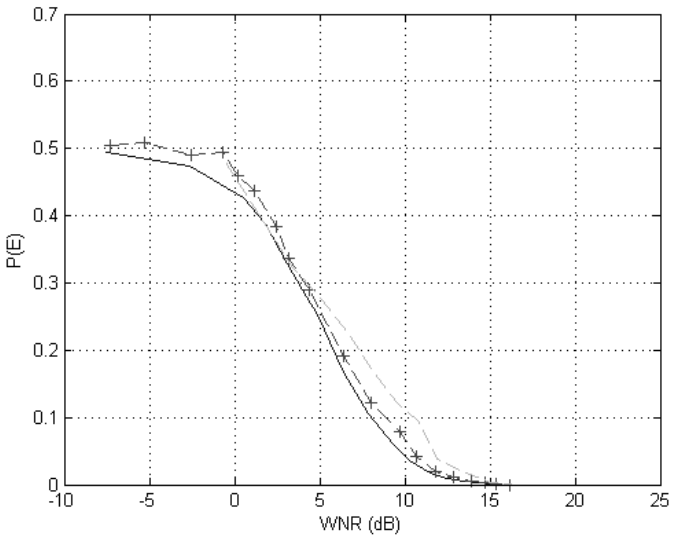


Figure 4.11: Gaussian Source (0,1) and Gaussian (0,1) Channel. (*Solid* line denotes TCQ-IS, *dashed* line denotes TCQ-PS, and dashed line with *plus* sign denotes DM)

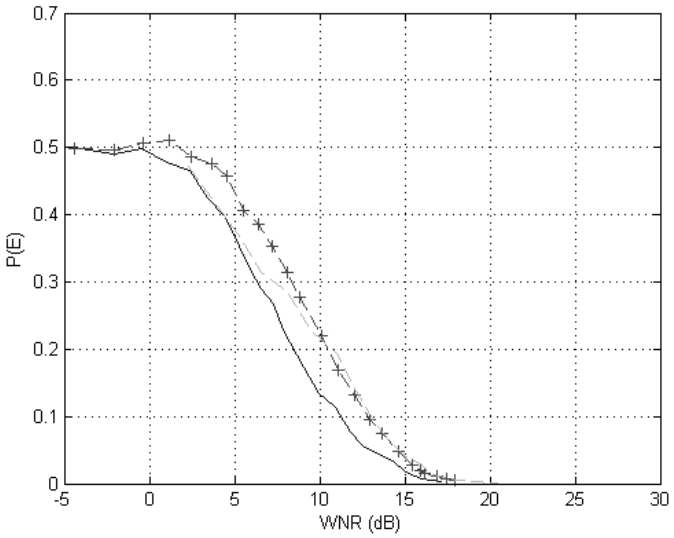


Figure 4.12: Gaussian Source (0,1) and Gaussian (0,2) Channel. (*Solid* line denotes TCQ-IS, *dashed* line denotes TCQ-PS, and dashed line with *plus* sign denotes DM)

4.5 Image Data Hiding with TCQ-IS

TCQ-IS described is applied to image data hiding similar to Section 3.5. The image is partitioned into blocks and for each block Discrete Fourier Transform (DFT) is calculated. The coefficients, for which TCQ-IS will be applied, are selected from the middle frequency band, as shown in Figure 4.13. The low frequency coefficients are not included, since modifications on these coefficients are expected to be more visible. The high frequency band is also not considered, since the coefficients in this band are expected not to survive compression. The magnitudes of the selected mid-frequency DFT coefficients are fed into TCQ-IS. Resulting quantized values are replaced with the originals and finally, the marked image is obtained.

The decoder uses the same set of coefficients and extracts the hidden bits after the Viterbi decoding. Figure 4.14 shows a typical marked image (grayscale image Lena of size 512x512) with embedding distortion of 43dB.

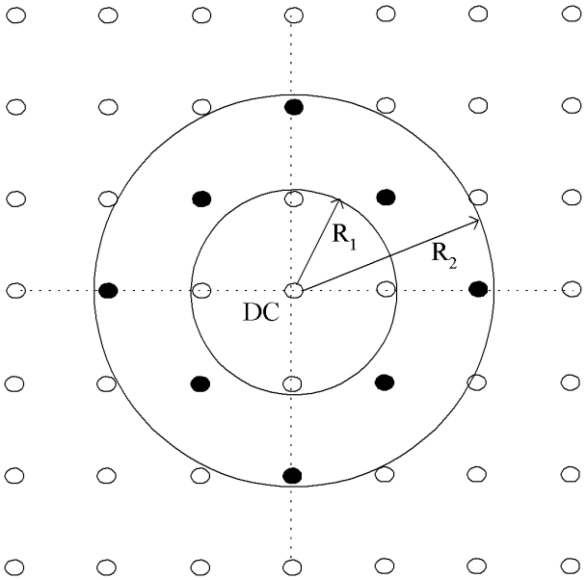


Figure 4.13: Coefficient selection.

Figure 4.14: Marked image (43 dB Embedding Distortion).

The robustness of TCQ-IS for image data hiding is computed against JPEG compression attack using different trellises and codebooks. The block size is taken as 16. The first 6 coefficients between the circles of radii 3 and 2 are selected in raster scan. In addition to 4-state trellis shown in Figure 4.1, 8-PSK trellises with 8 and 16 states [70] are also employed. The results are shown in Figure 4.15, as the embedding distortion versus probability of error against JPEG-80 compression attack. It is apparent that as the trellis structure becomes dense, the robustness increases. It is also observed that even if the state numbers differ two PSK schemes behave similarly, since they share the same codebook.

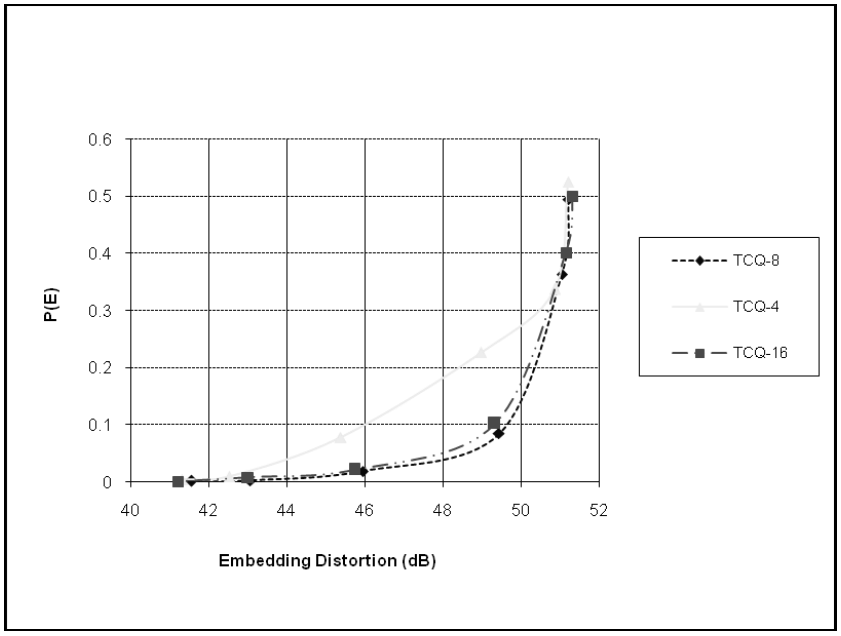


Figure 4.15: JPEG-80 compression attack performance.

CHAPTER 5

FORBIDDEN ZONE DATA HIDING

Blind data hiding methods are generally based on quantization, in order to provide host interference rejection. In the data hiding context, quantization refers to a selection of set of codebooks and mapping the host signal to the appropriate codeword depending on the data. This simple approach enables the method to be oblivious of the host signal at the decoder, once the selected codebooks are assured to be synchronized between embedder and decoder. In this manner, Quantization Index Modulation (QIM) [12] can be considered as a general framework for the methods that incorporate quantization into data hiding techniques and it can be simply defined as the quantization of the host signal by using the quantizers whose indices are modulated by the data to be hidden [12]. This simple formulation encapsulates a very broad range of methods ranging from least significant bit modulation to DC-QIM, or from scalar Dither Modulation (DM) [12] to lattice-QIM methods [6].

Blind data hiding problem can be considered identical to communication with side information at the encoder. This correspondence was first indicated by Chen [33] and Cox [41]. Chen has applied the work of Costa [32], which is called *dirty paper coding*, to data hiding problem. Costa showed that the channel capacity for independent and identically distributed (iid) Gaussian host signal is ½log2 $(1+P_w/P_n)$, where P_w is the watermark power and P_n is the channel noise power. This capacity is independent of the host signal power; therefore, it is equal to the case where side information is also available at the decoder. By introducing the Costa's work, Chen showed that blind methods that achieve the same performance with the non-blind algorithms can be devised. The channel capacity can be achieved with a random codebook of infinite dimension; therefore, the Costa scheme is not practical. Hence, some practical methods are proposed for this purpose, such as Distortion Compensated QIM (DC-QIM) [12] and

its equivalent form Scalar Costa Scheme (SCS) [34]. These methods are all variants of QIM [12].

The general QIM scheme performs poorly for low WNR (Watermark-to-Noise-Ratio), where channel noise level is high or watermark power (i.e. the embedding distortion) is low [12]. DC-QIM is introduced as a remedy for this problem. DC-QIM can be considered as a post-processed version of its predecessor QIM. In DC-QIM, in order to increase the robustness, the distance between the quantization reconstruction points are increased by scaling quantizer cell width with a compensation factor (α) smaller than one. This operation increases the embedding distortion. Therefore, a portion of the quantization error (i.e. the distortion compensation term) is added back to the quantized value. The optimal value of α that maximizes the *SNR* at the receiver is shown to be *WNR/(1+WNR)* [12] and later, a numerical approximation of α is also given in [34] for SCS. In contrast to distortion compensation different approaches are also introduced, such as the works introduced by Ramkumar [37], [5]. They use thresholding during embedding in order to hard limit the possible distortion and obtain comparable performances [38]. In the context of data hiding, theoretical limits could be achieved with random codebooks. Hence, the methods based on random coding have been used to achieve the capacity limits [42], [43], [44]. However, due to their unstructured nature, they are still unpractical. As a remedy, lattice vector quantization methods can be employed due to their manageable structure. In [42], it is shown that structural constraints do not result in a loss of capacity in the asymptotical case. Nevertheless, there is a loss for lower dimensional lattices, whereas the design and implementation of higher dimensional lattices can be overwhelmingly expensive. Therefore, more special constraints can be used as in [45], [46], [47], which are based on Trellis Coded Quantization.

In the literature, new methods and analysis based on QIM are still introduced. In [48], QIM is applied block-wise in a game theoretic framework. QIM is also utilized in many data hiding applications: for instance, [49] uses QIM for image data hiding and [50] for video data hiding. A more recent work [51] utilizes the indices of a vector quantizer to hide data in an image data hiding application. For a comprehensive review and discussion of quantization based data hiding methods the readers are referred to [6].

We propose a novel data hiding method, which lies beyond the QIM framework. We approach the problem from a different perspective, where the main motive is to introduce distortion as much as needed, while keeping a range of host signal intact depending on the desired level of robustness. The method relies on the newly introduced concept of Forbidden Zone (FZ) [52], which is described in Section 5.1, in addition to the general and simple parametric forms of FZDH. It is also shown that the simple parametric form includes QIM as a special case. In Section 5.2, the decoding error analysis of FZDH is given. Next, the proposed method is compared against QIM and DC-QIM in Section 5.3 and 5.4.

5.1 Forbidden Zone Data Hiding

Forbidden Zone (FZ) is defined as the host signal range, where alteration is not allowed during data hiding process. Forbidden Zone Data Hiding (FZDH) simply makes use of FZ to adjust the robustness-invisibility trade-off.

The definition of FZ concept may lead to an impression of similarity between FZ and masking [53], whereas they correspond to totally different concepts. Masking is applied to data hiding and watermarking in a number of efforts, as in [54], [55], [56], in order to incorporate perceptual analysis, so that perceptually usable host signal samples and permissible distortion margins are determined. However, FZ does not involve any perceptual analysis and adaptive coefficient selection process.

The main motivation of FZ is decreasing the embedding distortion at a certain decoding error level. Similar to QIM, FZ should be applied, when the embedding distortion is within perceptually feasible margins. This requirement is generally satisfied as a result of the host signal power constraint, which states that the host signal power is significantly greater than embedding distortion.

The general and simple parametric forms of FZDH are given in the following subsections.

5.1.1 General Form

Let $\bar{s}$ be the host signal in R^N, m be the data to be hidden; then the marked signal $\bar{x}$ is given by:

$$\bar{x} = \begin{cases} \bar{s}, & \bar{s} \in FZ_m \\ \mathrm{M}_m(\bar{s}), & \bar{s} \in AZ_m \end{cases}, \tag{5.1}$$

where the union of FZ_m and AZ_m (Allowed Zone indexed by the message) is

$$FZ_m \bigcup AZ_m = R^N, \tag{5.2}$$

and $\mathrm{M_m}(.)$ is a mapping from R^N to a partition of R^N corresponding to m:

$$\mathrm{M}_m(.): R^N \rightarrow P_m^N. \tag{5.3}$$

The partitions and the zones in (5.1) should be formed in such a way that they are mutually exclusive:

$$(FZ_i \cup P_i^N) \cap (FZ_j \cup P_j^N) = \phi. \tag{5.4}$$

The union of the partitions does not necessarily need to be equal to R^N; the only requirement is the fact that they should not overlap.

In (5.1), m is an element of an alphabet of size M. Therefore, the data hiding rate is $log_2 M$ bits per sample.

In the data extraction step, a generic minimum distance decoder is utilized:

$$\hat{m} = \arg\min_{m} d(\bar{y}, \bar{y}_m), \tag{5.5}$$

where $\bar{y}$ is the received signal and $\bar{y}_m$ is equal to its FZDH operation applied version as in (5.1). The decoder and embedder should be synchronized in terms of the zones and the partitions.

5.1.2 Simple Parametric Form

The critical issue in FZDH is the determination of the zones and the partitions: FZ_m and AZ_m, and P_m^N. Although there are infinite ways to achieve this aim, a practical design can be performed by using quantizers. Such a simple parametric form is given in (5.6) and (5.8). The mapping function is equal to:

$$\begin{aligned} \mathrm{M}_m(\bar{s}) &= \begin{cases} \bar{s} + \bar{e}_m (1 - \dfrac{r}{\|\bar{e}_m\|}) \end{cases} \\ &= \begin{cases} \dfrac{r}{\|\bar{e}_m\|} \bar{s} + (1 - \dfrac{r}{\|\bar{e}_m\|}) q_m(\bar{s}) \end{cases} \end{aligned}, \tag{5.6}$$

where r is the control parameter, $q_m(.)$ is a quantizer indexed by m, and $\bar{e}_m$ is defined as the difference vector between the host signal and its quantized version:

$$\bar{e}_m \overset{\Delta}{=} q_m(\bar{s}) - \bar{s}. \tag{5.7}$$

FZ_m and AZ_m are defined by using the control parameter and the difference vector:

$$FZ_m = \{\bar{s} \mid \|\bar{e}_m\| \le r\}, AZ_m = \{\bar{s} \mid \|\bar{e}_m\| > r\}. \tag{5.8}$$

In order to fulfill the requirement in (5.4), the reconstruction points of the quantizers that are indexed by various m values should be different, which can be achieved by using a base quantizer and shifting its reconstruction points depending on m, similar to Dither Modulation [12].

In Figure 5., a sample embedding function in 1-D is presented, where c_i is a codeword of the selected quantizer. An element of FZ_m is $[c_i - r, c_i + r]$ and the host signal is not altered in that region. In AZ_m, the host signal is mapped to the nearest reconstruction point modified by the control parameter r. The abrupt change in AZ_m is a result of using quantizers in the mapping function. However, this abrupt change is not strictly necessary; i.e., different functions can be used to have smoother embedding functions, such as the ones used in DC-QIM.

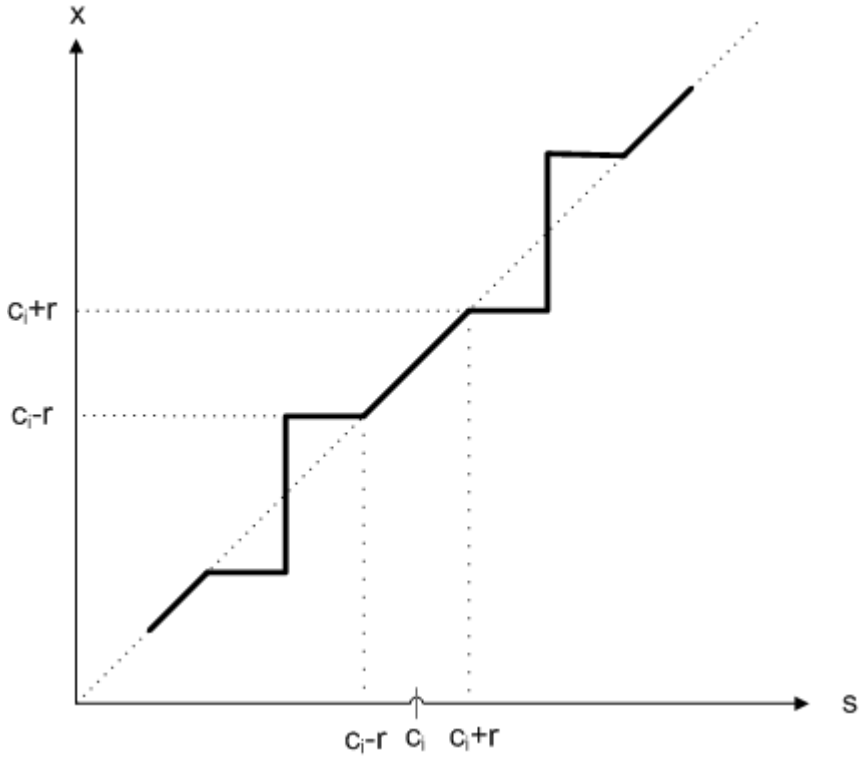


Figure 5.1: 1-D sample embedding function.

DC-QIM and FZDH can be considered similar when 1-D simple parametric form is considered. However, DC-QIM and FZDH are essentially two different concepts. Firstly,

FZDH involves a set partitioning to determine the range of host signal where alteration is allowed. There is no such partitioning beforehand in DC-QIM. Afterwards, FZDH employs a mapping in the AZ, for which quantizers are not the only choice. FZDH and DC-QIM approaches the problem from two different perspectives. In FZDH, initially all regions are forbidden and one decreases these zones according to the desired level of decoding error with respect to a channel noise level, wheres in DC-QIM one distorts the signal with respect to the desired level of robustness and then compensates some portion of the embedding distortion. FZDH keeps some of the host signal unaltered, whereas DC-QIM always alters the host signal.

5.2 Decoding Error Analysis

We theoretically analyze the decoding error performance of FZDH in 1-D by using the proposed simple parametric form, in which a uniform base quantizer is employed.

Let $q_m(.)$ be a uniform quantizer with cell width 2Δ, where $m \in \{0,1\}$. $q_m(.)$ is obtained by shifting the cells and reconstruction points of the uniform base quantizer with cell width 2Δ, as in Dither Modulation [12]. Depending on this base quantizer, r is defined to be in the range [0, Δ/2], in order to avoid overlapping of FZ_m. Otherwise, even in the absence of channel noise, it will not be possible to extract the hidden data perfectly.

We utilize the origin cell of the base quantizer in the following analysis without loss of generality. In this region, let s be uniformly distributed and $|s|<\Delta$. The uniformity of s in the region of interest is a fair assumption for large host signal power with respect to the watermark power; since in that scenario, the case for s falling into a quantization cell should be evenly distributed along the cell and should approximately behave as a uniform distribution.

According to these assumptions, the distribution of the marked signal is equal to:

$$f_x(x) = \frac{1}{2\Delta} rect(x,r) + \frac{1}{2}(1-\frac{r}{\Delta})(\delta(x+r)+\delta(x-r)) \quad , \tag{5.9}$$

where $rect(x,r) = 1$ for $|x| \le r$ and 0 otherwise.

Let w denote the equivalent additive watermark ($w=x-s$). Then, the distribution of w becomes

$$f_w(w) = \frac{r}{\Delta}\delta(w) + \frac{1}{2\Delta} rect(w, \Delta - r) \quad . \tag{5.10}$$

The probability density functions (*pdf*) of x and w are depicted in Figure 5.2.

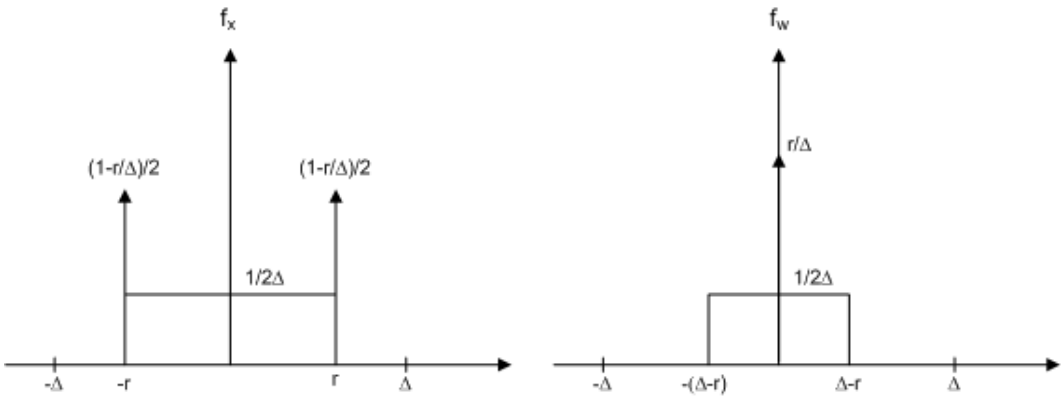


Figure 5.2: The *pdf*s of x and w.

Let y be the received signal after AWGN channel with zero mean and σ_n^2 variance. The distribution of the channel is denoted by f_n. Hence, the distribution of y is given by the convolution of f_x and f_n:

$$f_y(y) = f_x * f_n = \frac{1}{2}(1-\frac{r}{\Delta})(f_n(y+r) + f_n(y-r)) + \frac{1}{2\Delta}\int_{-r}^{r} f_n(y-\tau)d\tau \tag{5.11}$$

Let $\hat{m}$ be the decoded message. Then, the event for the decoding error (E) is defined as the case where $\hat{m} \neq m$. Since the error is independent of m, one can assume $m=0$ without loss of generality. Then, the complete decoding error probability is given by:

$$P(E) = P(m \neq \hat{m}) = \sum_{k=-\infty}^{\infty} P((4k+1)\frac{\Delta}{2} < y < (4k+3)\frac{\Delta}{2}) \tag{5.12}$$

The dominant error term is within the fundamental cell for practical conditions for which *WNR* does not reach to -∞. Such a non-practical case occurs, when there is no embedding distortion or channel noise power goes to infinity. In that case, all the quantizer cells contribute to the decoding error equally and the final probability becomes 0.5. On the other hand, for a practical region of interest for WNR, one can simplify the error probability by considering only the fundamental cell. Then, the simplified decoding error probability becomes:

$$P(E) = P(|y| > \frac{\Delta}{2}) = 2P(y > \frac{\Delta}{2}) \tag{5.13}$$

.

The last equality in (5.13) is a result of the symmetric structure of f_y around the origin. When we substitute f_y into (5.13), we obtain the decoding error probability as,

$$P(E) = (1-\frac{r}{\Delta})\left\{\frac{1}{2}Q\left(\frac{\frac{\Delta}{2}+r}{\sqrt{2\sigma_n^2}}\right) + \frac{1}{2}Q\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right)\right\} + \frac{1}{2\Delta}\int_{-r}^{r} Q\left(\frac{\frac{\Delta}{2}-\tau}{\sqrt{2\sigma_n^2}}\right)d\tau \tag{5.14}$$

,

where *Q(.)* is the complementary error function.

In order to understand the behavior of *P(E)* in (5.14), one could analyze its limiting conditions valid under the given assumptions. As *r* approaches to zero, *P(E)* becomes :

$$\lim_{r\to 0} P(E) = Q\left(\frac{\frac{\Delta}{2}}{\sqrt{2\sigma_n^2}}\right), \tag{5.15}$$

which is equal to decoding error probability of QIM as expected, since when the control parameter *r* forces the forbidden zone to disappear then FZDH reduces to QIM as its special case. Secondly, we analyze the case where watermark power goes to infinity ($WNR \to \infty$):

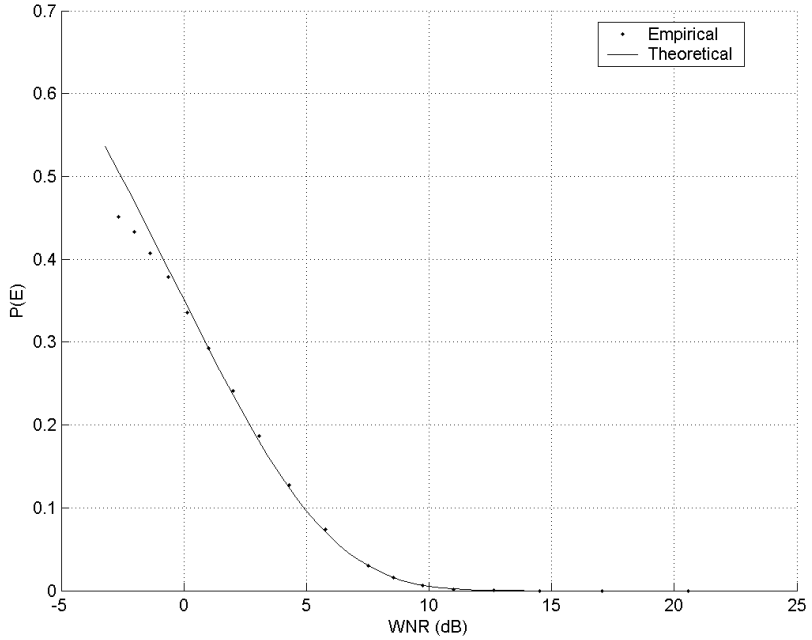
$$\lim_{WNR\to 0} P(E) = 0 \quad . \tag{5.16}$$

This result is due to the fact that $Q(\infty)$=0. Naturally, as the watermark power increases (i.e. Δ increases and the marked signal remains within the fundamental cell), we do not expect any decoding error.

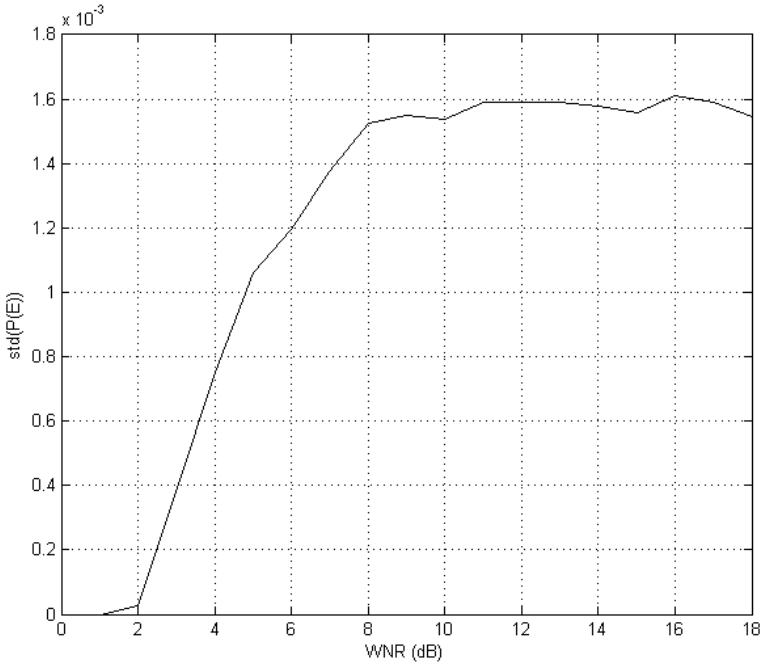
The analysis on the limiting conditions indicates that *P(E)* in (5.14) is in accordance with the theoretical expectations and can be assumed as a valid decoding error probability.

We also compare the simplified *P(E)* with some empirical results. For this purpose, we conduct 10^5 random experiments for each *WNR* value and compute the decoding error as the average error of these experiments. The *WNR* range is adjusted by keeping channel noise constant and varying the embedding distortion (i.e. changing Δ under constant *r*). The comparison is depicted in Figure 5.3(a). The results indicate that empirical values coincide with the theoretical ones; hence, the closed form expression for *P(E)* is verified. The deviation in the low *WNR* range is a result of the assumptions becoming invalid for such practical scenarios.

Figure 5.3 (b) depicts the standard deviation of the P(E) estimate shown in Figure 5.3 (a). The standard deviation is estimated as the average of 10^3 random experiments. We observe that standard deviation saturates around 1.6 10^{-3}. Assuming a Gaussian distribution for the standard deviation estimate we can claim that the 95% confidence interval of P(E) estimate is within the $\pm 3.2\ 10^{-3}$ proximity of the mean value. This interval is not visible in Figure 5.3 (a). We perform at least 10^5 random experiments for the rest of the P(E) estimations and we are interested in P(E) ranges greater than 10^{-2}. Therefore the confidence interval deduced from Figure 5.3 (b) is adequate to justify the validity of the P(E) estimates and comparisons on them for the rest of the experiments in this chapter.



(a)



(b)

Figure 5.3: (a) Empirical vs. theoretical probability of error for $\Delta=1$ and $r=\Delta/10$, (b) Standard deviation of the P(E) estimate.

The empirical *P(E)* values with respect to r/Δ and $\Delta=1$ for different *WNR* values are also depicted in Figure 5.4. The curves in Figure 5.4 are obtained by interpolating the experimental values. We fix the value of Δ and vary r from 0 to $\Delta/2$. For an (r, Δ) pair, we vary σ_n from a value slightly greater than 0 to a suitable multiple of Δ, which is adequate to cover the desired *WNR* range of 0 to 20 dB. Then, for each r/Δ, we have *P(E)* data as a function of *WNR*. Since *WNR* axis may not contain exact values of (0, 5, 10, 15, 20), we use their nearest neighbors in linear interpolation to obtain the corresponding *P(E)* value. For *WNR*=0, *P(E)*=0 is not achievable, whereas the minimum value is attained around $r/\Delta=0.3$. This result shows that FZDH outperforms QIM in this range. The slope of the decrease indicates the amount of improvement that can be introduced by FZDH. As *WNR* increases, the potential for improvement reduces, i.e. QIM becomes sufficient.

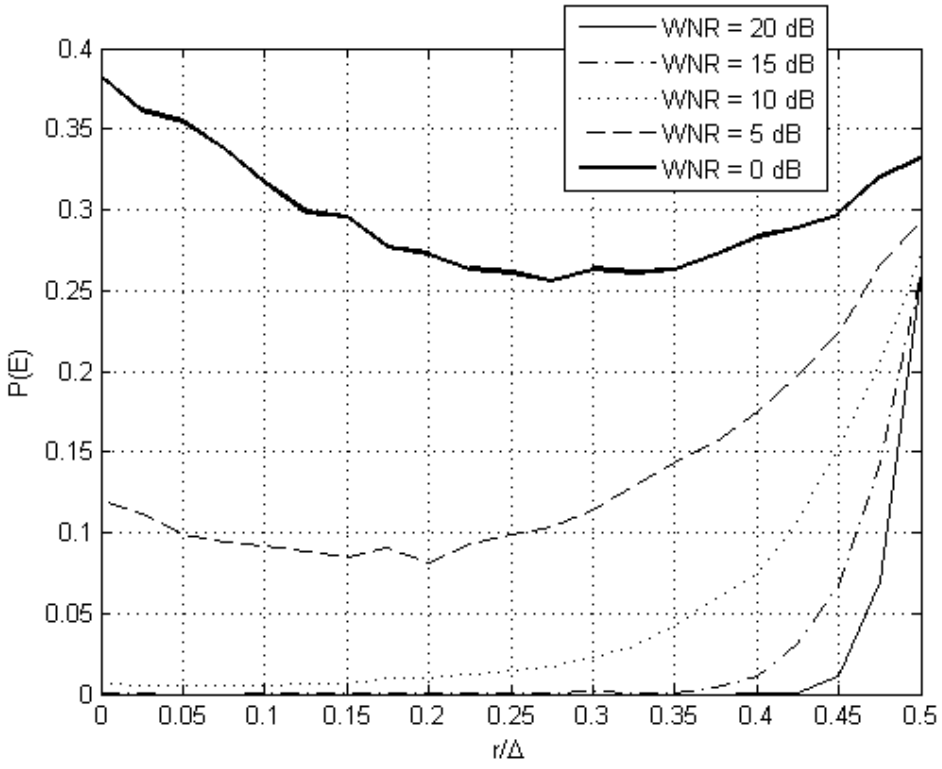


Figure 5.4: *P(E)* vs. r/Δ for different *WNR* values 0 dB, 5 dB, 10 dB, 15 dB, 20 dB.

In its simple parametric form, a single control parameter is used in FZDH. However, a constant r value cannot be optimal for all *WNR* range. Therefore, we empirically determine the best *P(E)* and the corresponding r/Δ values, which are depicted in Figure 5.5 and Figure 5.6, respectively. The values in Figure 5.5 are slightly different than the ones in Figure 5.4. This difference is due to the interpolation step involved in the computation of the values in Figure 5.4. The experiments are conducted by using the possible range for r/Δ, which is equal to (0,0.5). For each *WNR*, the minimum *P(E)* is determined and the corresponding r/Δ is noted. Figure 5. shows that for low *WNR* range, one could increase the forbidden zone to the limiting case. On the other hand, after 15 dB, there is no forbidden zone left and the algorithm converges to QIM.

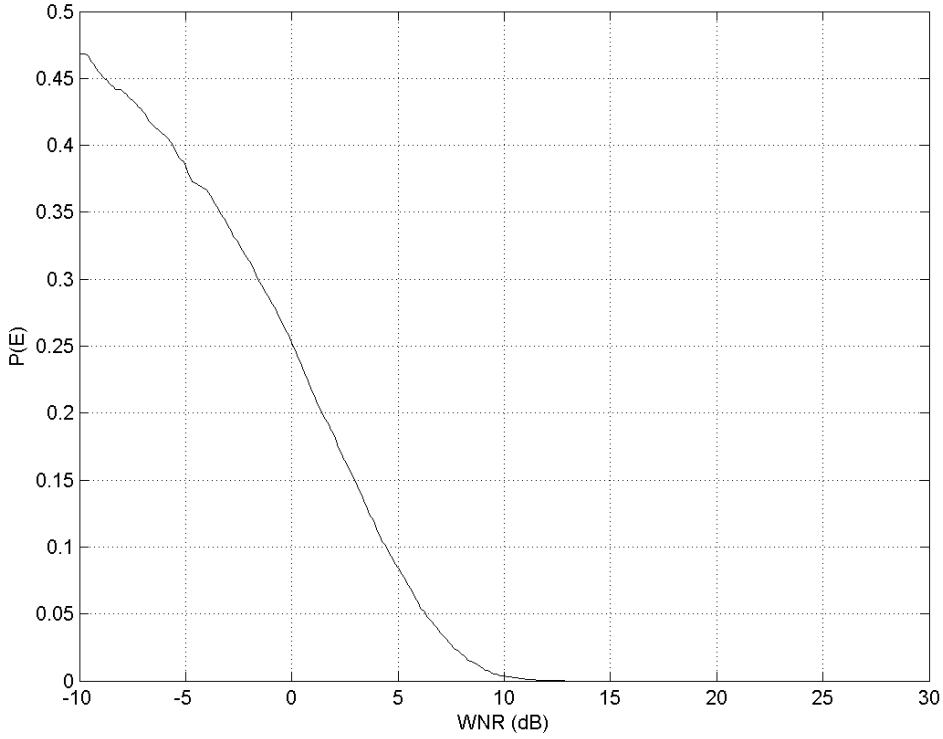


Figure 5.5: Empirically optimal *P(E)* values.

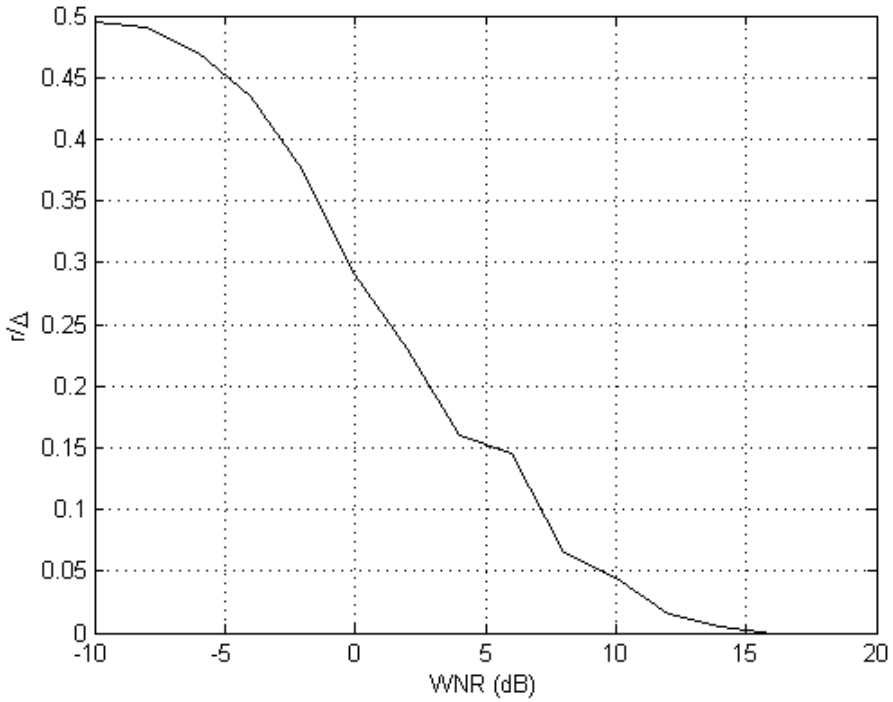


Figure 5.6: Empirically optimal *r* values corresponding to the minimum *P(E)*.

We compare the empirical results given Figure 5.5 and Figure 5.6 with brute force numerical optimization results for optimal P(E) and corresponding *r* value. For this purpose we select 20 uniformly sampled *r* values in the range [0, Δ/2], where Δ=1. We evaluate the P(E) expression given in (5.14) numerically for each *r*. We determine the minimum P(E) value and record the corresponding *r* value. The numerically optimal P(E) values in addition with the empirical results are shown in Figure 5.7. Similarly, optimal *r* values determined numerically and empirically are shown in Figure 5.8.

Figure 5.7 and 5.8 indicate the concordance of the empirical results and the brute force numerical optimization of the P(E) statement in (5.14). We should note that the small discrepancies exist in Figure 5.8 are due to the interpolation in determining the empirically best *r* value.

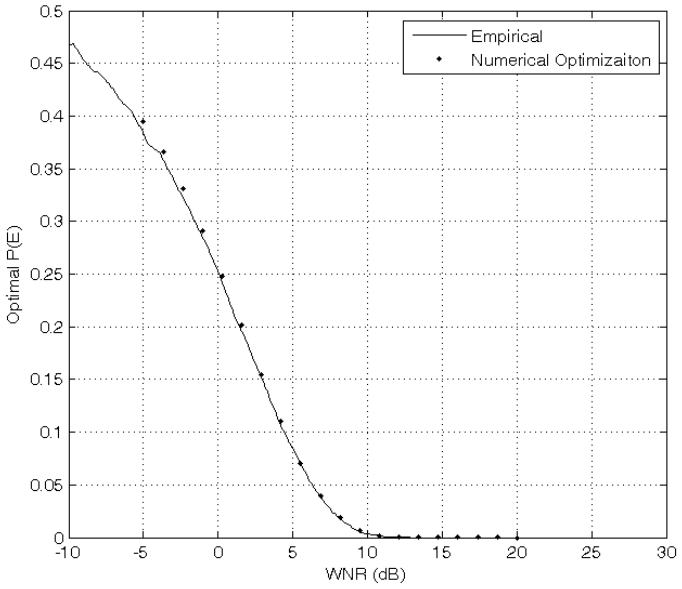


Figure 5.7: Numerical vs. empirical optimal P(E).

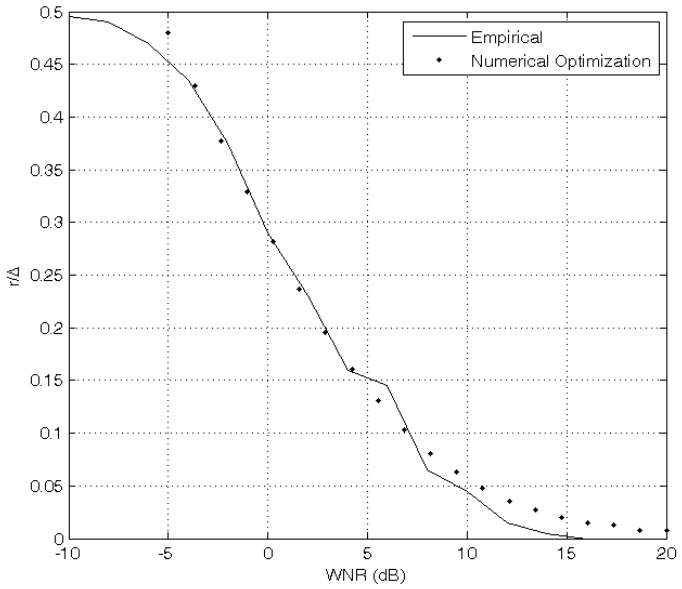


Figure 5.8: Numerical vs. empirical optimal *r* values.

5.3 Comparison against QIM

We first compare FZDH and QIM in a theoretical basis, then verify the results empirically. For this purpose, we evaluate the induced embedding distortions at the same data hiding rate and probability of error. The comparison is based on the assumptions stated in the previous section.

The expected difference between the host and marked signals as a result of the embedding operation, namely embedding distortion, can be obtained by using f_w given in (5.10):

$$\varepsilon = \int_{-(\Delta-r)}^{\Delta-r} \frac{1}{2\Delta} z^2 dz = \frac{\Delta^2}{3} - \Delta r + r^2 - \frac{r^3}{3\Delta} \quad . \tag{5.17}$$

The same result could also be obtained by using the difference term between the host and marked signals in AZ. This equation shows that embedding distortion depends on (Δ,r) pair nonlinearly and one can obtain the same embedding distortion amount with different (Δ,r) pair.

In (5.17), ε is monotonically decreasing with r. The trivial solution, r_o, which will minimize ε, is simply $r_o=\Delta$, which is equivalent to considering the whole host signal range as *FZ*, yielding no embedding distortion as well as no robustness. The additional constraint on r should be due to the desired probability of error. Therefore, we place an upper bound for both FZDH and QIM.

Let probability of error for both FZDH and QIM be bounded by an upper limit γ. However, it is not possible to obtain a closed form simple expression for r using (5.14). Therefore, we replace an upper bound for (5.14) that will be valid for all possible values of r. Since the complementary error function is monotonically decreasing, the dominant term in (5.14) is the second term. Hence, (5.14) is guaranteed to be bounded as:

$$P(E) \le Q\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right). \tag{5.18}$$

Proof of (5.18) is straightforward. Q(.) is monotonically decreasing and $0 < r < \Delta/2$. Hence,

$$Q\left(\frac{\frac{\Delta}{2}+r}{\sqrt{2\sigma_n^2}}\right) < Q\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right) \qquad \text{and} \qquad \int_{-r}^{r} Q\left(\frac{\frac{\Delta}{2}-\tau}{\sqrt{2\sigma_n^2}}\right) d\tau < 2rQ\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right). \tag{5.19}$$

Then,

$$\begin{aligned} P(E) &< (1-\frac{r}{\Delta})\left\{\frac{1}{2}Q\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right)+\frac{1}{2}Q\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right)\right\}+\frac{1}{2\Delta}2rQ\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right) \\ &< (1-\frac{r}{\Delta})Q\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right)+\frac{r}{\Delta}Q\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right) \\ &< Q\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right). \end{aligned} \tag{5.20}$$

Using this intermediate bound, we can obtain the relation between the parameters that satisfy the desired probability of error level as follows:

$$\begin{aligned} Q\left(\frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}}\right) < \gamma \Rightarrow \frac{\frac{\Delta}{2}-r}{\sqrt{2\sigma_n^2}} &> Q^{-1}(\gamma) \\ \Rightarrow r &< \frac{\Delta}{2}-\sqrt{2\sigma_n^2}Q^{-1}(\gamma) \end{aligned}. \tag{5.21}$$

Let the auxiliary variable λ be defined as $\lambda = \sqrt{2\sigma_n^2}Q^{-1}(\gamma)$. Then, the optimal r that minimizes ε and complies with *P(E)* constraint is the limiting value $r_o = \frac{\Delta}{2} - \lambda$.

The value of r_o depends on channel noise and desired *P(E)*. When channel noise increases or desired *P(E)* decreases to zero, r_o goes to zero, that is FZDH converges to QIM. On the other hand, for small channel noise and a certain *P(E)*, r_o converges to $\Delta/2$. In the noise-free case, one can assign $\Delta/2$ for r_o.

The same *P(E)* bound is achieved for QIM when

$$Q\left(\frac{\frac{\Delta}{2}}{\sqrt{2\sigma_n^2}}\right) < \gamma \Rightarrow \frac{\frac{\Delta}{2}}{\sqrt{2\sigma_n^2}} > Q^{-1}(\gamma) \quad . \qquad (5.22)$$
$$\Rightarrow \frac{\Delta}{2} > \lambda$$

The constraint in (5.22) also corresponds to the range where r_o is positive. Additionally, since both probability of error values depend on Δ, we assume both of them decrease at the same speed for the range smaller than γ. Hence, it is possible to compare these two methods at an error level smaller than γ, where we have a non-empty *FZ* and non-zero r_o.

When we substitute r_o into (5.14) and compare the embedding distortions of FZDH and QIM, the ratio of embedding distortions appears to be:

$$\frac{\varepsilon_o}{\varepsilon_{QIM}} = \frac{\frac{\Delta^2}{3} - \Delta r_o + r_o^2 - \frac{r_o^3}{3\Delta}}{\frac{\Delta^2}{3}} \qquad (5.23)$$
$$= \frac{1}{8} + \frac{3}{4}\frac{\lambda}{\Delta} + \frac{3}{2}\frac{\lambda^2}{\Delta^2} + \frac{\lambda^3}{\Delta^3},$$

where ε_o is the optimal embedding distortion of FZDH and ε_{QIM} is the embedding distortion of QIM which is equal to the uniform quantization error $\Delta^2/3$. The polynomial in the second line of (5.23) is smaller than one for the range below:

$$\frac{\lambda}{\Delta} \le 0.5 \Rightarrow \frac{\Delta}{2} \ge \lambda \quad . \tag{5.24}$$

The range in (5.24), where FZDH has smaller embedding distortion than QIM, coincides with the *P(E)* constraint of QIM in (5.22). Therefore, we conclude that once (5.21) and the assumption for decreasing at the same rate are both satisfied, the embedding distortion of FZDH is smaller than that of QIM at the same decoding error.

The theoretical comparisons, as well as the assumptions involved, are both verified by means of random experiments. Figure 9 and Figure 10 present the results for two different values of *r*. These experiments are conducted by keeping channel noise constant and varying the embedding distortion (i.e. Δ is varied and *r* value is changed accordingly). In all comparisons the data hiding rate is taken to be equal for each method and this rate is taken as 1 bps. The decoding error probabilities are computed as the average of 10^5 random experiments. We clearly observe that FZDH outperforms QIM for a certain range of WNR. There is a crossover between FZDH and QIM, at which point the constraint in (5.21) becomes obsolete. Naturally, this crossover occurs at a higher *WNR* value for the smaller value of *r*.

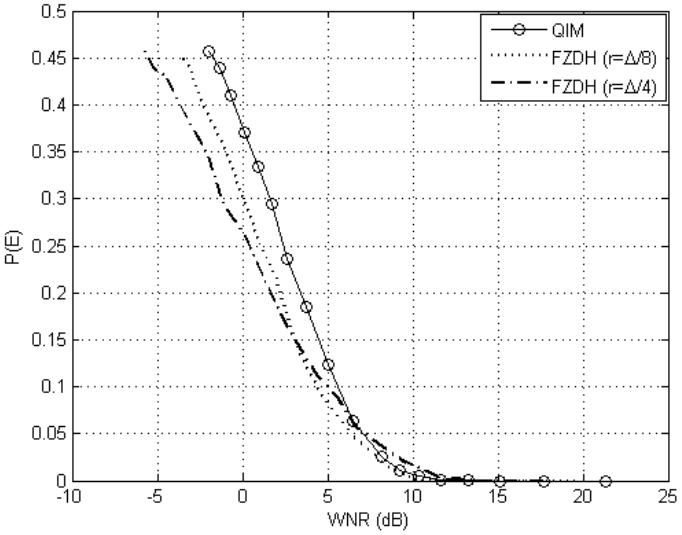


Figure 5.9: FZDH vs. QIM with constant *r* values.

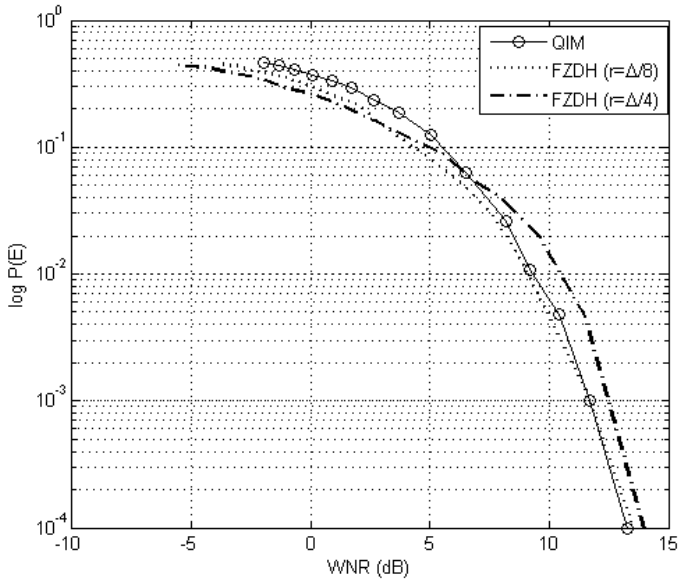


Figure 5.10: FZDH vs. QIM with constant *r* values in semi-log scale.

5.4 Comparison against DC-QIM

DC-QIM is a modified version of QIM, in which embedding function is composed of two parts: quantization of the scaled host signal and a compensation term due to the increased quantization error. The difference between FZDH and DC-QIM is shown in Figure 5.11 by comparing 1-D embedding functions. The fundamental difference that all host signals are modified in DC-QIM whereas there are unaltered host signal ranges in FZDH is clearly seen in Figure 5.11.

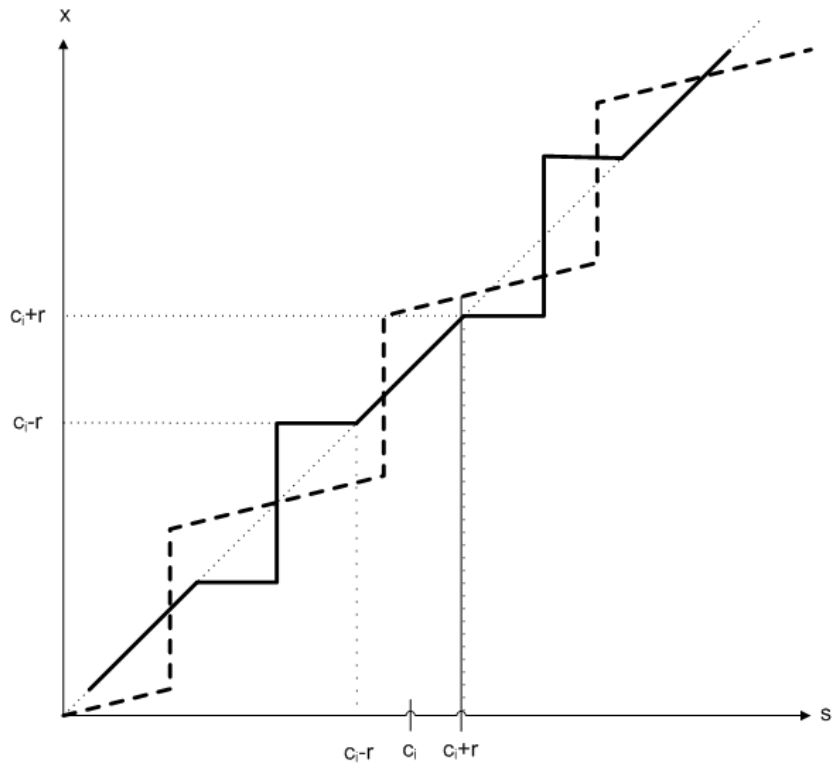


Figure 5.11: Embedding functions of FZDH and DC-QIM (solid FZDH, dashed DC-QIM).

We experimentally compare FZDH against DC-QIM. For this purpose, we utilize the optimized parameters with respect to WNR. Optimal *r* values, which are determined empirically for FZDH, are used during this step. On the other hand, the numerical approximation of the DC-QIM compensation parameter given in [34] for SCS form is used. The compensation parameter is given as $\sqrt{\sigma_w^2/(\sigma_w^2+2.71\sigma_n^2)}$ [34], in which σ_w^2 represents the embedding distortion and σ_n^2 represents the channel noise.

The results of the empirical comparison are shown in Figure 5.12 and Figure 5.13. The results indicate that for low-WNR range, DC-QIM outperforms FZDH, for mid-WNR range both methods have similar performances, whereas for high-WNR range FZDH has a slight superiority.

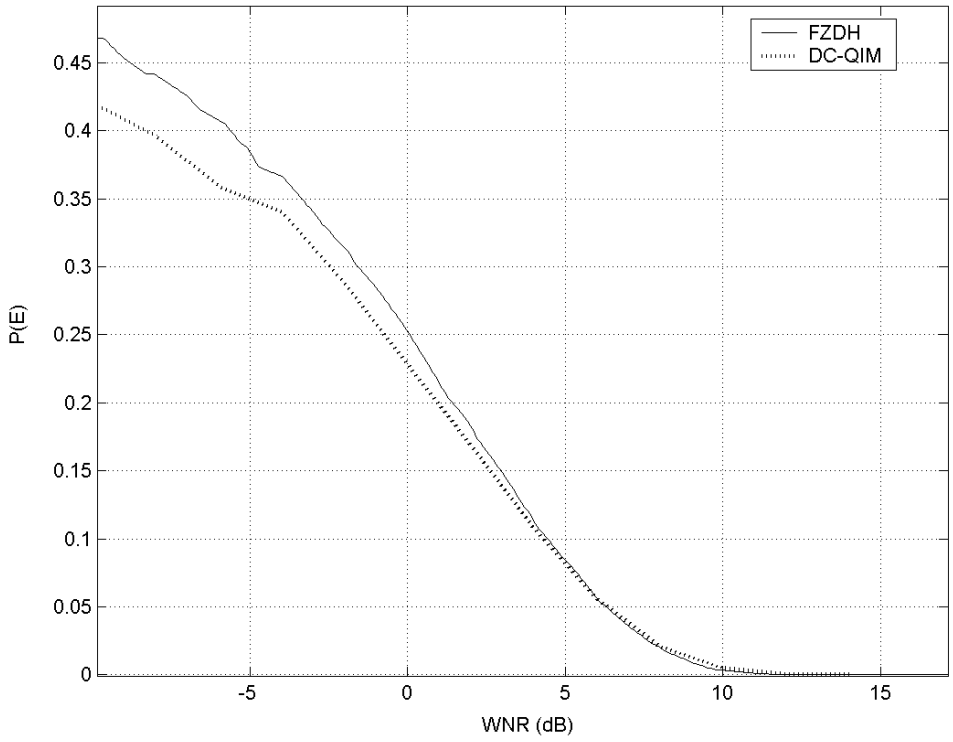


Figure 5.12: FZDH with optimal *r* values vs. DC-QIM.

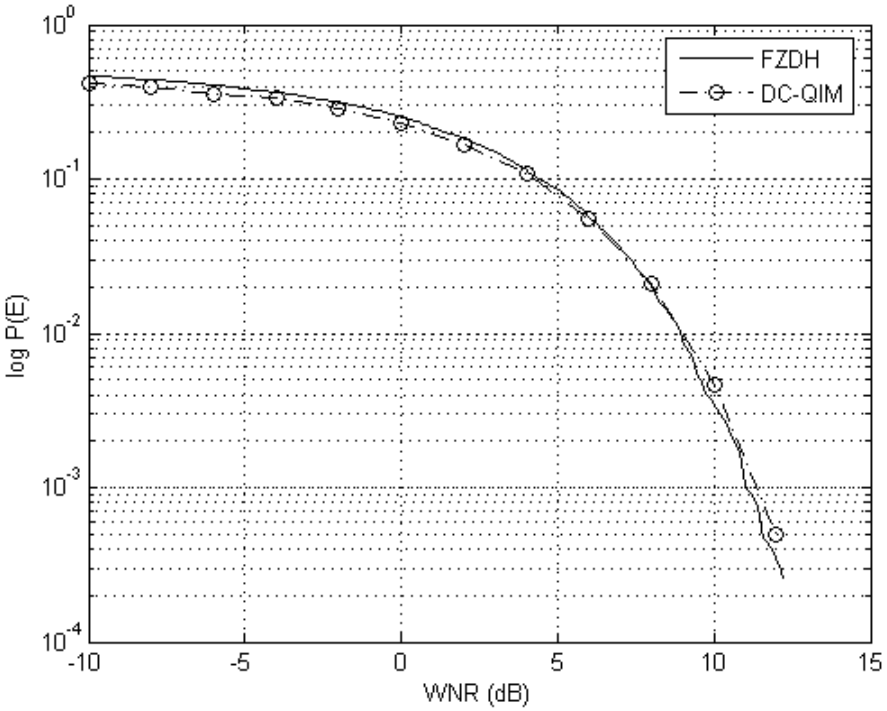


Figure 5.13: FZDH with optimal *r* values vs. DC-QIM in semi-log scale.

In 1-D, FZDH has competitive performance with DC-QIM. Furthermore, FZDH is better than both QIM and DC-QIM around 10 dB *WNR*. As a result of slowly varying nature of optimal *r* values, one can use a typical fixed *r* value for a given *WNR* range without the need for optimality for a fixed *WNR* value.

When we increase the host signal dimension, we empirically observe that the superiority of FZDH becomes more apparent. For this purpose we hide one bit to *N* host samples, where *N* is the dimension of the host signal vector, and hence the data hiding rate is decreased. We utilize cubic lattice for both FZDH and DC-QIM. Using cubic lattice reduces to independently handling each dimension for DC-QIM. On the other hand, FZs become hyperspheres centered at the cubic lattice points. The usage of shifted quantizer cells and reconstruction points as in Dither Modulation [12] increases the minimum distance between quantizers associated with different data bits. Therefore, the robustness

increases in return for the decreased data hiding rate. One should note that increased minimum distance necessitates the usage of higher values of *r* for higher dimensions.

The results for two different dimensions (8 and 20) are reported. Figure 5.14 and Figure 5.15 show the results for *N*=8 and Figure 5.16 and Figure 5.17 show the results for *N*=20. We used typical *r* values since it is prohibitive to obtain optimal values experimentally. The results indicate that FZDH has better decoding error performance than DC-QIM for certain WNR ranges, even with typical fixed *r* values.

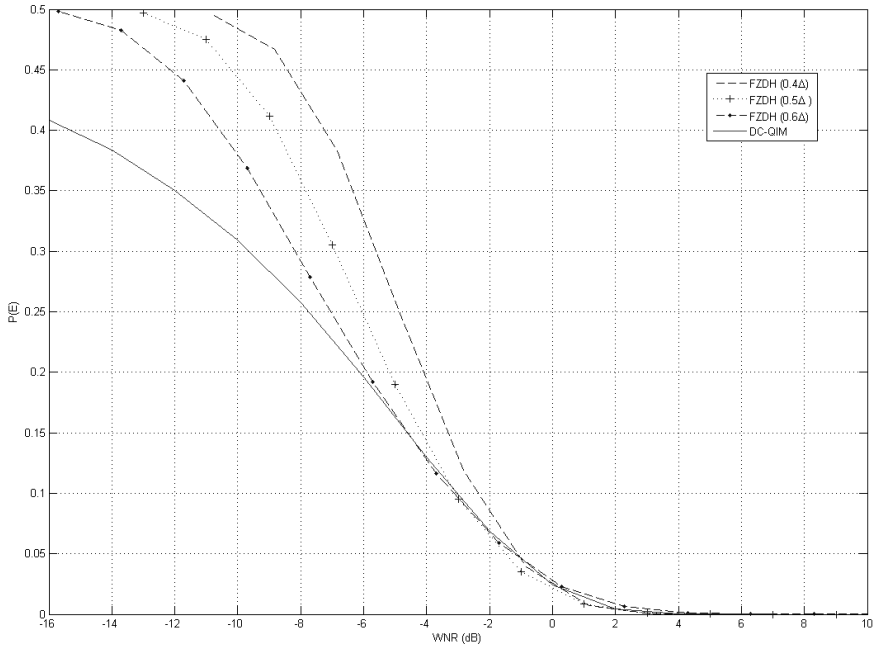


Figure 5.14: FZDH vs. DC-QIM in 8 dimensions.

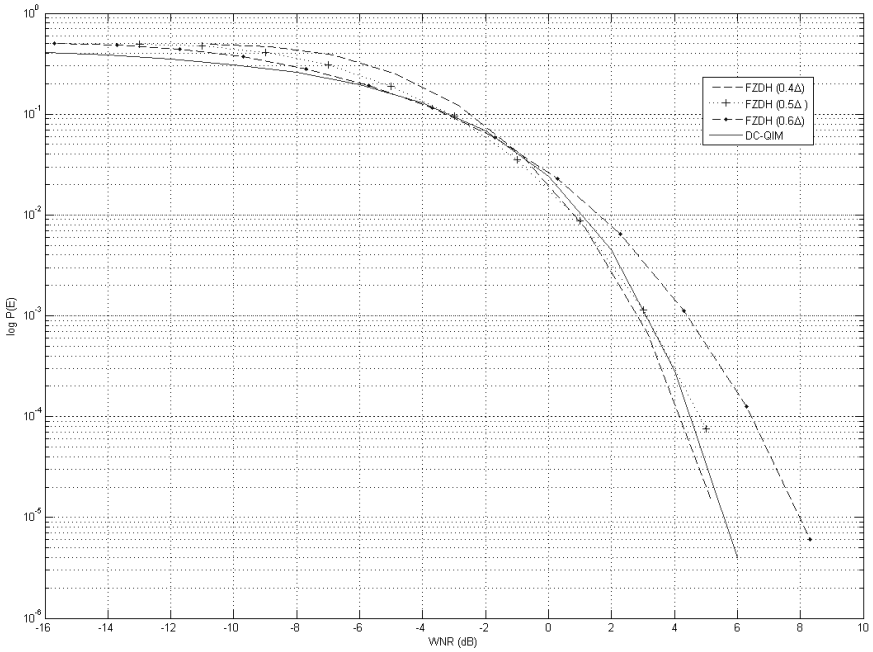


Figure 5.15: FZDH vs. DC-QIM in 8 dimensions in semi-log scale.

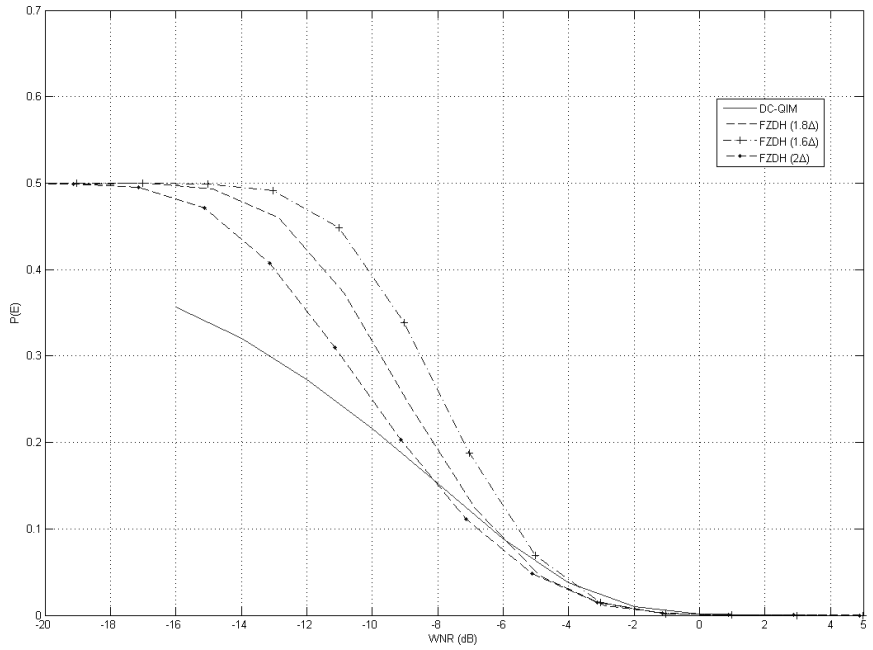


Figure 5.16: FZDH vs. DC-QIM in 20 dimensions.

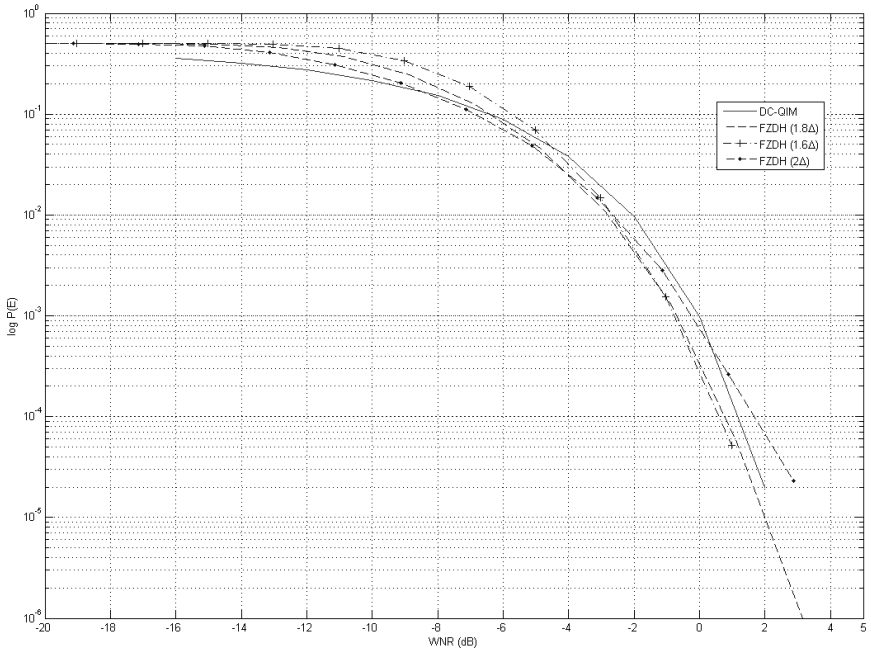


Figure 5.17: FZDH vs. DC-QIM in 20 dimensions in semi-log scale.

5.4.1 Discussion on the Multi-Dimensional Improvement

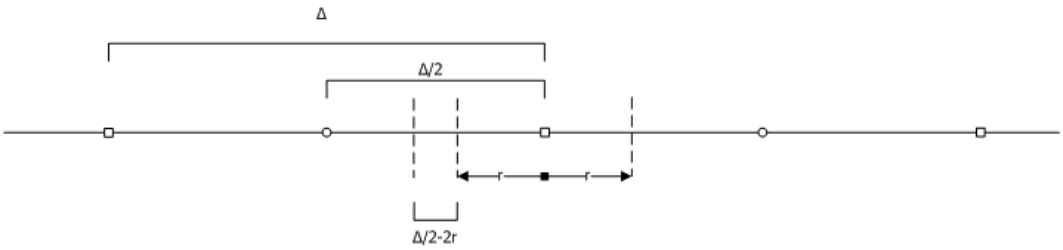
Although we cannot provide a formal proof for the multi-dimensional superiority of FZDH, we propose a conjecture based on the minimum distance of the channel codes.

For cubic lattice, scalar and multi-dimensional embedding distortions are same. Hence, increasing the dimension does not incur an advantage for embedding distortion. However, usage of shifted versions of a cubic base quantizer results in a face centered cubic lattice [57] as the channel codes. Hence the minimum distance of the channel code increases with the host signal dimension [6]:

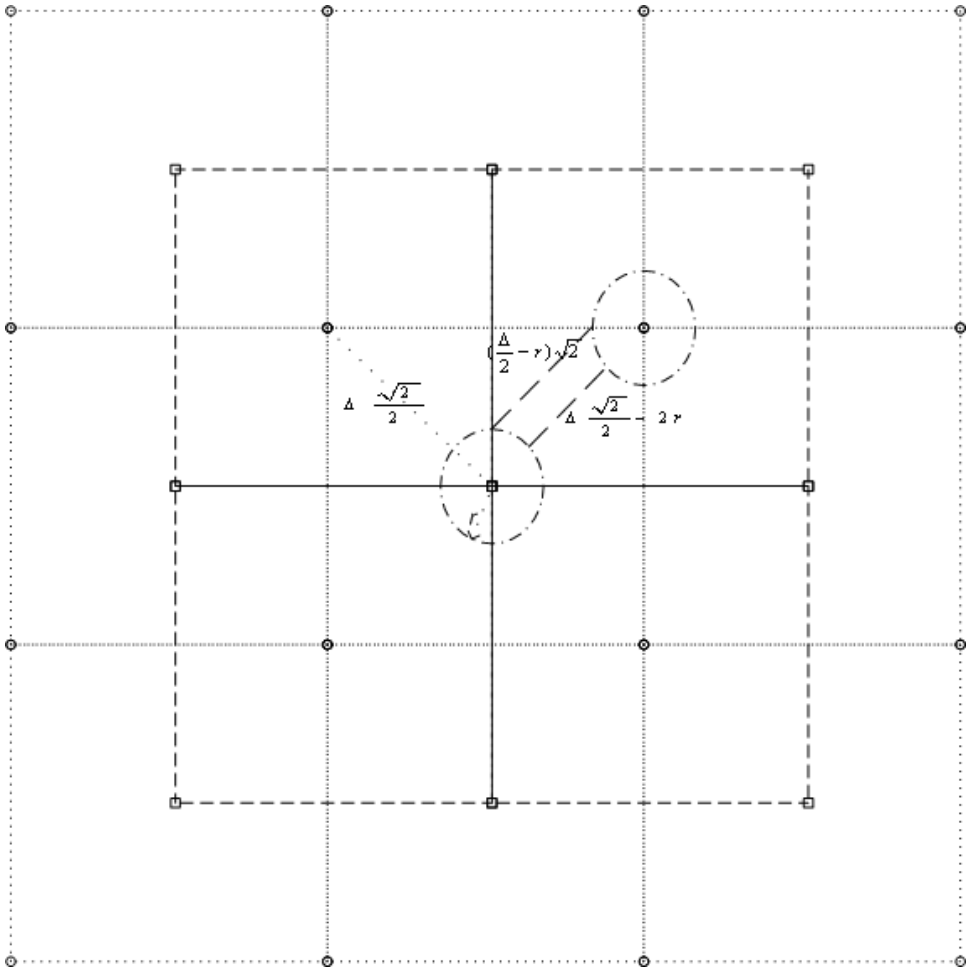
$$d_{\min} = \frac{\Delta}{2}\sqrt{N}\,. \tag{5.25}$$

The robustness of DC-QIM increases due to the increase in d_{min}. A similar argument can also be made for FZDH. Minimum distances for 1-D and 2-D are shown in Figure 5.18. As the dimension increases d_{min} value of FZDH also increases.

In 1-D, d_{min} of FZDH (discarding the range in FZ, which would increase d_{min} further) is ($\Delta/2-2r$). On the other hand, in 2-D, the minimum distance would be equal to $(\Delta/2)\sqrt{2}-2r$ if it increased with the same speed as DC-QIM. However, one could observe that average d_{min} in 2-D is greater than $(\Delta/2)\sqrt{2}-2r$. Therefore, given that in 1-D, DC-QIM and FZDH operate similarly, faster increase of d_{min} with respect to N results in better robustness for FZDH.



(a)



(b)

Figure 5.18: Cubic lattice constellations for (a) 1-D and (b) 2-D (*squares* and *circles* represent the constellations for different *m*).

5.5 Comparison against ST-QIM

We empirically compare FZDH and ST-QIM. For this purpose we apply FZDH in the random spread direction also. Therefore, comparison is essentially performed in the 1-D spread direction.

P(E) values are computed as the average of 10^5 random experiments. The results are given in Figure 5.19 and Figure 5.20 for N=8 and Figure 5.21 and Figure 5.22 for N=20.

Figure 5.19 and Figure 5.21 depict FZDH results for some possible r values. The numerically optimal P(E) values of FZDH are shown in Figures 5.20 and 5.22. They also contain the results of DC-QIM obtained using cubic lattice.

When we observe the results for both dimensions spread FZDH and ST-QIM outperform DC-QIM significantly. Furthermore, for low WNR ranges ST-QIM is better than spread FZDH. However, towards zero error spread FZDH and ST-QIM have comparable performances.

The comparable performances of spread FZDH and ST-QIM is a result of operating in 1-D, since the superiority of Forbidden Zone against distortion compensation diminishes in 1-D. A similar behavior is observed in the comparison of FZDH and DC-QIM in 1-D, which is shown in Figure 5.12.

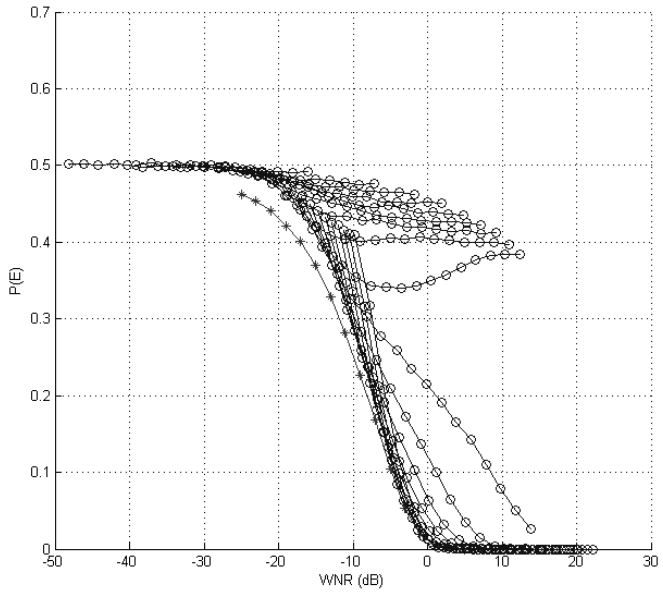


Figure 5.19: ST-QIM vs. typical FZDH results with different *r* values for *N*=8. *Plus* denotes ST-QIM and *circle* denotes FZDH.

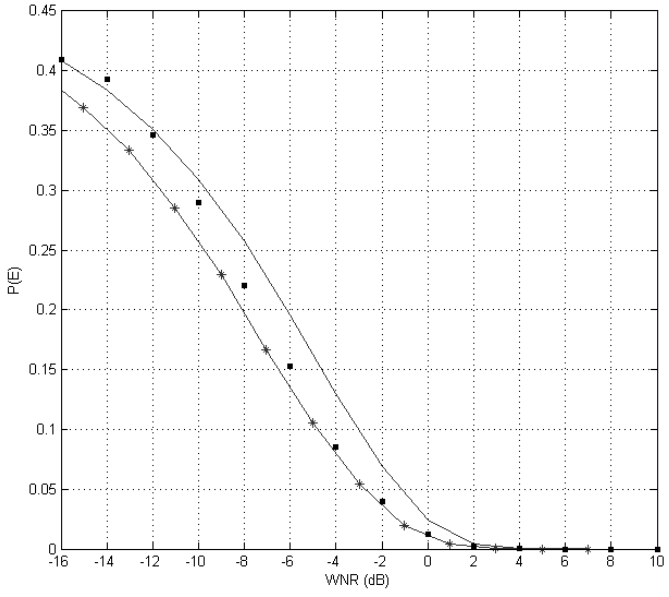


Figure 5.20: Best FZDH vs. ST-QIM vs. DC-QIM for *N*=8.

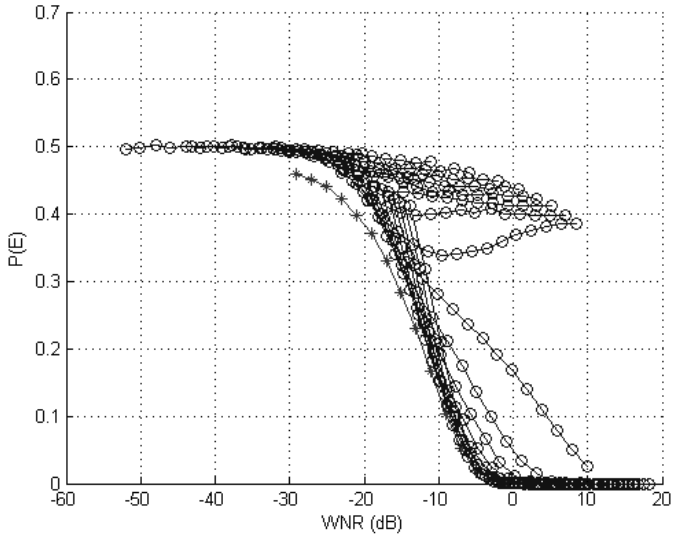


Figure 5.21: ST-QIM vs. typical FZDH results with different *r* values for *N*=20. *Plus* denotes ST-QIM and *circle* denotes FZDH.

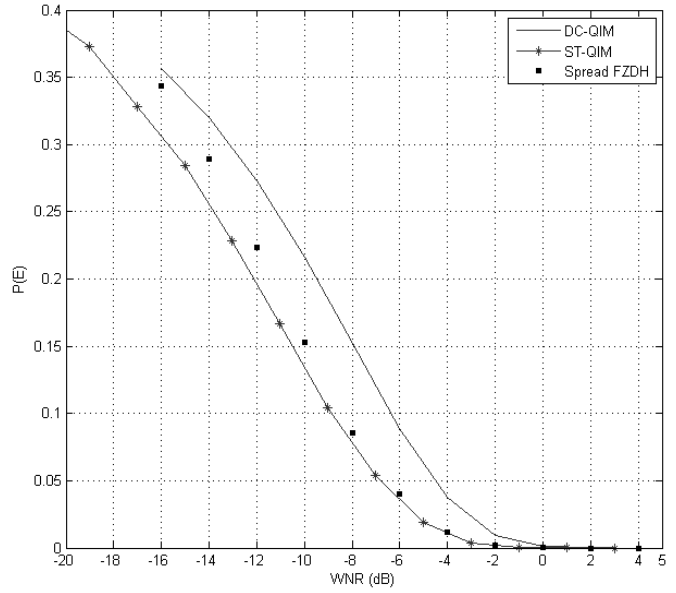


Figure 5.22: Best FZDH vs. ST-QIM vs. DC-QIM for *N*=20.

CHAPTER 6

QUANTIZATION BASED VIDEO DATA HIDING

One of the first video data hiding methods [10] is an application of spread spectrum technique of Cox [58] to the video content. In this method, a pseudo-random watermark sequence that is spread over the entire spectrum is generated. The watermark sequence is shifted in certain amounts according to a specific coding scheme and shifted versions are summed to form a composite sequence. The final watermark sequence is superposed onto the luminance channel of the video frame. At decoder, the same watermark is generated and hidden bits are decoded using correlation.

For video data hiding literature taxonomy, we can place the quantization based methods against the spread spectrum based approaches. There exist various methods [59], [40], [50] that lie within QIM [12] framework. In general, the common process in these types of methods is the application of QIM to some transform coefficients. Although spread spectrum methods have stronger robustness against some attacks, quantization based methods have generally more payload.

With respect to host signal domain, data hiding in video sequences is performed in two major ways: bitstream level and data level. In bitstream level, the redundancies within the current compression standards are exploited. Typically, encoders have various options during encoding and this freedom of selection is suitable for manipulation with the aim of data hiding. However, these methods highly rely on the structure of the bitstream; hence they are quite fragile; in the sense that in many cases, they cannot survive any format conversion or transcoding even without any significant loss of perceptual quality. As a result, this type of data hiding methods is generally proposed for fragile applications, such as authentication. On the other hand, data level methods are more robust to attacks. Therefore, they are suitable for a broader range of applications.

Despite their fragility, the bitstream based methods are still attractive for data hiding applications. For instance, in [60], the redundancy in block size selection of H.264 encoding is exploited to hide data. However, most of the video data hiding methods utilize uncompressed video data. Sarkar *et. al.* [50] proposes a high volume transform domain data hiding in MPEG-2 videos. They apply QIM to low-frequency DCT coefficients and adapt the quantization parameter based on MPEG-2 parameters. Furthermore, they vary the embedding rate depending on the type of the frame. As a result, insertions and erasures occur at the decoder, which causes de-synchronization. They utilize Repeat Accumulate (RA) codes in order to withstand erasures. Since they adapt the parameters according to type of frame, each frame is processed separately.

RA codes are already applied in image data hiding. In [49], adaptive block selection results in de-synchronization and they utilize RA codes to handle erasures. Insertions and erasures can be also handled by convolutional codes as in [61]. The authors use convolutional codes at embedder. However, the burden is placed on the decoder. Multiple parallel Viterbi decoders are used to correct de-synchronization errors. However, it is observed [61] that such a scheme is successful when the number of the selected host signal samples is much less than the total number of host signal samples.

In [62], 3-D DWT domain is used to hide data. They use lowest subband coefficients and do not perform any adaptive selection. Therefore, they do not use error correction codes robust to erasures. Instead, they use BCH code to increase error correction capability. The authors perform 3-D interleaving in order to get rid of local burst of errors. Additionally, they propose a temporal synchronization technique to cope with temporal attacks, such as frame drop, insert and repeat.

Image and video data hiding share many common points; however, video data hiding necessitates more complex designs [59], [40]. Therefore video data hiding continues to constitute an active research topic.

We propose a new block based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH) [52] and RA codes in accordance with an additional temporal synchronization mechanism. FZDH is a practical data hiding

method, which is shown to be superior to the conventional Quantization Index Modulation (QIM) [12]. RA codes are already used in image [49] and video [50] data hiding due to their robustness against erasures. This robustness allows handling de-synchronization between embedder and decoder that occurs as a result of the differences in the selected coefficients. In order to incorporate frame synchronization markers, we partition the blocks into two groups. One group is used for frame marker embedding and the other set is used for message bits. By means of simple rules applied to the frame markers, we introduce a certain level of robustness against frame drop, repeat and insert attacks. We utilize systematic RA codes to encode message bits and frame marker bits. Each bit is associated with a block residing in a group of frames. The random interleaving is performed spatio-temporally; hence, dependency to local characteristics is reduced.

In the proposed approach, host signal coefficients used for data hiding are selected at four stages. First, frame selection is performed. Frames with sufficient number of blocks are selected. Next, only some predetermined low frequency DCT coefficients are permitted to hide data. Then, the average energy of the block is expected to be greater than a predetermined threshold. In the final stage, the energy of each coefficient is compared against another threshold. The unselected blocks are labeled as erasures and they are not processed. For each selected block, there exists variable number of coefficients. These coefficients are used to embed and decode single message bit by employing multi-dimensional form of FZDH that uses cubic lattice as its base quantizer.

This chapter is organized as follows. In Section 6.1 the frame work is described. In the following sections the parts of the framework is explained in detail. Section 6.2 describes selective embedding process. In Section 6.3, block partitioning for message bits and frame synchronization markers is described. In Section 6.4, erasure handling mechanism is explained. In Section 6.5, frame synchronization markers are presented. Section 6.6 is devoted to soft decoding process. In Section 6.7, experiment results and conclusions are given.

6.1 Video Data Hiding Framework

We propose a block based adaptive video data hiding method that incorporates FZDH, which is shown to be superior to QIM [52], and erasure handling through RA Codes. We utilize selective embedding to determine which host signal coefficients will be used in data hiding as in [49]. However, unlike the method in [49], we employ block selection (Entropy Selection Scheme [49]) and coefficient selection (Selectively Embedding in Coefficients Scheme [49]) together. The de-synchronization due to block selection is handled via RA Codes as in [49], [50]. The de-synchronization due to coefficient selection is handled by using multi-dimensional form of FZDH in varying dimensions. In [50], the frames are processed independently. It is observed that [63] intra and inter frames do not yield significant differences. Therefore, in order to overcome local bursts of error we utilize 3D interleaving similar to [62], which does not utilize selective embedding but uses the whole lowest subband of Discrete Wavelet Transform. Furthermore, as in [62], we equip the method with frame synchronization markers in order to handle frame drop, insert or repeat attacks.

Hence, original contribution of this work is to devise a complete video data hiding method that is resistant to de-synchronization due to selective embedding and robust to temporal attacks, whereas it makes use of the superiority of FZDH.

The embedding operation for a single frame is shown in Figure 6.1. Y-channel is utilized for data embedding. In the first step, frame selection is performed. The selected frames are processed block-wise. For each block, only a single bit is hidden. After 8x8 DCT of the block is obtained, energy check is performed on the coefficients that are predefined in mask M. Selected coefficients of variable length are used to hide data bit m. m is a member of message bits or frame synchronization marker bits. Message sequence of each group is obtained by using RA code for T consecutive frames. Each block is assigned to one of these groups at the beginning. After the inverse transform host frame is obtained.

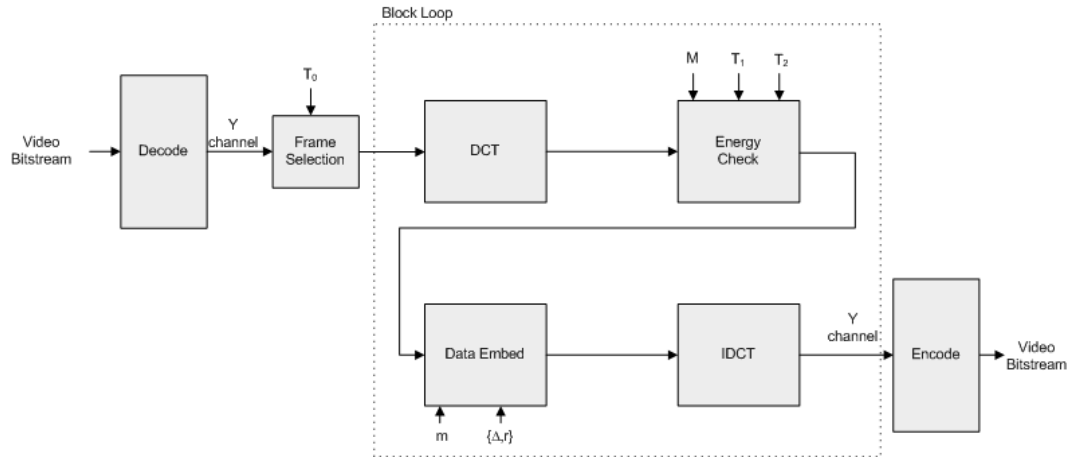


Figure 6.1: Embedder flowchart.

Decoder is the dual of the embedder, with the exception that frame selection is not performed. Figure 6.2 shows the flowchart for a single frame at the decoder. Marked frames are detected by using frame synchronization markers. Decoder employs the same system parameters and determines the marked signal values that will be fed to data extraction step.

Channel observation probabilities (o_m) that will be input to the RA decoder are obtained using the distances to each candidate message bit:

$$o_m = \frac{d(\mathbf{y}, \mathbf{y}_m)^{-1}}{d(\mathbf{y}, \mathbf{y}_0)^{-1} + d(\mathbf{y}, \mathbf{y}_1)^{-1}} \quad . \tag{6.1}$$

Non-selected blocks are handled as erasures. Erasures and decoded message data probabilities (o_m) are passed to RA decoder for T consecutive frames as a whole and the hidden data is decoded.

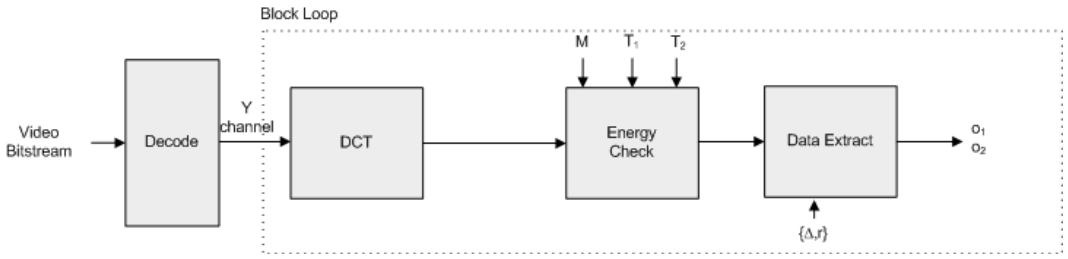


Figure 6.2: Decoder flowchart.

6.2 Selective Embedding

Host signal samples, which will be used during data hiding, are determined adaptively. The selection is performed at four stages: frame selection, frequency band determination, block selection, and coefficient selection.

- *Frame Selection*: Selected number of blocks in the whole frame is counted. If the ratio of selected blocks to all blocks is above a certain value (T_0) the frame is processed. Otherwise, this frame is skipped.

- *Frequency Band*: Only certain DCT coefficients are utilized. Middle frequency band of DCT coefficients shown in Figure 6.3 is utilized similar to [50].

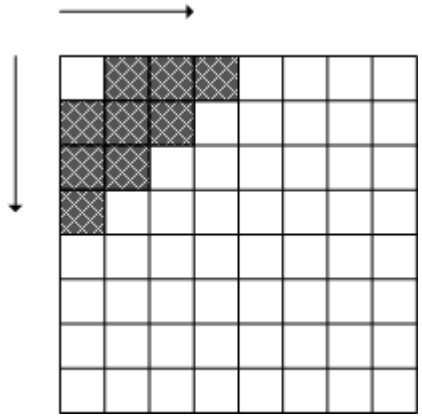


Figure 6.3: Coefficient mask (*M*) denoting the selected frequency band.

- *Block Selection*: Energy of the coefficients in *M* is computed. If the energy of the block is above a certain value (T_1) then the block is processed. Otherwise it is skipped.

- *Coefficient Selection*: Energy of each coefficient is compared to another threshold T_2. If the energy is above T_2, then it is used during data embedding together with other selected coefficients in the same block.

6.3 Block Partitioning

Two disjoint data sets are embedded: message bits (m_1) and frame synchronization markers (m_2). The block locations of m_2 are determined randomly depending on a key. The rest of the blocks are reserved for m_1. Same partitioning is used for all frames. A typical partitioning is shown in Figure 6.4. m_2 is embedded frame by frame. On the other hand, m_1 is dispersed to *T* consecutive frames. Both of them are obtained as the outcomes of the RA encoder.

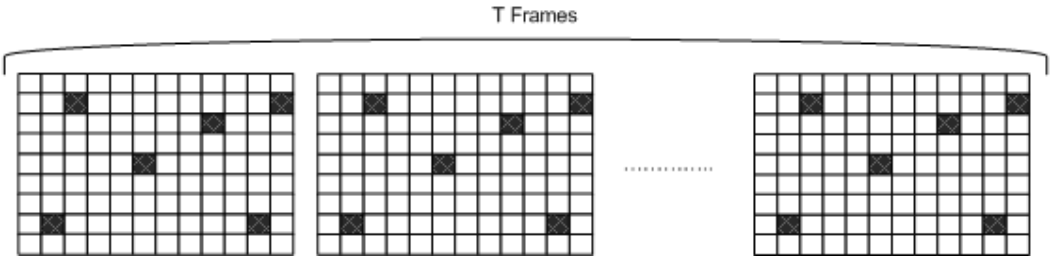


Figure 6.4: Block partitioning for message bits and frame synchronization markers.

6.4 Erasure Handling

Due to adaptive block selection, de-synchronization occurs between embedder and decoder. As a result of attacks or even embedding operation decoder may not perfectly determine the selected blocks at the embedder. In order to overcome this problem, error correction codes resilient to erasures, such as RA codes, are used in image [49] and video [50] data hiding previously.

RA code is a low complexity turbo-like code [64]. It is composed of repetition code, interleaver and a convolutional encoder. The source bits (u) are repeated R times and randomly permuted depending on a key. The interleaved sequence is passed through a convolutional encoder with a transfer function $1/(1+D)$, where D denotes first order delay.

In systematic RA code, input is placed at the beginning of the output as shown in Figure 6.5. In this work, we utilize systematic RA codes to obtain m_1 as u_1+v_1 and m_2 as u_2+v_2. Here, u_1 denotes the uncoded message bits and u_2 is the uncoded frame synchronization marker bits.

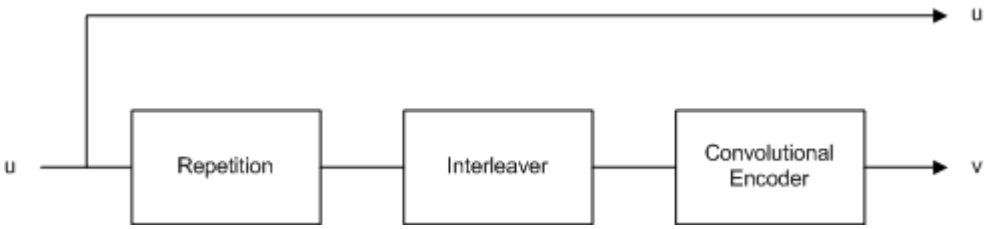


Figure 6.5: RA encoder.

RA code is decoded by using sum-product algorithm. We utilize the message passing algorithm given in [65].

6.5 Frame Synchronization Markers

Each frame within a group of T consecutive frames is assigned a local frame index starting from 0 to $T-1$. These markers are used to determine the frame drops, inserts and repeats, as well as the end of the group of frames at which point all necessary message bits are available for RA decoder.

Frame indices are represented by K_2 bits. After RA encoder RK_2 bits are obtained. Hence, RK_2 blocks are reserved for frame markers. $K_2 >> log_2 T$, so that a small portion of 2^{K_2} codewords is valid. Therefore, one can detect the valid frames with higher probability. Using the sequential frame index information, the robustness increases. Furthermore, RA code spreads the output codewords of the adjacent frame indices; hence, errors are less likely to occur when decoding adjacent frame indices.

Once one reserves RK_2 blocks for frame markers, $T(N-RK_2)$ blocks remain for message bits. Then, the actual number of message bits (K_1) becomes equal to $\lfloor T(N - RK_2)/R \rfloor$, where $\lfloor . \rfloor$ denotes floor operation. The remaining blocks at the end of last frame is left untouched.

6.6 Soft Decoding

At the decoder a data structure of length RK_1 is kept for channel observation probability values, o_m. The structure is initialized with erasures ($o_m = 0.5$ for $m=0$ and $m=1$). At each frame, frame synchronization markers are decoded first. Message decoding is performed once the end of the group of frames is detected.

Two frame index values are stored: current and previous indices. Let f_{cur} and f_{pre} denote the current and previous frame indices, respectively. Then the following rules are used to decode u_1.

- If $f_{cur} > T$, then skip this frame. (This case corresponds to unmarked frame.)
- If $f_{cur} = f_{pre}$, then skip this frame. (This case corresponds to frame repeat.)
- Otherwise, process the current frame. Put o_m values in the corresponding place of the data structure. Non-selected blocks are left as erasures.
- If $f_{cur} < f_{pre}$, then the end of the group of frames is reached. Decode the message bits and obtain u_1. Initialize data structure.

6.7 Robustness Experiments

We perform the experiments at two stages. First, we measure the raw decoding error performance without any error correction and compare QIM and FZDH. Then, we apply the complete framework and measure the performance of FZDH against common video processing attacks.

For the first stage we utilize MPEG-2 DVB-S videos from 5 different TV channels. The total duration of the host video set is equal to 60 minutes. The resolution of the videos is 720 by 576. Initial bitrates of the videos range from 6 Mbps to 9 Mbps. The marked

videos are re-encoded at various bitrates and decoding errors are computed. The raw channel performance is measured by hiding the same data bit (i.e. constant m) to the whole video. Additionally, frame selection is not active. Hence de-synchronization due to selective embedding is not affective.

QIM and FZDH are compared at the same embedding distortion and data hiding rate. Two different embedding distortion values are utilized: 48 dB and 51 dB average PSNR. Embedding distortion is computed as the average PSNR between host and marked frames. The data hiding parameters that yield these values are tabulated in Table 6.1. We should note that different pairs of (Δ,r) may yield the same embedding distortion. We make use of typical values determined manually. T_1 is selected as 2000 and T_2 is set to 1000. A typical host and marked frame pair for FZDH (at 48 dB) is shown in Figure 6.6.

Table 6.1: Data hiding parameters.

Average Embedding Distortion	**QIM (Δ)**	**FZDH (Δ,r)**
48 dB	30	40,4
51 dB	15	20,2

(a)

(b)

Figure 6.6: Typical host (a) and marked frame (b) pair for FZDH.

Comparison results against MPEG-2 compression attack are shown in Figures 6.7, 6.8, 6.9, and 6.10 for Intra and Inter frames, respectively for 48 dB and 51 dB cases each. We observe that FZDH is superior to QIM especially at low compression bitrates and small

embedding distortion values. These conditions correspond to low WNR values; hence, the results comply with the reported results for AWGN in [52]. Furthermore, we observe the Intra and Inter frames do not yield significant differences.

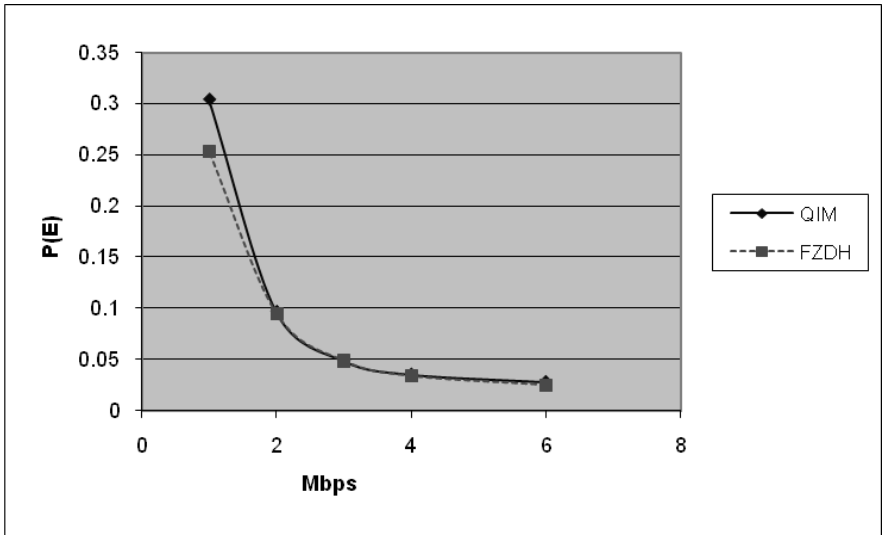


Figure 6.7: FZDH vs. QIM (Intra frames, 48 dB average embedding distortion).

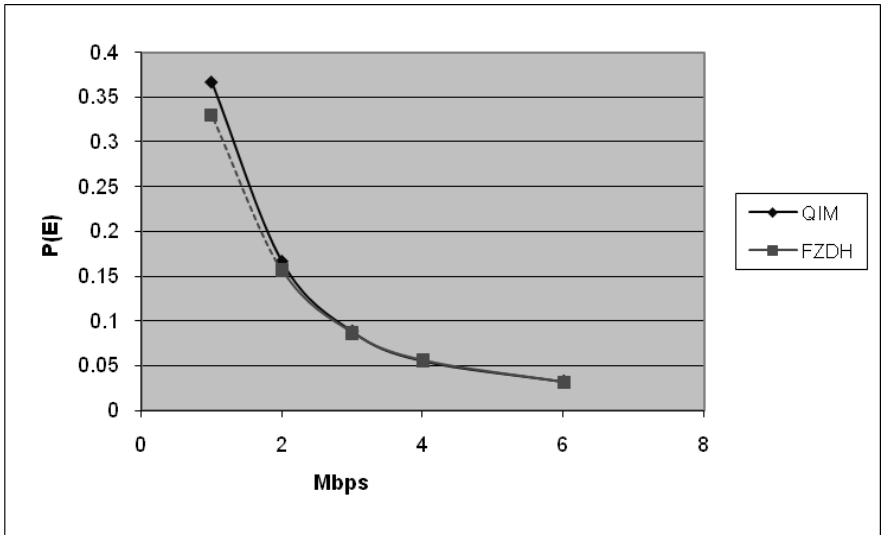


Figure 6.8: FZDH vs. QIM (Inter frames, 48 dB average embedding distortion).

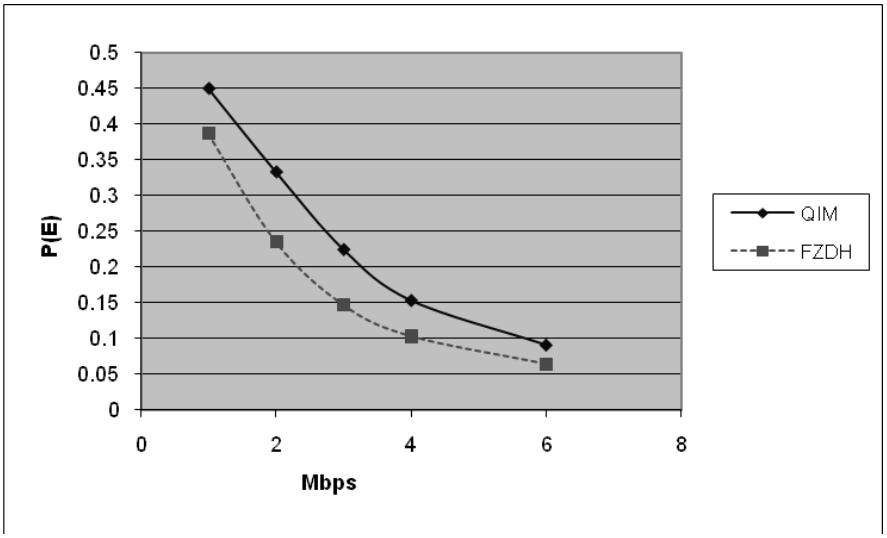


Figure 6.9: FZDH vs. QIM (Intra frames, 51 dB average embedding distortion).

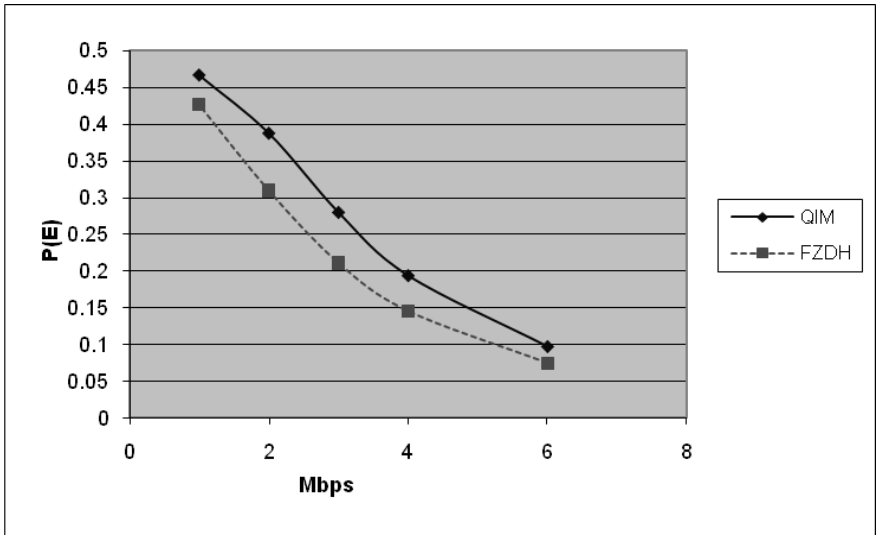


Figure 6.10: FZDH vs. QIM (Inter frames, 51 dB average embedding distortion).

At the second stage, we apply error correction and assess the performance of FZDH against some common video processing attacks. We utilize a typical TV broadcast material of 10 minutes. We prefer a smaller duration, which is still accurate to draw conclusions, due to the computational burden of RA decoding. The format of the test video is MPEG-2 at 9 Mbps and its resolution is 720 by 576.

The system parameters are tuned manually. We utilize the following values during the experiments: T_0=0.05, T_1=1000, T_2=500, K_1=10, T=3. One should note that threshold values are selected for this resolution and block size of 8x8. Different dimensions might require some other threshold values. Typical R values are used according to the attack. Once these values are set, the embedding rate is determined. For instance for R=150, K_1 is 98, i.e., 32 bits are hidden per frame. Typical host and marked frames are shown in Figure 6.11.

(a)

(b)

(c)

Figure 6.11: Typical host and marked frames for FZDH: (a) host frame, (b) marked frame (with Δ=40,r=4), (c) marked frame (with Δ=80,r=8).

Firstly, we observe the effect of the parameters on the number of selected block rate. Results for a 4-second video segment are shown in Figure 6.12. The number of the

selected blocks depends on the content and varies slowly with time. The abrupt changes correspond to shot boundaries. We observe that embedder and decoder select different number of blocks. Interestingly, for low rates the decoder can select higher number of blocks. However, due to frame selection at embedder (with respect to T_0), the decoder can correctly determine the group of frame and extract the hidden data as a result of the frame synchronization markers.

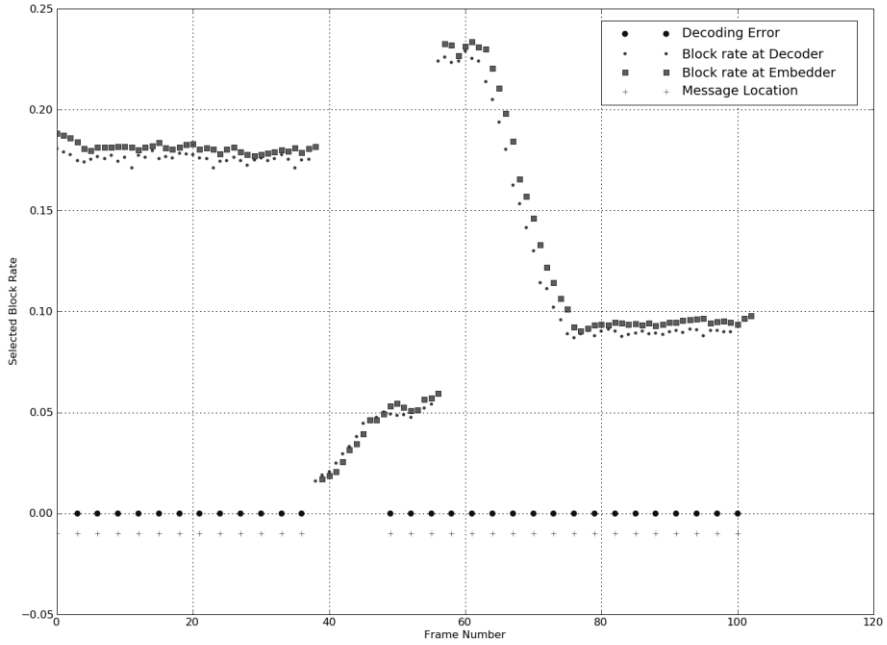


Figure 6.12: Typical selected block rates and decoding errors for T_0=0.05, T_1=1000, K_1=10, T=3, R=150, Δ=80, r=8 and MPGE-2 4 Mbps compression. Circle denotes decoding error, square denotes selected block rate at embedder, dot denotes selected block rate at decoder and plus denotes the frame locations where message is embedded.

Secondly, we observe the decoding error performance against compression attack. We utilize typical bitrates for this resolution. We increase R to the point where one obtains

error-free decoding. The results are tabulated in Table 6.2 for two different embedding distortion values. 46.0 dB and 40.46 dB embedding distortion values are obtained with the following FZDH parameters {Δ=40, *r*=4}, {Δ=80, *r*=8}, respectively. The results indicate that we need repetition number higher than the erasure rate. The reason for this observation is due to the fact that decoding errors occur as a result of compression as well as the erasures due to the block selection. Furthermore, we observe that H.264 appears to be a stronger attack compared to MPEG-2. Therefore, we need higher repetition for error-free decoding.

Table 6.2: Decoding error for MPEG-2 and H.264 compression attacks at 4 Mbps and 2 Mbps.

		Embedding Distortion (46.0 dB)		**Embedding Distortion (40.68 dB)**	
		R=100	*R*=150	*R*=100	*R*=150
MPEG-2	4 Mbps	0.0170089	0.014457	0.000098	0
	2 Mbps	0.207233	0.136266	0.0349629	0.0281465
H.264	4 Mbps	0.327757	0.230392	0.007989	0.000469
	2 Mbps	0.494789	0.482247	0.151802	0.070663

Thirdly, we test the performance of the method against another common video processing: frame-rate conversion. The frame rate of the original video is 25 fps. We change this frame-rate to a higher as well as a lower value and measure the decoding error rate. We should note that frame-rate conversion could be achieved in various ways, some of which could be quiet complex. However, we utilize an open source codec (ffmpeg[1]), which performs frame-rate conversion by frame drop/repeat and re-encoding. First, we present the selected block rates at embedder and decoder in Figure 6.13 by using the same video segment in Figure 6.12. The frame rate of the marked video is changed to 30 fps from 25 fps. We observe that even if the message locations are shifted

[1] http://www.ffmpeg.org

we can successfully decode the message bits as a result of the frame synchronization markers.

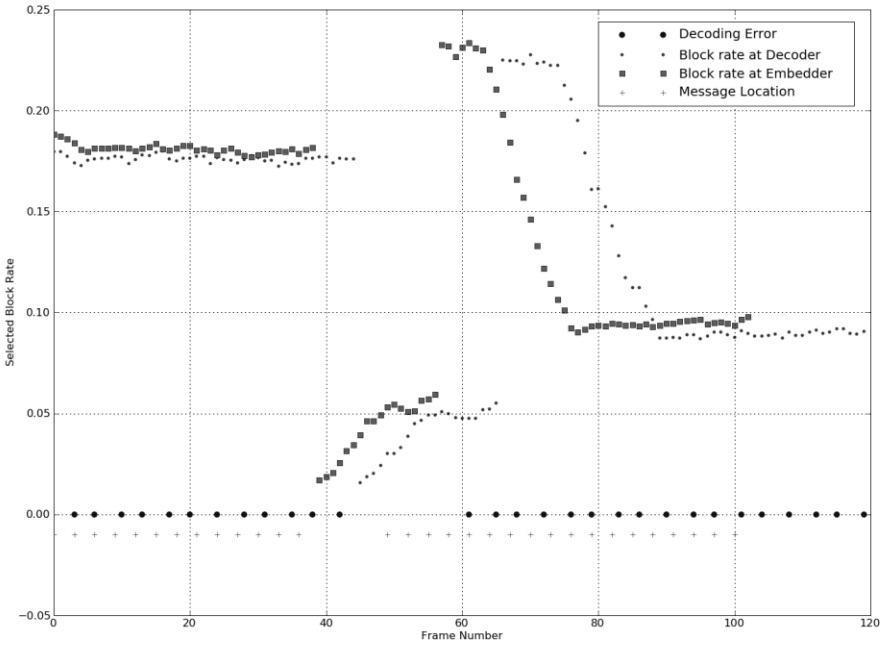


Figure 6.13: Typical selected block rates and decoding errors for T_0=0.05, T_1=1000, K_1=10, T=3, R=150, Δ=80, r=8, MPGE-2 4 Mbps compression against frame rate conversion from 25 fps to 30 fps. Circle denotes decoding error, square denotes selected block rate at embedder, dot denotes selected block rate at decoder and plus denotes the frame locations where message is embedded.

The total decoding error results are tabulated in Table 6.3. We observe that different rates have similar results. Frame insertions and drops do not differ as long as they can be detected correctly by synchronization markers. We should note that for lower fps value of 23.98, frame drop rate is so small and at most one frame per group of frames can be dropped. Additionally, we require higher repetitions than compression attack.

Table 6.3: Decoding error for frame rate conversion with frame drops and repeats at 40.68 dB embedding distortion and MPEG-2 4 Mbps.

Frame Per Second	***R*=150**	***R*=200**
30	0.000221199	0
23.98	0.00020057	0

Finally, we test the scaling performance. For this purpose, we downscale the marked video, and then, upscale the attacked video to its original size. Scaling operations are performed using ffmpeg library. The decoding error values for three different dimensions are given in Table 6.4.

Table 6.4: Decoding error for downscaling at MPEG-2 4 Mbps and 40.6 dB average embedding distortion.

Size	***R*=200**	***R*=250**
CIF (352x288)	0.492966	0.443106
VGA (640x480)	0.0136099	0.00362576
SVGA (800x600)	0.0150746	0.00525774

Scaling test results indicate that CIF resolution attack totally removes the hidden data. On the other hand, we can obtain better results for VGA and SVGA resolutions. However, error-free decoding is not possible with the utilized system parameters. One should increase the repetition rate, embedding distortion, number of frames in order to achieve error-free decoding.

As a summary, the results indicate that the framework can be successfully utilized in video data hiding applications. However, insertion of Human Visual System based spatio-temporally adaptation of data hiding method parameters as in [67] remains as a future direction.

6.8 Subjective Visual Quality Experiments

In order to evaluate the proposed video data hiding framework visually, we performed subjective quality experiments. A test setup similar to [71] is prepared. Five visually quality levels are determined. The levels start from 1 up to 5 representing annoyingly different and identical, respectively. The level scores and their meanings are given in Table 6.5.

Five different levels of embedding distortion are utilized in the experiments. The range of embedding distortions varies from 36 dB to 46 dB average PSNR. The utilized values and their labels are given in Table 6.6. The relevant system are parameters are chosen as T_0=0.05, T_1=1000, T_2=500, K_1=10, T=5, and R=100.

Table 6.5: Visual quality levels.

Visual Quality Level	**Interpretation**
5	Identical
4	Suspicious of changes
3	Small visible differences
2	Highly different
1	Annoyingly different

Table 6.6: Embedding distortion levels utilized in subjective tests.

EmbeddingDistortion Levels	**PSNR**
A	36 dB
B	38 dB
C	40 dB
D	43 dB
E	46 dB

Four different host videos of 15 seconds are prepared. The host videos are MPEG-2 DVB-S bitstreams with a resolution of 720 by 576.For each host video; five different marked videos are generated with the embedding distortion levels given in Table 6.6.

The host and marked videos are presented to the subject set by set. The subjects watch the videos at full resolution on a 19 inch LCD monitor at a distance of 1 meter. First, the subject watches the host video set and then the marked videos in any order. The subject can watch the videos as many times as he desires.

The individual scores of the subjects for each set are tabulated in Table 6.7. The average scores with respect to different embedding distortion levels are given in Table 6.8

Table 6.7: Individual scores of the subjects for four different video sets.

Subject	**Set 1**					**Set 2**					**Set 3**					**Set 4**				
	A	**B**	**C**	**D**	**E**	**A**	**B**	**C**	**D**	**E**	**A**	**B**	**C**	**D**	**E**	**A**	**B**	**C**	**D**	**E**
Subject 1	3	4	5	5	5	2	3	4	4	5	3	4	4	5	5	2	3	4	4	5
Subject 2	2	3	4	5	5	2	3	4	5	5	2	3	5	5	5	2	3	3	5	5
Subject 3	3	4	4	5	5	4	5	5	5	5	5	5	5	5	5	4	5	5	5	5
Subject 4	2	3	4	4	5	1	1	2	3	4	3	4	4	5	5	1	2	3	4	4
Subject 5	3	4	5	5	5	3	3	4	4	5	3	4	4	5	5	3	3	4	5	5
Subject 6	1	2	4	4	5	1	2	3	4	5	2	3	4	4	5	1	2	3	4	4
Subject 7	3	3	4	4	5	3	3	3	4	4	3	4	4	5	5	2	3	4	5	5
Subject 8	1	2	3	4	5	1	2	3	4	5	3	4	4	5	5	1	1	3	5	5
Subject 9	2	2	3	4	5	1	2	3	3	4	2	2	4	5	5	2	2	3	4	5
Subject 10	1	3	4	4	5	1	1	1	2	3	2	3	3	4	5	1	2	2	3	4
Average	2.1	3	4	4.4	5	1.9	2.5	3.2	3.8	4.5	2.8	3.6	4.1	4.8	5	1.9	2.6	3.4	4.4	4.7
Standard Deviation	0.88	0.82	0.7	0.5	0	1.1	1.2	1.1	0.9	0.7	0.9	0.84	0.57	0.4	0	1	1.1	0.84	0.7	0.5

Table 6.8: Average scores for five different embedding distortion levels.

Embedding Distortion Level	Average Score
A (36 dB)	2.2
B (38 dB)	2.9
C (40 dB)	3.7
D (43 dB)	4.4
E (46 dB)	4.8

The average results indicate above 43 dB PSNR, there is no visible artifact due to data hiding. Around 40 dB PSNR small differences occur. Below 38 dB PSNR the marked videos contain highly visible distortions.

As a result of the subjective experiments we conclude that the robustness experiments reported in Section 6.7 reside within the visually safe region.

6.9 Comparison Against Other Well-known Methods

We compare the proposed framework against the canonical video watermarking methods JAWS [10] and a more recent quantization based method [50].

JAWS is a spatial domain additive spread spectrum based watermarking method [10]. It is utilized for DVD copyright protection [72] and broadcast monitoring [19]. In JAWS, luminance channel of the frame in tiles. A pseudo-random watermark pattern is generated. The size of this pattern matches the size of the tile elements. The payload is increased by using shifted versions of the base watermark. The amount of payload depends on the number of shifts and possible shift locations determined by a fixed grid. The superposition of the base watermark and its shifted versions is added to each tile element of the luminance channel spatially. The strength of the watermark is adjusted by means of a global scaling parameter. At the decoder, the received frame is folded by averaging tile elements and the same base watermark is generated. Correlation is

performed to detect the locations of the peaks in Fourier domain. The relative positioning of the peaks give the decoded message bits.

We compare the proposed framework and JAWS at the same data hiding rate and embedding distortion. We utilize the same host video used for the experiments whose results are given in Table 6.2. For JAWS, we utilize a tile with 4 elements, 4 shift locations inside a grid of 32x32. The resultant data hiding bit rate is 30 bits per frame. This rate is assured with R=150 (33 bits per frame) in the proposed framework. The global scaling parameter of JAWS is varied to adjust the embedding distortion. The results of JAWS against MPEG-2 compression attack are given Table 6.9. When we compare Table 6.2 and Table 6.9, we observe that at the same embedding distortion (40 dB PSNR), the proposed framework is significantly superior to JAWS. The results indicate that for high payload applications JAWS cannot achieve an acceptable performance level.

Table 6.9: Decoding error values for JAWS against MPEG-2 compression attack.

Global Scaling Parameter	**Average Embedding Distortion**	**2 Mbps**	**4 Mbps**	**6 Mbps**
0.25	40.2 dB	0.30375	0.1436	0.1164
0.5	34.44 dB	0.15425	0.10455	0.0987

We compare the proposed framework and adaptive quantization based scheme of Sarkar et. al. [50] by means of the results they report. For this purpose we increase the data embedding rate (R=25 yields 249 bits per frame) and the embedding distortion (37.06 dB PSNR) in order to reach the same operation conditions with [50]. Furthermore, we utilize 5 consecutive frames (i.e. T=5). With these parameters, the decoding bit error of the proposed framework is 0.06125. The performance of [50] is given in terms of "frame error rate", which corresponds to the frames with non-converging RA decoder. For GOP size of 6, best frame error rate of [50] is given as 0.082 at 36.26 dB PSNR embedding

distortion. Assuming converging frames yield zero decoding error, we can compare both performance values. Although we cannot precisely conclude on the superiority of any method, since host video is not same, we can claim that the methods have comparable performances. However, we should note that at this level of embedding distortion visible artifacts occur and hence for a more realistic comparison embedding distortion should be decreased to an acceptable level.

CHAPTER 7

SUMMARY and CONCLUSIONS

This thesis introduces new data hiding methods and visual applications of the proposed methods. The methods are compared against state-of-the-art methods and the improvements are shown experimentally and theoretically. The performances of the methods are also examined in typical visual applications. Finally, an error-free video data hiding framework is proposed and tested with various common attacks.

The very first outcome of the thesis work is TCQ-IS, which as a product of the search for practical multi-dimensional data hiding. The proposed method is based on Trellis Coded Quantization (TCQ). Initial state selection is arbitrary in TCQ; hence one can embed information by enforcing the selection of the initial state. TCQ-IS exploits this redundancy. As a result a practical multi-dimensional data hiding method is obtained. The data hiding rate of TCQ-IS depends on only the trellis instead of host signal dimension. Hence the same structure can be used for any dimension. This way the prohibitive task of designing high dimensional quantizers are eliminated.TCQ-IS is compared against QIM and a trellis path selection based algorithm. Especially for low WNR range, it is observed that TCQ-IS has superior performance to the compared methods. Since tThe data hiding rate of TCQ-IS depends solely on the trellis structure, its robustness does not increase with the host dimension. This practical issue imposes a limitation on the robustness.

FZDH is the second contribution of this thesis. FZDH approaches to the data hiding problem from a different perspective than coding techniques: there exists uncoded portions of the host signal range. The main motivation is to keep the host signal unaltered for some ranges, which should be determined according to the desired level of robustness, embedding distortion amount and channel noise level. Generic formulation of

FZDH is given as well as its practical realizations that involve quantizers. FZDH is shown to be superior to QIM empirically and theoretically. It is also compared with DC-QIM experimentally. In 1-D both methods have similar performances. However, as the host signal dimension increases the performance of FZDH becomes better. The reason behind this improvement is established by means of an argument based on the minimum distance of the channel codes. Additionally, FZDH is compared with ST-QIM. It is observed that both methods outperform DC-QIM with cubic lattice. ST-QIM appears to have better performance for low WNR. Nevertheless, FZDH and ST-QIM perform compatibly as error approaches to zero.

The third contribution of this thesis is the proposed video data hiding framework that consists of FZDH, selective embedding, erasure handling, and temporal synchronization. The proposed video data hiding framework makes use of erasure correction capability of Repeat Accumulate codes and superiority of FZDH. Selective embedding is utilized to determine host signal samples suitable for data hiding. The temporal synchronization scheme is employed to withstand frame drop and insert attacks.

RA codes were previously used in image and video data hiding due to their robustness against erasures. This robustness allows handling the de-synchronization between embedder and decoder that occurs as a result of the differences in the selected host signal samples. In order to incorporate frame synchronization markers, the blocks are partitioned into two groups. One group is used for frame marker embedding and the rest is reserved for message bits. By means of simple rules applied to the frame markers we introduce certain level of robustness against frame drop, repeat and insert attacks. We utilize systematic RA codes to encode message bits and frame marker bits. Each bit is associated with a block residing in a group of frames. The random interleaving is performed spatio-temporally; hence dependency to local characteristics is diminished. Host signal coefficients used for data hiding are selected at four stages: frame selection, frequency band selection, block selection, and DCT coefficient selection. The unselected blocks are labeled as erasures and they are not processed. For each selected block there exists variable number of coefficients. These coefficients are used to embed and decode single message bit by employing multi-dimensional form of FZDH that uses cubic lattice as its base quantizer.

The proposed framework is tested with typical broadcast material against common video processing attacks. The decoding bit error values are reported for typical system parameters.

The framework is also compared with other video data hiding methods. The proposed framework outperforms JAWS [10], whereas has a comparable performance with another quantization based method [50].

Subjective visual experiments are performed in order to evaluate the embedding distortion level of the data hiding process. The subjective experiment results are given in accordance with the corresponding objective distortion metric in terms of PSNR values. The results of these experiments assure that all attack performances are measured using system parameters that yield embedding distortion levels within the visually safe zone.

The results indicate that the framework can be successfully utilized in video data hiding applications.

Remarks on the Contributions and Future Directions

TCQ-IS is a practical but a limited method. It can be preferred to DM with cubic lattice. However, as the host dimension increases its advantage diminishes. Therefore, there is a certain upper limit of the host signal dimension for TCQ-IS to be preferable.

Merger of TCQ-IS and FZDH can yield better results and remains as a topic for further exploration.

In [6], it is stated that DC-QIM does not have optimal distortion compensation claim and it is possible to find embedding functions that exhibit slightly better performance. Furthermore, the gain would be negligible and the complexity of the optimization problem involved in finding the best embedding function might render this effort prohibitive [6]. However, FZDH provides a practical framework and substantial improvement over DC-QIM in higher dimensions. We should note that there is no

optimization involved in FZDH and its computation complexity is comparable to DC-QIM.

The theoretical analysis of FZDH in multi-dimensions requires further effort due to its complexity. However, implementing FZDH with different types of lattices as in [46], [66] remains as a promising direction. This way denser packing paradigm [57] will lead to decreased embedding distortion and hence, the same decoding error level can be reached at a smaller *WNR*. Another future direction is fusion of *Distortion Compensation* and *Forbidden Zone* concepts. As a result of such an approach, the embedding function will have two degrees of freedom.

Additionally, regarding the comparison of FZDH and ST-QIM, projection onto 1-D diminishes the advantage of FZDH, and hence ST-QIM outperforms FZDH for low WNR. In order to preserve the advantage of FZDH in high dimensions, projections onto higher dimensions instead of 1-D can be tested. In the projected domain, lattices other than cubic can be utilized in order to make use of the superiority of FZDH over DC-QIM in high dimensions. This remarks remains as a promising future direction.

As a final remark on FZDH, although steganography is not within the scope of this thesis, steganalysis of FZDH may yield promising results. Conceptually, we believe that there is a potential in keeping some portion of the host signal intact for making the detection of the hidden message harder. Especially, for lower *WNR* range, we can obtain larger *FZ*s and larger parts of the host signal range remain unaltered. Hence, the distributions of the host and marked signals become more similar and indistinguishable. This way, FZDH may yield steganalytically better performance with respect to conventional quantization based methods.

The proposed video data hiding framework provides a complete solution that can be used in real-life applications. However, there exist potential improvements.

Firstly, we utilize constant system parameters for all selected host signal samples. Determining parameters adaptively according to HVS can increase perceptual

performance. However, we should note that de-synchronization in these parameters would necessitate additional control mechanisms.

Secondly, we handle consecutive frames as a group. In order to diminish local dependence further, frames belonging to a message packet can be selected randomly from the whole video. Naturally, this type of improvement is not suitable for streaming applications but valid for off-line applications.

Thirdly, especially under high embedding distortion some frames exhibit flickers. In order to avoid or decrease the effect of this problem, we can employ 3-D transforms or averaging between frames.

The proposed framework contains some manually adjusted thresholds. A systematic mechanism for determining the thresholds would be helpful. For this purpose, possible ranges for the thresholds can be learned from a large set of training samples and some heuristics can be proposed to select reasonable values.

Another remark is that the framework suffers from geometric attacks as all block based methods that heavily rely on spatial synchronization. In order to gain robustness against geometric attacks, spatial synchronization markers can be embedded to detect and cancel such attacks. Additionally, the feasibility of passive approaches that involve the utilization of interest points can be investigated.

Lastly, depending on the prevision regarding the potential of FZDH in steganography, the less explored field of video steganography constitutes an open research area. The successful application of FZDH can be also utilized for steganography purposes. In general, the same techniques are used for video and image steganography and information sources specific to video, such as motion, are often disregarded. Therefore, this field requires further effort, which may produce interesting results.

As a result, substantial contributions involving theoretical aspects and practical methods that can be utilized in real-life applications are introduced to the data hiding field, in this thesis.

REFERENCES

[1] van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F., "A digital watermark," Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference , vol.2, no., pp.86-90 vol.2, 13-16 Nov 1994.

[2] I. J. Cox, M. L. Miller, J. A. Bloom, *Digital Watermarking*, Academic Press, 2002.

[3] H. M. Meral, E. Sevinc, E. Unkar, B. Sankur, A. S. Ozsoy, T. Gungor, "Syntactic tools for text watermarking", In Proc. of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, 2007.

[4] S. Katzenbeisser and Fabien A. P. Petitcolas, *Information Hiding Techniques*, Artech House, 2000.

[5] M. Ramkumar, A.N. Akansu, Signaling for multimedia steganography, IEEE Transactions on Signal Processing 52 (2004) 1100-1111.

[6] P. Moulin, R. Koetter, Data hiding codes, Proceedings of the IEEE 93 (2005) 2083-2127.

[7] Fridrich, J.; Goljan, M.; Baldoza, A.C., "New fragile authentication watermark for images," Image Processing, 2000. Proceedings. 2000 International Conference on , vol.1, no., pp.446-449 vol.1, 2000.

[8] Min Wu; Bede Liu, "Data hiding in binary image for authentication and annotation," Multimedia, IEEE Transactions on , vol.6, no.4, pp. 528-538, Aug. 2004.

[9] Cox, I.J.; Kilian, J.; Leighton, T.; Shamoon, T., "Secure spread spectrum watermarking for images, audio and video," Image Processing, 1996. Proceedings., International Conference on , vol.3, no., pp.243-246 vol.3, 16-19 Sep 1996.

[10] Ton Kalker, Geert Depovere, Jaap Haitsma, and Maurice J. Maes, “Video watermarking system for broadcast monitoring,” Proc. SPIE, 1999, 3657, 103.

[11] Kirovski, D.; Malvar, H., "Robust spread-spectrum audio watermarking," Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on , vol.3, no., pp.1345-1348 vol.3, 2001.

[12] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inform. Theory, vol. 47, no.4, May 2001.

[13] Digimarc: https://www.digimarc.com/, Last Access Date: 06.02.2010.

[14] Bloom, J.A.; Cox, I.J.; Kalker, T.; Linnartz, J.-P.M.G.; Miller, M.L.; Traw, C.B.S., "Copy protection for DVD video," Proceedings of the IEEE , vol.87, no.7, pp.1267-1276, Jul 1999.

[15] Yu, H.H., "Multilayer data hiding for multimedia authentication," Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE , vol.3, no., pp.2055-2059 vol.3, 2001.

[16] Zhicheng Ni; Shi, Y.Q.; Ansari, N.; Wei Su; Qibin Sun; Xiao Lin, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication," Circuits and Systems for Video Technology, IEEE Transactions on , vol.18, no.4, pp.497-509, April 2008.

[17] Dekun Zou; Chai Wah Wu; Guorong Xuan; Shi, Y.Q., "A content-based image authentication system with lossless data hiding," Multimedia and Expo, 2003. ICME '03. Proceedings. 2003 International Conference on , vol.2, no., pp. II-213-16 vol.2, 6-9 July 2003.

[18] Kundur, D.; Hatzinakos, D., "Digital watermarking for telltale tamper proofing and authentication," Proceedings of the IEEE, vol.87, no.7, pp.1167-1180, Jul 1999.

[19] Depovere, G.; Kalker, T.; Haitsma, J.; Maes, M.; de Strycker, L.; Termont, P.; Vandewege, J.; Langell, A.; Alm, C.; Norman, P.; O'Reilly, G.; Howes, B.; Vaanholt, H.; Hintzen, R.; Donnelly, P.; Hudson, A., "The VIVA project: digital watermarking for broadcast monitoring," Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on, vol.2, no., pp.202-205 vol.2, 1999.

[20] Haitsma, J., van der Veen, M., Kalker, T., and Bruekers, F. 2000. Audio watermarking for monitoring and copy protection. In Proceedings of the 2000 ACM Workshops on Multimedia (Los Angeles, California, United States, October 30 - November 03, 2000). MULTIMEDIA '00. ACM, New York, NY, 119-122.

[21] Teletrax – Global Media Intelligence: http://www.teletrax.tv/, Last Access Date: 06.02.2010.

[22] Auditue: http://www.auditude.com/technology/, Last Access Date: 06.02.2010.

[23] Audio Auditing: http://www.audioauditing.com, Last Access Date: 06.02.2010.

[24] Jiang, J.; Armstrong, A., "Data hiding approach for efficient image indexing," Electronics Letters , vol.38, no.23, pp. 1424-1425, 7 Nov 2002.

[25] Libin Cai; Pying Zhao, "Audio quality measurement by using digital watermarking," Electrical and Computer Engineering, 2004. Canadian Conference on , vol.2, no., pp. 1159-1162 Vol.2, 2-5 May 2004.

[26] Nitin Khanna, Aravind K. Mikkilineni, Anthony F. Martone, Gazi N. Ali, George T.-C. Chiu, Jan P. Allebach, Edward J. Delp, A survey of forensic characterization methods for physical devices, Digital Investigation, Volume 3, Supplement 1, The Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06), September 2006, Pages 17-28.

[27] Licks, V.; Jordan, R., "Geometric attacks on image watermarking systems," Multimedia, IEEE , vol.12, no.3, pp. 68-78, July-Sept. 2005.

[28] Petitcolas F. A. P., "Watermarking schemes evaluation," IEEE Signal Processing, vol. 17, no. 5, pp. 58–64, September 2000.

[29] Shelby Pereira, Sviatoslav Voloshynovskiy, Maribel Madueño, Stéphane Marchand-Maillet and Thierry Pun, Second generation benchmarking and application oriented evaluation, In Information Hiding Workshop III, Pittsburgh, PA, USA, April 2001.

[30] V. Solachidis, A. Tefas, N. Nikolaidis, S. Tsekeridou, A. Nikolaidis, I.Pitas, ``A benchmarking protocol for watermarking methods'', 2001 IEEE Int. Conf. on Image Processing (ICIP'01), pp. 1023-1026, Thessaloniki, Greece, 7-10 October, 2001.

[31] S. I. Gelfand and M. S. Pinsker, "Coding for Channel with Random Parameters," Problems of Control and Information Theory, vol. 9, No. 1, pp. 19-31, 1980.

[32] M. Costa, Writing on dirty paper, IEEE Transactions on Information Theory 29 (1983) 439-441.

[33] B. Chen and G. W. Wornell, "An Information-Theoretic Approach to the Design of Robust Digital Watermarking Systems," *Proc. Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Phoneix, AZ, March 1999.

[34] J.J. Eggers, R. Bäuml, R. Tzschoppe, B. Girod, Scalar Costa scheme for information embedding, IEEE Transactions on Signal Processing 51 (2003) 1003-1019.

[35] Perez-Gonzalez, F.; Balado, F., "Quantized projection data hiding," Image Processing. 2002. Proceedings. 2002 International Conference on , vol.2, no., pp. II-889-II-892 vol.2, 2002.

[36] Perez-Freire, L.; Perez-Gonzalez, F.; Voloshynovskiy, S., "An accurate analysis of scalar quantization-based data hiding," Information Forensics and Security, IEEE Transactions on , vol.1, no.1, pp. 80-86, March 2006.

[37] M. Ramkumar, A. N. Akansu, Self-noise suppression schemes in blind image steganography, Proceedings of SPIE Multimedia Systems and Applications II 3845 (1999) 55-65.

[38] H. T. Sencar, M. Ramkumar, A.N. Akansu, A new perspective for embedding-detection methods with distortion compensation and thresholding processing techniques, in: IEEE International Conference on Image Processing 2 (2003) 507-510.

[39] Ramkumar, M.; Akansu, A.N., "Capacity estimates for data hiding in compressed images," Image Processing, IEEE Transactions on , vol.10, no.8, pp.1252-1263, Aug 2001.

[40] Wu, M., Yu, H., Liu, B.: Data hiding in image and video .II. Designs and applications. IEEE Transactions on Image Processing 12, 696--705 (2003).

[41] I.J. Cox, M.L. Miller, A.L. McKellips, Watermarking as communications with side information, Proceedings of the IEEE 87 (1999) 1127-1141.

[42] U. Erez, R. Zamir, Achieving 1/2 log (1+SNR) on the AWGN channel with lattice encoding and decoding, IEEE Transactions on Information Theory 50 (2004) 2293-2314.

[43] T. Liu, P. Moulin, R. Koetter, On error exponents of modulo lattice additive noise channels, IEEE Transactions on Information Theory 52 (2006) 454–471.

[44] A.S. Cohen, A. Lapidoth, The Gaussian watermarking game, IEEE Transactions on Information Theory 48 (2002) 1639-1667.

[45] E. Esen and A. A. Alatan, "Data Hiding Using Trellis Coded Quantization", IEEE ICIP 2004, Singapore, 24-27 October 2004.

[46] E. Esen, A. A. Alatan, A practical lattice QIM method: TCQ-IS, in: 13th European Signal Processing Conference (EUSIPCO 2005), Antalya, Turkey, September 2005.

[47] J. Chou, S.S. Pradhan, K. Ramchandran, Turbo coded trellis-based constructions for data embedding: channel coding with side information, in: Signals, Thirty-Fifth Asilomar Conference on Systems and Computers 1 (2001) 305-309.

[48] P. Moulin, A. K. Goteti, Block QIM watermarking games, IEEE Transactions on Information Forensics and Security 1 (2006) 293-310.

[49] K. Solanki, N. Jacobsen, U. Madhow, B.S. Manjunath, S. Chandrasekaran, Robust image-adaptive data hiding using erasure and error correction, IEEE Transactions on Image Processing 13 (2004) 1627-1639.

[50] A. Sarkar U. Madhow, S. Chandrasekaran, B.S. Manjunath, Adaptive MPEG-2 Video Data Hiding Scheme, in: Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents IX (2007).

[51] W. Chen, W. Huang, VQ indexes compression and information hiding using hybrid lossless index coding, Digital Signal Processing 19 (2009) 433-443.

[52] E. Esen, A. A. Alatan, Forbidden zone data hiding, in: IEEE International Conference on Image Processing (2006) 1393-1396.

[53] A. B. Watson, R. Borthwick, M. Taylor, Image quality and entropy masking, Proceedings of SPIE Human Vision and Electronic Imaging 3016 (1997) 2-12.

[54] C. I. Podilcuk, W. Zeng, Perceptual watermarking of still images, in: IEEE First Workshop on Multimedia Signal Processing (1997) 363-368.

[55] C.I. Podilcuk, W. Zeng, Image-adaptive watermarking using visual models, IEEE Journal on Selected Areas in Communications 16 (1998) 525-539.

[56] J. Huang, Y.Q. Shi, Adaptive image watermarking scheme based on visual masking, Electronics Letters 34 (1998) 748-750.

[57] Conway, J.H., Sloane, N.J.A., *Sphere Packings, Lattices, and Groups*, Springer-Verlag, New York, 1988.

[58] I. Cox, J . Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing 6, pp. 1673 — 1687, Dec. 1997.

[59] Wu, M., Yu, H., Liu, B.: Data hiding in image and video .I. Fundamental issues and solutions. IEEE Transactions on Image Processing 12, 685--695 (2003).

[60] Kapotas, S.K.; Varsaki, E.E.; Skodras, A.N.: Data Hiding in H. 264 Encoded Video Sequences. In: IEEE 9th Workshop on Multimedia Signal Processing, MMSP 2007, pp.373--376. (2007).

[61] Schlauweg, M., Profrock, D., Muller, E.: Correction of Insertions and Deletions in Selective Watermarking. In: IEEE International Conference on Signal Image Technology and Internet Based Systems, SITIS '08, pp.277—284. (2008).

[62] Liu, H., Huang, J., Shi, Y.Q.: DWT-Based Video Data Hiding Robust to MPEG Compression and Frame Loss. Int. Journal of Image and Graphics 5, 111—134 (2005).

[63] Esen, E., Doğan, Z., Ates, T.K., Alatan, A.A.: Comparison of Quantization Index Modulation and Forbidden Zone Data Hiding for Compressed Domain Video Data Hiding. In: IEEE 17th Signal Processing and Communications Applications Conference SIU (2009).

[64] Divsalar, D., Jin, H., McEliece, R.J.:Coding theorems for turbo-like codes. In: Proc. 36th Allerton Conf. Communications, Control, and Computing, pp. 201--210. (1998).

[65] Mansour, M.M.: A Turbo-Decoding Message-Passing Algorithm for Sparse Parity-Check Matrix Codes. IEEE Transactions on Signal Processing 54, 4376--4392 (2006).

[66] R.Zamir, S.Shamai, U.Erez, Nested linear/lattice codes for structured multiterminal binning, IEEE Transactions on Information Theory 48 (2002) 1250-1276.

[67] Wei, Z., Ngan, K.N.: Spatio-Temporal Just Noticeable Distortion Profile for Grey Scale Image/Video in DCT Domain. IEEE Transactions on Circuits and Systems for Video Technology 19, 337--346 (2009).

[68] M.W. Marcellin and T.R. Fischer, "Trellis coded quantization of memoryless and Gauss-Markov sources," IEEE Transactions on Communications, vol. 38, pp. 82–93, January 1990.

[69] J. Chou, S. S. Pradhan, L. El Ghaoui, and K. Ramchandran, "A robust optimization solution to the data hiding problem using distributed source coding principles," Proc. SPIE conference, San Jose, CA, Jan. 2000.

[70] G. Ungerboeck, "Channel coding with multilevel/phase signals," IEEE Trans. Inform. Theory, vol.28, pp.55-67, Jan. 1982.

[71] Kefeng Fan; Qingqi Pei; Wei Mo; Xinhua Zhao; Xiaoji Li, "A Test Platform for the Security and Quality of Video Watermarking Content Protection System," Communication Technology, 2006. ICCT '06. International Conference on , vol., no., pp.1-4, 27-30 Nov. 2006.

[72] Maes, M.; Kalker, T.; Linnartz, J.-P.M.G.; Talstra, J.; Depovere, F.G.; Haitsma, J., "Digital watermarking for DVD video copy protection," Signal Processing Magazine, IEEE , vol.17, no.5, pp.47-57, Sep 2000.

[73] M. K. Mihcak, R. Venkatesan, and T. Liu, "Watermarking via optimization algorithms for quantizing randomized semi-global image statistics," *Multimedia Systems*, vol. 11, no. 2, pp.185-200, December 2005.

VITA

Ersin Esen was born in Karadeniz Ereğli, Turkey, in 1976. He received the B.S. and M.S degrees in Electrical and Electronics Engineering, from Bilkent University, Ankara, Turkey in 1998 and 2000, respectively. Between 1998 and 2001 he was a research assistant at the same department. In 2001 he commenced his doctorate study at Electrical and Electronics Engineering at Middle East Technical University. Since 2001 he works as a researcher at TÜBİTAK (The Scientific and Technological Research Council of Turkey) UZAY (formerly BİLTEN) Research Institute. In 2005, he worked at Microsoft Research for three months as an intern. He worked as technical leader in RTÜK SKAAS (Digital Recording Archiving and Analysis System of Radio Television Supreme Council of Turkey) Project. Since 2008 he is working as the manager of SKAAS KAVTAN (Development of Concept Detection System for SKAAS) Project. His research interests include data hiding, content based retrieval, video archive management, and audio-visual concept detection.

His publications are as follows:

Conference Papers

- E. Esen and A. Aydın Alatan, "Block Based Video Data Hiding using Repeat Accumulate Codes and Forbidden Zone Data Hiding," IEEE Pacific-Rim Conference on Multimedia, December 15-18, 2009, Bangkok, Thailand.
- Esen, E., Doğan, Z., Ates, T.K., Alatan, A.A., "Comparison of Quantization Index Modulation and Forbidden Zone Data Hiding for Compressed Domain Video Data Hiding", SIU 2009, IEEE 17th Signal Processing and Communications Applications Conference, Antalya, Turkey.
- A. Saracoglu, E. Esen, T. K. Ates, B. Oskay Acar, U. Zubari, E. C. Ozan, E. Ozalp, A. A. Alatan, T. Ciloglu, "Content Based Copy Detection with Coarse Audio Visual Fingerprints", CBMI 2009, Chania in Crete Island, Greece.
- B. Oskay Acar , Ü. Zubari, E. C. Ozan, A. Saracoğlu, E. Esen, T. Çiloğlu, "Voting System Based Robust and Efficient Audio Copy Detection", SIU 2009,

IEEE 17th Signal Processing and Communications Applications Conference, Antalya, Turkey.

- Esen, E., Saracoğlu, A., Ates, T.K., Oskay Acar, B., Zubari, U., Alatan, A.A., "Content Based Video Copy Detection with Coarse Features", SIU 2009, IEEE 17th Signal Processing and Communications Applications Conference, Antalya, Turkey.
- E. Esen, M. Soysal, T. K. Ateş, A. Saraçoğlu and A. A. Alatan, "A Fast Method for Animated TV Logo Detection", CBMI 2008, London, England.
- T. K. Ateş, E. Esen, A. Saraçoğlu ve A. A. Alatan, "Sınır Eşlemeye Dayalı Yarı-Saydam TV Logosu Tespiti", IEEE SIU 2008, Antalya, Türkiye.
- E. Esen ve Y. Kemal Alp, "Özyineli En Kisa Kapsayan Ağaç Algoritmasinda Bölgesel ve Sinirsal Bilginin Birleştirimi ile İmge Bölütleme", IEEE SIU 2007, Eskişehir, Türkiye.
- E. Esen ve A. A. Alatan, "Bilgi Saklamada Yeni Bir Kavram: Yasak Bölge", to be presented in SİU 2006, Antalya Turkey.
- E. Esen and A. A. Alatan, "Forbidden Zone Data Hiding", IEEE ICIP 2006, 8-11 October 2006, Atlanta, GA, USA.
- E. Esen and A. A. Alatan, "A Practical Lattice QIM Method: TCQ-IS", EUSIPCO 2005, 4-8 September 2005, Antalya Turkey.
- E. Esen ve A. A. Alatan, "Kafes Kodlamali Nicemleme ile Bilgi Saklama", IEEE SIU , Kusadasi Turkiye, 28-30.04.2004.
- E. Esen and A. A. Alatan, "Data Hiding Using Trellis Coded Quantization", IEEE ICIP 2004, 24-27 October 2004, Singapore.
- Ersin Esen, Ozgur Onur, Medeni Soysal, Yagiz Yasaroglu, Serhat Tekinalp, and A. Aydin Alatan, "A Mpeg-7 compliant Video Management System: BilVMS", WIAMIS 2003, London, UK.
- A. Yilmaz, E. Esen and A. A. Alatan, "Combined Concealment, Synchronzation, and Error Detection Using Data Hiding," WIAMIS '2003, London, UK.
- Esen, E., Yaşaroğlu, Y., Önür, Ö., Soysal, M., Tekinalp, S. ve Alatan, A.A., "MPEG-7 Uyumlu Video Yönetim Sistemi", Sinyal İşleme ve İletişim Uygulamaları Kurultayı, SIU 2003, 18-20 Haziran 2003, Koç Üniversitesi, İstanbul, Türkiye.

- E. Esen, A. A. Alatan, and M. Askar, "Trellis Coded Quantization for Data Hiding," EUROCON 2003, September 22-24 2003, Ljubljana, Slovenia.
- E. Esen ve A. Alatan, "Nicemleme Dizin Modulasyonu ile Bilgi Saklama", SIU 2002, Denizli, Türkiye.
- E. Esen and L. Onural, "Supervised Segmentation for Video Applications", Proc. of 16th International Symposium on Computer and Information Sciences, Nov.5-7, 2001, Antalya Turkey, pp.576-583.